CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 35 / PCEMI 35

MDS RESEARCH PROJECT/PROJET DE RECHERCHE MED

MAKING NEW FRIENDS, TRUSTING NEW FRIENDS

THE CHALLENGES OF COALITION INTELLIGENCE SHARING IN AFGHANISTAN

By/par lcol L.H. Rémillard

24 avril 2009

ABSTRACT

The current military operating environment (CMOE), characterized by insurgency, counter-insurgency (COIN) and coalition operations has greatly impacted how intelligence is shared at the tactical and operational levels. The case of Afghanistan is studied in order to evaluate the effectiveness of the coalition intelligence apparatus with regards to intelligence sharing and the development of a common intelligence picture (CIP) in Afghanistan. The intelligence function is directly connected to the concepts of national interest and trust which dictates how intelligence is been shared amongst partner nations. Intelligence sharing is also affected by factors such as policies, organizational culture, and information technology. Solutions to improve the current intelligence exchange mechanisms are found at the strategic, operational and tactical levels. These changes require strong leadership and initiative from existing multinational organizations as well as from nations who will be leading future military coalitions.

TABLE OF CONTENTS

INTRODUCTION

"So it is said that if you know others and know yourself, you will not be imperiled in a hundred battles."[1] Intelligence has played a critical part in the success of military operations throughout the history of man[2]. Renowned military strategists such as Sun Tzu, Jomini and Clausewitz, have always defined intelligence, the knowledge of the enemy's capabilities and intentions, as a key element of military success. Modern governments have also invested significant sums of money over the years in developing methods and technical means that provide advantages over and insights into potential competitors or enemies. According to Brigadier-General Nordick, former Canadian Chief of Defence Intelligence (CDI):

> …intelligence capabilities are protected like the crown's jewels in most countries and it remains difficult to share information related to sources and capabilities because of the risk of compromise.[3]

In an article discussing the difficulties and dilemmas of international intelligence cooperation, Stéphane Lefebvre recognizes the importance of sharing tactical intelligence to ensure military success.[4] He adds that "for these enhanced relationship to work well, confidence and trust are essential ingredients, as are the perceived benefits to both sides in the liaison."[5]

---

[1] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1971), 84.

[2] John Keegan, *Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda*. (Toronto: Key Porter Books, 2003), 2.

[3] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

[4] Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence*, Vol 16 (2003): 527.

[5] *Ibid*, 528.

The events of 11 September 2001[6] and the emergence of fundamentalist terrorism have led Western intelligence communities[7] to re-visit the way that they have been operating and to focus on the importance of expediting and facilitating collaboration between national and international partners. The post 9/11 period has also been characterized by a shift in organizational culture from the "need to know" to the "need to share" philosophy.[8] Intelligence was now viewed by the highest levels of command as the nerve of the war against the Islamist fundamentalist movement known by many in the U.S. as the Global War on Terror (GWOT).[9]

The attacks of 9/11 have resulted in the worldwide denunciation of the fundamentalist Islamist movement and the establishment of an ad-hoc military coalition to stabilize Afghanistan. The rapid overthrow of the Taliban regime in 2001 prompted a violent insurgency to develop.[10] A heterogeneous group of insurgents' elements have since then been involved in an insurgency that has continued to intensify over that past seven years.[11]

---

[6] The terrorist attacks conducted on the United States on 11 September 2001 will be referred to as 9/11.

[7] Different intelligence communities (IC) exist: National IC refers to one country's intelligence organizations (for example, the U.S. IC includes organizations such as the CIA, DIA, NSA, NRO, elements of the FBI, State Department, Homeland, and others). International IC refers to the association of foreign intelligence organizations that share intelligence of mutual interests. Defence IC refers to the military numerous specialized intelligence organizations that work together in support of the Defence of a nation.

[8] US DNI 500 Day Plan and Lieutenant-Colonel G. Jensen CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006.

[9] The GWOT (also known as the War on Terror and most recently the Long War) is a campaign initiated by the United States government under President George W. Bush which includes various military, political, and legal actions following the September 11, 2001 attacks on the United States.

[10] Seth Jones, *Counterinsurgency in Afghanistan.* (Santa Monica, CA: RAND Corporation, 2008), 30.

[11] *Ibid.*, xi.

The military coalition in Afghanistan under Operation Enduring Freedom (OEF) and the International Security Assistance Force (ISAF) has brought together a mix of countries that have not traditionally been involved neither in complex combined military operations nor in the sharing of sensitive intelligence matters in recent years. While some intelligence liaison programs existed between NATO, western nations and countries from the Middle East and from Central Asia, the events of 9/11 provided a new operational twist to these relationships.[12] This new spontaneous coalition has been facing many complex challenges such as interoperability, cultural and linguistic issues as well as the absence of existing mechanisms to effectively share intelligence between all. As argued by Australian intelligence specialist Desmond Ball, "the few multilateral arrangements of the Cold War offered no models for the current situation."[13]

Many of the countries involved in the current military coalition for Afghanistan were not members of established Western multinational organizations such as NATO, the North American Aerospace Defense Command (NORAD), the America, Britain, Canada and Australia military standardization group (ABCA), the European Union or the "Five Eyes" Community (ABCA nations and New Zealand). Many of these non-traditional partners have just recently developed common interests on the basis of the emergence of a new indiscriminate global threat that is transnational by nature. For example, within the current military coalition in Afghanistan, problems with regards to intelligence sharing stems mainly from the participation of those countries which are not associated with any of the long standing military alliances.

---

[12] Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence*, Vol 16 (2003): 527.

[13] *Ibid*, 529.

Coalition operations such as the recent missions in Bosnia, Kosovo, Afghanistan and Iraq have all presented complex challenges where the exchange of intelligence among participating nations has always been highlighted as problematic.[14] In Afghanistan, where the situation is one of asymmetric and unpredictable threats, the development of a Common Intelligence Picture (CIP) remains one of the key challenges for commanders and intelligence staff of the coalition.[15] All partners need to agree on how they view the threats in order to conduct successful coordinated coalition operations.[16] Despite being allies, coalition members are not all treated as equals by the more developed nations. Some of the most sensitive technical intelligence is not shared with many of the new allies based on the higher risk of compromise.[17] The lack of formal coalition intelligence sharing procedures, the limited level of trust displayed by some partner nations towards some members of the coalition and the restrictive security guidelines under which each country operates illustrate some of the causes of this intelligence dissemination problem.[18]

---

[14] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 2 & Melissa Patrick "Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operations Joint Endeavour" *Army War College* (10 April 2000): 3 & Major Barret K. Peavie (US Army) "Intelligence sharing in Bosnia" *United States Army Command and General Staff College* (AY 00-01): 1 & Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[15] Colonel, W. Semianiw OMM CD, former Commander Task Force Kabul, OP ATHENA Roto 3 (February 2005-August 2005), *Interview*, 3 March 05 & Major-General A.B. Leslie CMM MSC MSM CD, former Deputy Commander International Security Assistance Force – Kabul, Afghanistan (August 2003-February 2004), *Interview*, 27 April 2006.

[16] *Ibid*.

[17] Jorgen Kruger, Director Intelligence Policies and Programs, CDI, *Interview*, 2 November 2007 & Lieutenant-Colonel G. Jensen CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006.

RESEARCH QUESTIONS

Are the current methods and procedures associated with the sharing of intelligence involving coalition partners in Afghanistan able to maximize the efficiency of counterinsurgency operations? What are the difficulties, challenges and alternatives to intelligence sharing in a counterinsurgency environment such as Afghanistan?

THESIS

The counterinsurgency (COIN) context implies particular challenges, highlighted by the current practices in Afghanistan, which do not allow for the efficient sharing of intelligence between all of the coalition partners. The fact that the "*need to know*" concept is being replaced by the "*need to share*" or "*responsibility to provide*" philosophies reveals that it is possible to envision some practical solutions to improve the current situation.

OUTLINE

This dissertation has been divided into five chapters. Chapter 1 displays a review of the available literature on the issue of intelligence sharing in the context of coalition counterinsurgency warfare with a particular focus on Afghanistan. It focuses on the theories of COIN operations as well as through some Canadian and U.S. COIN doctrine. Finally, this chapter displays the intelligence theoretical framework that will be used as the baseline knowledge throughout this study. Chapter 2, entitled "the Afghan contexts", describes some of the main characteristics defining the current military operating environment (CMOE) in Afghanistan: insurgency, counterinsurgency and coalition

---

[18] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

warfare. Chapter 3 reveals the importance of intelligence in COIN operations through the writings of some of the most prominent authors on the subject. It also displays how the Afghan context is affecting the intelligence function as a whole and how the coalition intelligence apparatus is organized.

Chapter 4 focuses on identifying the hurdles to efficient intelligence sharing in Afghanistan. It highlights the fact that strategic decisions at the national level have had a colossal impact on how intelligence is being shared in Afghanistan. It identifies some of the elements responsible for the current problems in that field: trust, national interests, organizational cultures, policies and information technology (IT). Chapter 5 exhibits some of the lessons learned from the Afghanistan context that have already improved the efficiency of coalition intelligence sharing. It also presents a series of additional solutions that have the potential to improve sharing of intelligence among coalition partners in the future.

CHAPTER 1 – LITERATURE REVIEW AND THEORETICAL FRAMEWORK

LITERATURE REVIEW

There is very little literature published specifically on coalition intelligence sharing at the operational or tactical levels. There are a few unpublished papers from U.S. Command and Staff College as well as War College that focus at the heart of this thesis' topic. Those papers, written by Colonel George K. Gramer, Lieutenant-Colonel Steve Manning, Melissa Patrick and Major Barrett Peavie all denote a U.S. view on the issues of intelligence sharing, and always from the perspective of the lead nation.[19] These authors assess that the main problem with intelligence sharing in coalition operations is essentially a dissemination issue.

The fact that all these authors have viewed the problem mainly as a dissemination issue denotes the autonomy displayed by the U.S. military intelligence apparatus and its ability to operate without the support of any coalition partners if necessary. These papers also demonstrated that U.S.' concerns with intelligence sharing have historically been focused on the technical challenges associated with disseminating selected intelligence to its coalition partners rather than the other way around. This element is critical in order to better understand the way the U.S. military intelligence system can sometimes perceive the coalition intelligence community as a nuisance rather than a force multiplier. Moreover, none of the literature reviewed during this research examined the intelligence

---

[19] Colonel George K. Jr Gramer (U.S. Army). "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College*, 17 May 1999 & Lieutenant-Colonel Steve Manning (USMC). "Improved Intelligence Support to our Coalition Partners at the Operational Level" *Naval War College*, 9 May 2004 & Patrick, Melissa, Intelligence "Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operations Joint Endeavour" *Army War College*, 10 April 2000. & Major Barret K. Peavie (US Army). "Intelligence sharing in Bosnia" *United States Army Command and General Staff College* (AY 2000-2001).

sharing problem from the non-lead nation's point of view i.e. from a point of view other that of the U.S..

Some articles from specialized journals such as the *International Journal of Intelligence and Counter-intelligence* discuss the difficulties and dilemmas that are associated with intelligence sharing at the strategic and national levels.[20] All of these articles argue that there is no self-sufficient national intelligence system, not even in the U.S., and that alliances bring along more benefits than fallbacks. These articles also make constant reference to the fact that intelligence plays a pivotal role in the successes of military operations however; they all lack the supporting data at the operational and tactical levels to support their argument.

In general, books on intelligence are focused on the strategic/national level and did not provide many insights into the realities of coalition operations at the operational and tactical levels. For example, books written by Michael Herman, John Keegan, Abram Shulsky, Robert Steele and Adrian Weale all described western intelligence communities and their apparatus but at the strategic and national levels only.[21] Other

---

[20] Chris Clough. "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation" *International Journal of Intelligence and CounterIntelligence*, Vol 17 (2004):601-613 & Stéphane Lefebvre. "The Difficulties and Dilemmas of International Intelligence Cooperation" *International Journal of Intelligence and CounterIntelligence*, Vol 16 (2003):527-542 & Stephanie McLuhan. "One Issue, Two Voices. Intelligence Sharing between Canada and the United States: A Matter of National Survival" *International Journal of Intelligence and CounterIntelligence*, Issue 6 (January 2007):1-15 & Paul Rexton Kan. "Counternarcotics Operations within Counterinsurgency: The Pivotal Role of Intelligence" *International Journal of Intelligence and CounterIntelligence*, Vol 19 (2006):586-599 & Martin Rudner. "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism" *International Journal of Intelligence and CounterIntelligence*, Vol 17 (2004):193-230 & Jennifer E Simms. "Foreign Intelligence Liaison: Devils, Deals, and Details" *International Journal of Intelligence and CounterIntelligence*, Vol 19 (2006):195-217.

[21] Michael Herman. *Intelligence Power in Peace and War*. Cambridge University Press, 1996. & John Keegan. *Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda*. Toronto: Key Porter Books, 2003. & Abram N. Shulsky. *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. Washington D.C.: Potomac Books, 2002. & Robert David Steele. *The New Craft of Intelligence. Personal,*

books written by Jeffrey Richelson and David Stafford focused on intelligence alliances but were also exclusively centred on the strategic level.[22] They provided historical background about existing intelligence standing agreements between the U.S., Canada, Australia, Great Britain and New Zealand but no insight on how these alliances were transposed to military operations at the tactical and operational levels.

While the literature on military intelligence matters is somehow limited, the same cannot be said about the elements that characterize the CMOE in Afghanistan. Numerous books and articles have been written on insurgency, counterinsurgency, the current situation in Afghanistan as well as the concept of coalition warfare.[23] For instance, C*ounterinsurgency in Afghanistan*, written by Seth Jones provided a description of the current Afghan counterinsurgency as well as presenting some recommendations to improve the coalition' successes.[24]

Public and Political. Oakton, Virginia: OSS International Press, 2002. & Adrian Weale. *Secret Warfare*. London: Hodder & Stoughton, 1997.

[22] Jeffrey T. Richelson & Desmond Ball, The Ties that Bind: Intelligence Cooperation between the UKUSA Countries. Boston: Allen & Unwin, 1985. & David Stafford. American-British-Canadian Intelligence Relations 1939-2000. London: Frank Cass, 2000.

[23] Ian Becket et al. *Modern Counter-Insurgency*. Burlington: Asgate Publishing Limited, 2007 & Ronald Haycock et al. *Regular Armies and Insurgency*. London: Croom Helm, 1979. & Leroy Thompson. *The Counterinsurgency Manual*. London: Greenhill Books, 2002. & Roger Trinquier. *Modern Warfare: A French View of Counterinsurgency*. New-York: Praeger, 1964. & William Andres, Craig Wills and Thomas E. Griffith Jr. "Winning with Allies: The Strategic Value of the Afghan Model" *International Security*, Vol 30, no.3 (Winter 2005/2006):124-160. & Brigadier Nigel Aylwin-Foster, "Changing the Army for Counterinsurgency Operations" *Military Review*, (November-December 2005):2-15.& Jeffrey P Bialos and Stuart L. Koehl. "The NATO Response Force: Facilitating Coalition Warfare Through Technology Transfer and Information sharing" *Center for Technology and National Security Policy – National Defense University*, September 2005 & General Richard A Cody and Robert Maginnis. "Coalition Interoperability: ABCA's New Focus" *Military Review*, (November-December 2006):65-68. & James R. Howcroft. "Technology, Intelligence and Trust" *Joint Forces Quarterly*, Vol 46, no.2 (2007):20-26. & Robert Maginnis. "ABCA: A Petri Dish for Multinational Interoperability" *Joint Forces Quarterly*, Vol 37, no.2 (2005):53-58. & Steven Metz. "New Challenges and Old Concepts: Understanding 21st Century Insurgency" *Parameters*, Vol 37, Issue 4 (21 December 2007):20-32 & Robert Ricassi. "Principles for Coalition Warfare" *Joint Forces Quarterly*, Vol 1, no.1 (1993):58-71. & Elisabeth Sherwood-Randall. "The Case for Alliances" *Joint Forces Quarterly*, Issue 43, (2006):54-59.

[24] Seth Jones. *Counterinsurgency in Afghanistan*. Santa Monica, CA: RAND Corporation, 2008.

Newspaper articles, internet news services, professional and specialized journals also provided detailed information on topics such as counterinsurgency, advances in technologies, organizational culture, coalition operations and military intelligence. They also provided key information on specific situations and historical examples that supported this thesis all the way through. These articles were often forward-looking in that they provided new ways to look at current military issues.

Canadian, American, NATO and ABCA intelligence doctrines, policies and concepts have also been studied in details. However, more emphasis has been placed on studying U.S. Department of Defense (DOD) documentation with regards to intelligence sharing since the United States is undoubtedly the backbone of the current military coalition in Afghanistan. Specifically, the U.S. Joint Intelligence Doctrine 2-01 includes specific sections on how to perform intelligence operations in a coalition environment and refers to the Foreign Disclosure Program.[25] On the other hand Canadian doctrine on intelligence operations is not as complete even though it often looks very similar to the U.S. documentation. In Canada, there is neither a doctrine nor a policy that explains how intelligence can and must be shared with other coalition partners[26]. Intelligence doctrine is fairly general and even outdated in that it doesn't include some of the new concepts such as the all source intelligence centre (ASIC) even though it has been a model used in Afghanistan since 2003.[27] ABCA has developed a coalition intelligence handbook

---

[25] B-GJ-005-200FP-000, Joint Intelligence Doctrine, November 11, 2002 & U.S. Joint Chiefs of Staff, "Joint and National Intelligence Support to Military Operations" Joint Publication 2-01, 7 October 2004.

[26] Jorgen Kruger, Director Intelligence Policies and Programs, CDI, *Interview*, 2 November 2007, Ottawa, Canada.

[27] B-GJ-005-200FP-000, Joint Intelligence Doctrine, November 11, 2002.

detailing how to perform coalition intelligence operations.[28] This ABCA document presents some general guidance on how to organize multinational intelligence organizations in support of coalition operations but do not provide mechanisms or policies on how to share intelligence between coalition members.

This literature review has demonstrated that very few authors have written on intelligence sharing issues within coalition operations in general or on current operations in Afghanistan. It also highlights the fact that most of the literature on intelligence sharing has focused solely on strategic and national issues or exclusively on the U.S. perspective to the issue of sharing. It is important to note that there are no published studies that specifically discuss the topic of this thesis stressing the originality of this dissertation. The lack of documentation available at the unclassified level has forced the author to conduct over twenty interviews with intelligence officers and military commanders in order to answer many of the questions of this research. These interviews were conducted over the past three years with the approval of the RMC Research Ethics Board. The following segment will now present the intelligence theoretical framework utilized by the author throughout this paper.

INTELLIGENCE THEORETICAL FRAMEWORK

> "Foreknowledge' cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation."[29]

The term intelligence often makes reference to one of the three following categories:

---

[28] Coalition Intelligence Handbook, Quadripartite Advisory Publication (QAP) Number 325, Edition 2, Dated July 2003.

[29] Tzu Sun, *The Art of War* (Oxford: Oxford University Press, 1971), 145.

- an activity: associated with the conduct of operations;
- a function; which includes all of the specialties and organizations; and
- a product: which is the result of processed information.[30]

For the purpose of this paper, and specifically in the context of sharing, the author will focus on intelligence as the end product but he will also touch on the two others from time to time. The Concise Oxford Dictionary defines intelligence as: "The intellect, the understanding…the collection of information, especially of military or political value."[31] In the Canadian Forces Joint Intelligence Doctrine Manual, intelligence is defined as:

> The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements or areas of actual or potential operations.[32]

U.S. Joint Publication 2-01 entitled Joint and National Intelligence Support to Military Operations describes intelligence as:

> The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.[33]

These definitions all have some common characteristics even though the one from the dictionary is more general in comparison to the ones found in the two military intelligence publications presented above. Moreover, they all make reference to information and knowledge of an adversary and of a process of analyzing information pertinent for specific users. In blunt terms, intelligence is a type of knowledge acquired

---

[30] Canadian Forces Publications, *Joint Intelligence Manual- B-GL-005-200-FP-000*. (November 6, 2002): 1-2 & Sherman Kent "*Strategic Intelligence for American World Policy*" (Hamden: Anchon Books, 1965), xxiii.

[31] R.E. Allen, "*The Concise Oxford Dictionary of Current English*". (Oxford: Oxford University Press, 1990), 617.

[32] Canadian Forces Publications, *Joint Intelligence Manual- B-GL-005-200-FP-000*. (November 6, 2002): 1-3.

[33] United States Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations Joint Publication 2-01*, (October 7, 2004): GL-17.

through different methods that is required by an entity to obtain an advantage over an adversary/competitor or potential adversary/competitor.

The intelligence cycle is a framework employed by modern military forces in order to conduct intelligence operations. The U.S. military uses a six step process of planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.[34] The Canadian Forces version covers the same topics as the U.S. version but through four phases instead of six: direction, collection, processing and dissemination.[35] The intelligence cycle is a critical tool used by intelligence professionals in order to conduct efficient intelligence operations.

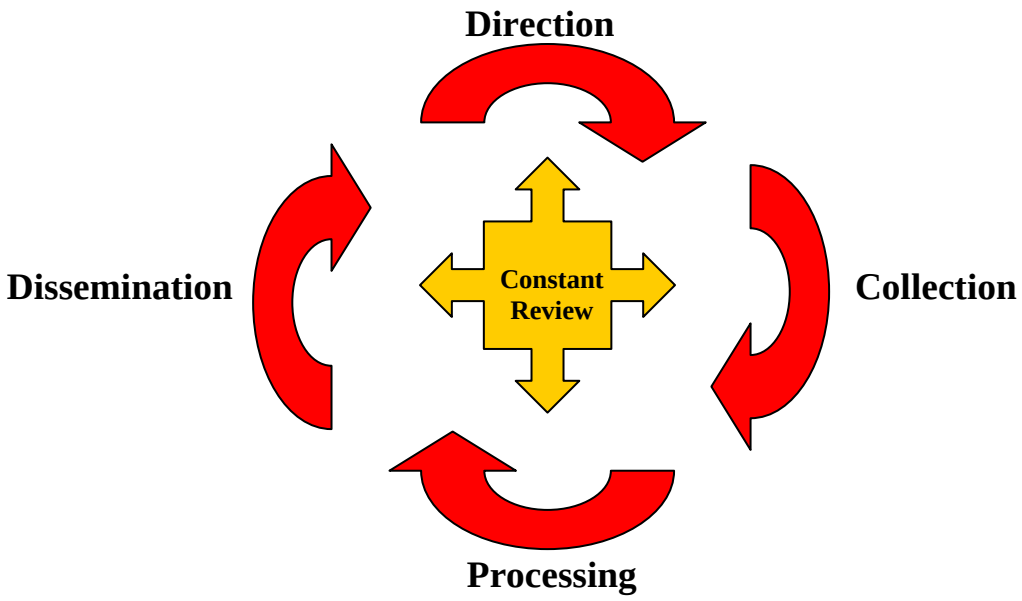

Figure 1: The Intelligence Cycle

[34] *Ibid*., III-1.

[35] Canadian Forces Publications, *Joint Intelligence Manual- B-GL-005-200-FP-000*. (November 6, 2002): 2-3.

The intelligence cycle always starts with the *direction* phase. Direction is divided in two distinct aspects: The first aspect is the direction given by a commander to his intelligence staff which will be translated into the development of the commander's priority intelligence requirements (PIRs). From those PIRs, the intelligence staff will provide the second aspect of the direction phase to the collectors, collators and analysts through the development of a comprehensive intelligence collection plan (ICP). The ICP will contain refined intelligence requirements (IR) based on the more generic PIRs and even more refined indicators or essential elements of information (EEIs). The development of the ICP will identify intelligence gaps which will require request for information (RFIs) to be produced and a proper collection management process to be established. This process is referred to as the Collection Coordination and Intelligence Requirements Management (CCIRM). The direction phase is arguably the most important of the four phases of the cycle as it provides the focus for all of the other intelligence related activities. This phase must be reviewed constantly in order to ensure that the intelligence produced and disseminated at the end of the cycle is relevant for commanders and decision makers as well as the soldiers who need it.[36]

The second phase of the intelligence cycle is *collection*. It is defined as "the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence."[37]

---

[36] *Ibid*., 2-4, 2-5 and Thibault, Master Warrant Officer, M., MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005. MWO Thibault is probably one of the most experienced intelligence operators in the Canadian Forces Intelligence Branch today with nine overseas operational tours in the Middle East, Afghanistan, the Balkans and the Caribbean. He has served in a myriad of functions including CCIRM manager, senior analyst, and HUMINT ops Warrant Officer.

[37] Canadian Forces Publications, *Joint Intelligence Manual- B-GL-005-200-FP-000*. (November 6, 2002): 2-6.

Collection is driven by the collection plan and is normally coordinated by a centralized CCIRM management authority in order to avoid duplication of efforts and also in prioritizing the collection effort. Proper direction is essential in order to avoid wasting limited assets on unnecessary tasks. This requires the ICP to be reviewed periodically.

Collection is probably the sexier aspect of the intelligence cycle. Most organized collectors are categorized in the following specialties: HUMINT, SIGINT and IMINT.[38] Collection is also conducted through activities that are not exclusive to intelligence organizations such as observation, surveillance and reconnaissance. The philosophy that sees every soldier, sailor and airmen as a potential collector is a good example that everyone has the potential to collect information that could lead to be processed into actionable intelligence.[39]

The third phase of the cycle is *processing*. This phase has often been referred to as the analytical part of the intelligence cycle. It is characterized by the manipulation of an important amount of data and information that has been collected and collated through the CCIRM process in order to answer specific IR and PIRs. This is the part where information and data is transformed into intelligence through an analytical process and often with the use of specifically developed software. These software provide tools to analysts and collators in order to help them deal with huge databases and the constant

---

[38] Human intelligence (HUMINT) is defined as a type of intelligence collected by individuals in an impromptu or organized fashion. HUMINT sub specialties include elicitation, liaison, counter-intelligence, source and agent handling, patrol reports and interrogation. Signals intelligence (SIGINT) is defined as the interception of signals between individuals (communications intelligence (COMINT)) or emanating from equipment/machine (electronic intelligence (ELINT)). Imagery Intelligence (IMINT) is defined as an intelligence collection discipline characterized by the acquisition of images (optical, infrared and radar) through the use of a technical medium such as satellites, reconnaissance aircraft and hand held cameras.

[39] Refers to information that when properly analyzed and processed would provide intelligence that commanders would use to take immediate offensive or defensive actions. Actionable intelligence is the type of information that a commander cannot ignore.

flow of incoming information. Analysts will also provide critical work by identifying intelligence gaps and in helping to provide feedback to the CCIRM process in order to influence the direction provided to collectors. Intelligence products are fashioned during this phase of the cycle in the form of written intelligence reports, graphics or presentations.

The final part of the intelligence cycle is *dissemination*. This phase's main *raison d'être* is to close the loop of the cycle by providing reports in different forms to the decision makers and other users. It is defined in the Canadian Forces Joint Intelligence Manual as "the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it."[40] Proper dissemination is often a difficult task to accomplish. It requires a robust information management (IM) capability in order to send the intelligence to the proper addresses in a timely fashion. These reports are useless if they cannot make it to the right users at the right time. This aspect of the intelligence cycle has also an important influence in the processing phase since it will sometimes require products to be distributed before the analysis is completed due to time sensitivities. This is particularly important in the COIN environment such as Afghanistan when intelligence on imminent attacks becomes available.

Any intelligence or unprocessed information that has the potential to have an impact on the safety of the troops will normally be disseminated with limited or no further analysis conducted.[41] In one particular case in 2006, Canadian soldiers were

---

[40] Canadian Forces Publications, *Joint Intelligence Manual- B-GL-005-200-FP-000*. (November 6, 2002): 2-12.

[41] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

taking a break and eating a meal in a fairly uncovered hide while insurgents started to assemble in order to mount a direct assault on the resting troops. The Canadians had taken off their protective gear including their anti-fragmentation vest and ballistic plates[42] and were most vulnerable to a direct attack. Insurgents were about to conduct a surprise attack on Canadian elements using rocket-propelled grenades (RPGs), mortar and small arms. Canadian intelligence personnel quickly radioed a report to the troops about this imminent threat which allowed them the time to prepare and repel the attack with minimal damages.[43] In this case, the timeliness of the intelligence was more important than the overall evaluation of the information and a more in-depth analysis conducted by intelligence staff. This example demonstrates the importance of disseminating intelligence expeditiously.

This chapter has introduced a thorough analysis of the available literature on the topic of intelligence sharing within coalition operations highlighting the very limited quantity of articles, papers and books published on the subject. Moreover, it has presented an exhaustive theoretical framework on the intelligence function in order to set the stage for the follow-on chapters. The next chapter will now focus on defining COIN operations within the Afghan context.

---

[42] This is probably the most important piece of protection that the soldier wears in a combat zone with his Kevlar helmet. Two ballistic plates made of bullet proof material are inserted in the anti fragmentation vest in order to provide soldiers protection against direct fire (up to 7.62mm calibre) and fragmentation from near by explosion. This vest weights approximately 25 pounds. A tactical vest is added on top of the frag vest in order to able the soldiers to carry magazines of ammunition, grenades and first aid kits. The tactical vest could easily weight an additional 15 pounds. Soldiers would ordinarily take off their vest in order to relax when they assess that they were in a secure area.

[43] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

CHAPTER 2 – THE AFGHAN CONTEXT

Before identifying problems areas and possible solutions to the coalition intelligence sharing mechanisms in Afghanistan, it is critical to understand the Afghan context as a whole. This framework is characterized by the following criteria's: insurgency and counterinsurgency as well as coalition warfare.[44] This chapter will define these terms in some detail in order to provide a solid understanding of the background before focusing more on the associated intelligence issues.

DEFINING INSURGENCY

Insurgency has existed throughout history as a subset of warfare but its strategic importance has recently increased drastically for those countries taking part in coalition operations in Afghanistan.[45] There is often confusion when the time comes to define the phenomenon of insurgency as it is often mixed and compared with the terms terrorism and guerilla warfare. The U.S. Counterinsurgency Field Manual differentiates between these terms by characterizing the terms terrorism and guerilla as tactics used by insurgents to achieve their goals.[46]

---

[44] Colonel George K. Gramer Jr "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College*, (17 May 1999): 1 and Gaétan Thibault, Lieutenant-Colonel M. Gareau and François Le May "Intelligence collation in asymmetric conflict: A Canadian armed forces perspective" *System of Systems Section, Defence R&D Canada Valcartier, Canada*, (July 2007): 1-2 & Steven Metz and Raymond Millen "Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response" *U.S. Army War College - Strategic Studies Institute*, (November 2004): 1.

[45] U.S. Department of the Army and U.S. Department of the Navy. *The U.S. Army and Marine Corps Counterinsurgency Field Manual* – U.S. Army FM-3-24 – Marine Corps Warfighting Publication No.3-33.5, (Chicago: The University of Chicago Press, 2007): 3.

[46] *Ibid.*, li.

A number of definitions exist for the term insurgency. Even though none has been universally agreed upon, most definitions include the following elements: violence, or the threat of violence, intimidation, propaganda and political aim.

One of the most imminent writers on the subject, David Galula describes insurgency as:

> …a protracted struggle conducted methodically, step by step, in order to attain specific intermediate objectives leading finally to the overthrow of the existing order.[47]

Steven Metz and Raymond Millen define insurgency as "a strategy adopted by groups which cannot attain their political objectives through conventional means or by quick seizure of power."[48]

Governments and military organizations have also developed their own way of defining insurgency. The draft Canadian Army Counterinsurgency (COIN) Doctrine dated July 2007 defines insurgency as: "A competition involving at least one non-state movement using means that include violence against an established authority to achieve political change."[49] According to the new Canadian COIN doctrine, the key to any insurgency is gaining at the very least an indifferent attitude, if not the outright support, of the population. Consequently, many insurgencies have sought to persuade through

---

[47] David, Galula. *Counter-Insurgency warfare: Theory and Practice*. (New York: Frederick A. Praeger, 1964), 4.

[48] Steven Metz and Raymond Millen "Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response" *U.S. Army War College - Strategic Studies Institute*, (November 2004): 2.

[49] B-GL-323-004/FP-003 Counter-Insurgency Operations, Ch 1, 2.

subversion, propaganda, intimidation, violence, large sectors of a population in order to gain support for those countering the insurgency.[50]

Janice Gross Stein and Eugene Lang describe the actions of insurgents.

> Insurgents will also challenge weak governments, or authoritarian governments, or governments dominated by a rival tribe or ethnic group. – They will in other words, escalate at the bottom. Insurgents will wage low-intensity warfare against governments and their armies over long period of time, with patience, determination, and endurance, over and over in the coming decades.[51]

In *The Art of Counter-Revolutionary War*, John McCuen argues that insurgents are involved in basic phases of revolutionary warfare that stem from organization, terrorism, guerilla warfare and mobile warfare.[52] In Afghanistan, most experts agree that the insurgents have been engaged in irregular warfare[53] using asymmetric[54] methods against the armed forces of the established Afghan regime and of the coalition forces. In other words, the Afghan insurgents continue to be involved, sometimes simultaneously, in the four basic phases of an insurgency as described by McCuen.

---

[50] *Ibid*., 2-3.

[51] Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Viking Canada, 2007), 211.

[52] John McCuen, The Art of Counter-Revolutionary War: A Psycho-Politico-Military Strategy of Counter-Insurgency. (Harrisburg: Stackpole Books, 1965), 40.

[53] Irregular warfare is defined as the type of conflict in which irregular forces (non-military) such as insurgents are engaged into. They include the use of non-conventional and asymmetric methods in order to avoid large scale combat and focuses mainly on low level hit and run tactics.

[54] The term asymmetric in this context makes reference to the type of tactics used by insurgents against coalition and government forces in Afghanistan. Insurgents do not attack military forces head on in order to annihilate one's military forces but focuses its weakest points and clearly identified centres of gravity. Asymmetric methods include the use of suicide attacks, improvised explosive devices (IED), indirect attacks using mortar and rockets, kidnapping and small scale ambushes.

DEFINING COUNTERINSURGENCY

Counterinsurgency seems to be an easier term to define than insurgency since it is a reaction to the first phenomenon. The NATO definition has been extensively used in official government publications such as the draft Canadian Army COIN doctrine which uses the definition *verbatim*. It is defined as: "Those military, paramilitary, political, economic, psychological and civic actions taken to defeat an insurgency."[55] Insurgents in Afghanistan have been difficult enemies to fight, especially for conventional armies that have trained over the past decades to fight wars of manoeuvre, employing firepower to suppress and attrit a conventional enemy.[56] James Howcroft noted that:

> What is clear is that strategic success is not the result of the destruction or capture of a single objective or individual. Capturing and killing Saddam, killing his sons, or killing Abu al-Zarqawi have not led to victory in Iraq. Capturing Osama bin Laden will not end the war on terror or result in victory in Afghanistan.[57]

Unconventional methods such as guerilla tactics, suicide attacks and terrorist acts combined with an unclear chain of command and the systematic use of cellular networks make counterinsurgencies that much more difficult to fight and win than any other conventional enemy in a complex coalition setting.[58] Foreign military forces engaged in COIN operations depend heavily on local leaders for intelligence, interpretation and for advice since they themselves cannot easily distinguish between friend or foe.[59] For the

---

[55] NATO, *Allied Administrative Publication (AAP) - 6 NATO Glossary of Terms and Definitions*, 2-C12.

[56] David, Galula. *Counter-Insurgency warfare: Theory and Practice*. (New York: Frederick A. Praeger, 1964), 71.

[57] James R. Howcroft, "Technology, Intelligence and Trust" *Joint Forces Quarterly*, Issue 46 (2007): 22.

[58] Leroy Thompson, *The Counterinsurgency Manual*. (London: Greenhill Books, 2002), 22.

purpose of this dissertation, counterinsurgency forces will include Afghan security and defense forces as well as coalition forces. After defining the terms insurgency and counterinsurgency in some detail, the following section will now focus specifically on the current Afghan insurgency.

THE CURRENT AFGHAN INSURGENCY

The current Afghan insurgency began following the overthrow of the Taliban regime in late 2001 and the establishment of a new interim government in 2002. Seth Jones believes that the collapse of governance following the overthrow of the Taliban is the most important pre-condition supporting the current insurgency[60]. It has involved a myriad of distinct groups including elements of the Taliban, Al Qaeda, Hezb-i-Islami, the Haqqani network, foreign fighters, various tribes as well as criminals associations.[61] Insurgents have employed the full range of irregular warfare, guerrilla and terrorist tactics to their advantage including ambushes, kidnappings, improvised explosive devices (IED), rocket, mortar and suicide attacks.[62] According to RAND statistics, insurgent-initiated attacks have augmented by about 400 percent from 2002 to 2006 and the number of deaths by about 800 percent over the same period.[63] Galula's observation on the behavior of insurgents, even if they have been written over 40 years ago, highlights some of the challenges of conducting efficient counterinsurgency operations in Afghanistan:

---

[59] Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Viking Canada, 2007), 213.

[60] Seth Jones, "The Rise of Afghanistan's Insurgency: State failure and Jihad" *International Journal*, Vol. 32, No 4 (Spring 2008), 8.

[61] Seth Jones, *Counterinsurgency in Afghanistan*. (Santa Monica, CA: RAND Corporation, 2008), 37.

[62] *Ibid*., 51.

[63] *Ibid*., 48.

"The trouble here is that the enemy holds no territory and refuses to fight for it. He is everywhere and nowhere."[64]

In their article entitled *Insurgency and Counterinsurgency in the 21st Century*, Metz and Millen differentiate between two forms of insurgencies: "national and liberation". In national insurgencies the primary antagonists are the insurgents and a national government while in liberation insurgencies, the goal of the insurgents is to liberate their nation from alien occupation.[65] The current insurgency in Afghanistan is characterized by both forms as it is not easy or always feasible to make a clear distinction between the two. In his article entitled *Counterinsurgency Redux*, David Kilcullen notes that there are multiple reasons that motivate insurgents to engage in an insurgency. The contemporary form of insurgency or the classical type sees an insurgent challenging the status quo of a functioning state. "Classical theory describes insurgent movement as seeking control of the state, or portion of it."[66] This applies not only to the wars of national liberation such has the de-colonization period of the 1950s, 1960s and 1970s but also to modern insurgencies such as the ones witnessed in Colombia, Thailand and Sri Lanka.[67]

Nonetheless, the intent to replace an existing government is not always as clear as depicted by the situation in Afghanistan. In this particular case, the insurgents seem to be

---

[64] David, Galula. *Counter-Insurgency warfare: Theory and Practice*. (New York: Frederick A. Praeger, 1964), 72.

[65] Steven Metz and Raymond Millen "Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response" *U.S. Army War College - Strategic Studies Institute*, (November 2004): 3.

[66] David Kilcullen,"Counterinsurgency *Redux*" *Small War Journal*, (July 2005): 4.

[67] Robert, Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*. (London: Chatto and Windus, 1966), 20.

more interested in paralyzing, discrediting and fragmenting the state than to taking control of all or portions of it.[68]

A myriad of issues make the Afghan insurgency a complex one to handle for coalition forces. The diversity of motivations behind the roots of the insurgency, the importance of the drug trade in the Afghan economic context as well as the existence of insurgents' safe heavens in Pakistan all contribute to the complexity of the situation. Afghan security elements and coalition forces have been actively engaged against the insurgents in a COIN type campaign to various degrees throughout the country. Some sectors have been stabilized while others, particularly the ones in the south and the east remain volatile. The insurgency has also been worsening over the past years, in particular since 2006. The Head of U.S. Central Command, General David Petraeus, noted in April 2009 that the insurgents' numbers were growing and that more coalition troops were required in order to succeed with the COIN campaign.[69] He also added that for the current COIN campaign to be successful, Afghanistan and Pakistan had to be viewed as a single theatre of operation.[70] The following section will now discuss the basics of coalition warfare and its application to the Afghan insurgency.

DEFINING COALITION WARFARE IN AFGANISTAN

> There is only one thing worse than fighting with allies; and that is fighting without them.[71]
>
> Sir Winston Churchill

---

[68] *Ibid*., 4.

[69] Bumiller, Elisabeth. "Petraeus Warns About Militants' Threat to Pakistan" New York Times (1 April 2009) http://www.nytimes.com/2009/04/02/washington/02military.html. Consulted on 12 April 2009.

[70] *Ibid*

[71] Sir Winston Churchill, quoted in Robert Maginnis "ABCA: A Petri Dish for Multinational Interoperability" *Joint Forces Quarterly*, Issue 37 (2005): 57.

Coalition, in the military context, is defined in the Oxford dictionary as: "a temporary alliance for combined action."[72] This definition clearly depicts the current military coalition in Afghanistan in which traditional and non-traditional allies have aligned in order to fight for a common objective. The temporary nature of these associations presents important challenges with regards to the level of interoperability throughout all of the military functions (operations, intelligence, communications, logistics, etc). It is also what makes them different from an alliance which is based on treaties or agreements which benefit the signatories. Elizabeth Sherwood-Randall adds that: "It is important to contrast an alliance with the "coalition of the willing". The two are entirely different organisms with respect to the durability of the commitment and the breath of cooperation."[73] Alliances have a more permanent character which allows for the development of common doctrine, protocols and procedures among the members. In his book *Questions d'intelligence*, Bruno Lamotte adds that:

> … force est de constater que les solidarités automatiques ont volées en éclats, remplacées par des accords conjoncturels, jetables, désormais fonction des préoccupations immédiates ou le mercantile prend souvent le pas sur le politique.[74]

The importance of coalitions lies mainly in their capacity to legitimize offensive military interventions and specifically the use of force against state or non-state entities.[75] Coalitions are also formed to allow for military operations to take place by providing

---

[72] R.E. Allen, "*The Concise Oxford Dictionary of Current English*". (Oxford: Oxford University Press, 1990), 215.

[73] Elisabeth Sherwood-Randall "The Case for Alliances" *Joint Forces Quarterly*, Issue 43 (2006): 55.

[74] Bruno Delamotte. Questions d'intelligence: le renseignement face au terrorisme. (Paris: Éditions Michalon, 2004), 11.

[75] Robert Ricassi "Principles for Coalition Warfare" *Joint Forces Quarterly*, Issue 1 (1993): 59.

specific military capabilities and/or access to geographic locations essential to the success of military operations. For example, Pakistan and other Gulf states are active members of the "coalition of the willing" for Afghanistan even if they don't have any troops deployed in country.[76] The access to their ports, airports, airspace or intelligence sharing agreement is considered to be their contribution to the coalition's efforts.

Since "war is not a mere act of policy but a true political instrument, a continuation of political activity by other means",[77] the creation of a military coalition for Afghanistan has allowed the U.S. to rely on the political and military assistance of many countries. A few weeks after the attacks against the United States in September 2001, Operation Enduring Freedom received the support of over 75 countries and important multinational organizations such as the European Union, NATO and the Gulf Cooperation Council.[78] UN Resolution 1368, adopted on 20 Dec 2001, authorized the establishment of the International Security Assistance Force (ISAF) and called for the support of member states to participate in this mission.[79] This UN mandate coupled with the participation of a large number of countries contributed to the legitimization of the military intervention in Afghanistan in the public eye. Coalitions are therefore always sensitive to public opinion since it will have a direct and important impact on its level of legitimacy. Moreover, an internationally supported coalition, especially the one fighting

---

[76] David Gerleman and Jennifer E. Stevens "Operation Enduring Freedom: Foreign Pledges of Military & Intelligence Support" *Report to the Congress*, (17 October 2001): 4, 7-8.

[77] Carl von Clausewitz, quoted in John Graham de Jones "*On War. Carl Von Clausewitz*" (New York: Barnes and Nobles Publishing, 2004), XV.

[78] David Gerleman and Jennifer E. Stevens "Operation Enduring Freedom: Foreign Pledges of Military & Intelligence Support" *Report to the Congress*, (17 October 2001): 1-10 & Martin Rudner "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism" *International Journal of Intelligence and CounterIntelligence*, Vol 17 (2004):196.

[79] UN Security Council Resolution 1386 (2001).

under the NATO and UN flag, are more politically acceptable even for the warring factions, both in intra-state and extra-state conflicts.[80]

In the post 9/11 era, one could argue that the United States, the only remaining superpower, had the military capacity required to engage in combat operations in Afghanistan without the support of any other military forces. However, in the United States, coalition operations are widely viewed as an essential method of conducting military operations today and in the future. Former U.S. Army Chief of Staff, General Eric Shinseki stated quite clearly that: "The coalition framework remains the essential framework for the application of military force."[81] However, the employment of military forces in a multinational coalition setting brings a myriad of military and political background that adds to the normal friction and complexity of conducting multinational operations. This requires modern military forces to develop agile and flexible elements in order to allow for a high level of interoperability among the coalition partners. Former British Army Chief, General Sir Roger Wheeler adds that: "There is simply no point, in my view, in developing battle-winning capabilities at the national level if it's muted through lack of interoperability in coalition."[82]

Long standing multinational organizations such as ABCA (for armies of America, Britain, Canada and Australia, with New Zealand as an associate member) have been formed in the post Second World War era in order to address mutual security concerns

---

[80] Colonel Paul de B. Taillon "Some of the Challenges of Multinational Force Command" *New Zealand Journal of Defence Studies*, Vol 1 (March 2007): 23.

[81] Robert Maginnis "ABCA: A Petri Dish for Multinational Interoperability" *Joint Forces Quarterly*, Issue 37 (2005): 56.

[82] General Sir Roger Wheeler, quoted in Robert Maginnis "ABCA: A Petri Dish for Multinational Interoperability" *Joint Forces Quarterly*, Issue 37 (2005): 56.

and interoperability issues.[83] The ABCA Army program was formed from the experiences of the Second World War and the security relationship between the United States and its Anglo-Saxon allies based on a common culture, historical experience and language.[84] The current ABCA mission statement is: "optimize interoperability through cooperation and collaboration in the continuous pursuit of standardization and mutual understanding in order to integrate the capabilities of the ABCA Armies in coalition operations."[85]

The fact that every coalition is developed on an ad hoc basis increases the level of difficulty of thoroughly integrating them into an efficient coalition.[86] With key differences in doctrine, language and culture comes increased risks based on poor communication and disorganization that can easily result in fratricide. Robert Riscassi emphasized the fact that there is no cookbook approach to coalition warfare. Every coalition has a different purpose, character, composition and scope which makes it that more difficult to create a universally accepted model.[87] He adds that the secret for success is based on method and not on personalities of commanders.

According to Riscassi, the key to successful coalition warfare is the development and use of a common doctrine, the agreement on a strategic campaign plan, the use of a common operating planning process, the integration of forces, the unity of command,

---

[83] General Richard A. Cody and Robert Maginnis "Coalition Interoperability: ABCA's New Focus" *Military Review*, (November-December 2006): 65.

[84] *Ibid*., 65.

[85] ABCA Web Site, http://www.abca-armies.org

[86] Robert Ricassi "Principles for Coalition Warfare" *Joint Forces Quarterly*, Issue 1 (1993): 59.

[87] *Ibid*., 59.

pre-deployment training, applying a common Command, Control, Communications, Computers and Intelligence (C4I) architecture and using mutual and supportive logistical support channels.[88] Recent articles published by Robert Maginnis, General Richard A. Cody and Elizabeth Sherwood-Randall indicate that the United States military is seriously considering all of the aspects of current and future coalition warfare.[89] Due to being the only real world power albeit with China, India and Russia closing in, the United States is the natural leading nation to put together effective military coalitions. It is also clearly in its interest to take the lead on these important issues.

Coalition effectiveness, morale and cohesion will often depend on some form of sharing of the burdens, of the risks and of the credit.[90] NATO is currently facing serious difficulties in convincing its members to pledge more troops in the most dangerous sectors of Afghanistan where skirmishes with Taliban and Al Qaeda occur on a daily basis. ISAF forces, who are for the most part NATO members (26 out of a total of 38), operate out of five regional commands. The bulk of the fighting and the higher level of risks for the troops take place in the southern and eastern sectors which are under the area of responsibility (AOR) of the American, British, Canadian and Dutch contingents. These countries and NATO senior leadership have been pledging to other NATO members to send more troops in those sectors in order to prevail against the continuing

---

[88] *Ibid*., 60-71.

[89] General Richard A. Cody and Robert Maginnis "Coalition Interoperability: ABCA's New Focus" Military Review, (November-December 2006): 65-68 & Elizabeth Sherwood-Randall "The Case for Alliances" Joint Forces Quarterly, Issue 43, (2006): 54-59.

[90] Robert Ricassi "Principles for Coalition Warfare" Joint Forces Quarterly, Issue 1 (1993): 59.

[90] *Ibid*., 71.

insurgency.[91] The US defense Secretary, Robert Gates has described the critical aspect of

the situation in a speech to the Conference of European Armies in July 2007:

> If an alliance of the world's greatest democracies cannot summon the will to get the job done in a mission that we agree is morally just and vital to our security, then our citizens may begin to question both the worth of the mission and the utility of the 60-year-old transatlantic security project itself.[92]

In sum, coalitions, like any other type of organization, are only as strong and efficient as their weakest elements. Insurgents are continuing to capitalize on this reality and are trying to take advantage of any weaknesses that may exist in the military coalition that they are facing: specifically cohesion and respective national and international public opinion.

SUMMARY

The current military operating environment (CMOE) represents a complex and demanding setting for coalition forces to be employed in. The challenges of conducting COIN operations, the volatility and diversity of the asymmetric threats and the inherent challenges of operating as part of a coalition have all had a direct impact on the conduct of modern military operations. This chapter has described the multifaceted environment in which coalition forces are asked to deploy and accomplish their missions. The non-permanent aspect of these organizations is a major obstacle to its efficiency and to the overall interoperability of its constituent members. Existing alliances such as NATO and ABCA have been able to take a leading role in recognizing this problem and by

---

[91] The author will provide more details and emphasis on the realities of coalition operations in Afghanistan in the following chapters. He has chosen to present some highlights of the main characteristics of the military coalition in order to introduce the reader to the situation in Afghanistan.

[92] Richard Norton-Taylor "Coalition of the unwilling" *The Guardian*. (7 November 2007) http://www.guardian.co.uk/afghanistan/comment/story/0,,2206425,00.html.

attempting to find ways to improve the current coalitions. The following chapter will focus on defining the important role played by the intelligence function in COIN operations.

CHAPTER 3 – THE INTELLIGENCE FUNCTION AND COALITION COIN OPERATIONS IN AFGHANISTAN

This chapter will now describe the intelligence apparatus in the Afghan COIN context. It will focus more specifically on the role of the intelligence function during COIN operations as well as on the ways that it has adapted to this type of warfare. This chapter will also define the role of intelligence organizations in the Afghan COIN environment with its associated challenges and opportunities. Finally, it will provide the reader with some examples of coalition intelligence sharing.

THE ROLE OF INTELLIGENCE IN COIN OPERATIONS

Most prominent writers on insurgency and counter-insurgency theories are adamant of the criticality of intelligence in the conduct of successful COIN operations. David Galula defines the role of intelligence as pivotal for the forces dealing with an insurgency and ads that intelligence collected from the local population will be of the highest value for COIN elements:

> Intelligence is the principal source of information on guerillas, and intelligence has to come from the population, but the population will not talk unless it feels safe, and it does not feel safe until the insurgent's power has been broken.[93]

Robert Thompson dedicates a whole chapter of his book *Defeating Communist Insurgency* to the intelligence function. He starts his chapter by quoting a newly arrived U.S. General in Viet Nam that, like many in those days, did not understand the value of intelligence in the COIN environment: "Let's go out and kill some Viet Cong, then we can worry about intelligence."[94] Robert Thompson adds that:

---

[93] David Galula. *Counter-Insurgency warfare: Theory and Practice*. (New York: Frederick A. Praeger, 1964), 72.

> Good intelligence leads to more frequent and rapid contacts. More contacts lead to more kill. These in turn lead to greater confidence in the population, resulting in better intelligence and still more contacts and kills. That, General, is why you should first worry about intelligence.[95]

He argues that a solid intelligence organization is paramount in order to defeat an insurgency and goes as far as saying that: "no government can hope to defeat a communist insurgent movement unless it gives top priority to, and is successful in, building in such an organization."[96] Thompson adds that the aim of the intelligence organization must be to identify insurgents, with the view of eliminating them or at least preventing them from carrying illegal acts against the security of the country.[97] "As intelligence builds up, more effective operations can be planned."[98] Like Galula, Thompson agrees that the best intelligence on the insurgents will come from the local population: "Apart from information provided by agents and ordinary members of the population, the two main sources of intelligence are captured documents and surrendered or captured enemy personnel."[99]

John McCuen describes to role of the intelligence apparatus as follow:

> The governing authorities must be able to recognize the difference between revolutionary and non-revolutionary political movements. They must know what the revolutionaries are doing. They must ensure that security forces have time to react. They must know where, when, and how to attack. They must know where, when, and how to defend.[100]

---

[94] Robert Thompson. Defeating Communist Insurgency: The Lessons of Malaya and Vietnam. (London: Chatto and Windus, 1966), 84.

[95] *Ibid*., 88.

[96] *Ibid*., 84.

[97] *Ibid*., 84.

[98] *Ibid*., 88.

[99] *Ibid*., 86.

He believes that the governing authorities must organize their intelligence networks clandestinely deep into the population.[101] McCuen recognizes some of the difficulties of organizing an effective intelligence apparatus considering the numerous governing security and defense bodies involved in the business of intelligence. He mentions that even though intelligence must be reported though the appropriate chain of commands that it is imperative that sharing mechanisms are in place so that it can be evaluated, interpreted and exchanged with other agencies at each administrative levels.[102]

According to John McCuen, the British displayed the proper way to use intelligence in a COIN setting under the leadership of General Sir Gerald Templer, who was appointed as Malayan High Commissioner in 1952. One of Templer's top priorities was to re-organize the existing intelligence system.[103] His solution was to integrate all types of intelligence under a Combined Intelligence Staff in order to produce intelligence that was tailored to the users. Within a few years, the intelligence authorities had identified all of the active insurgents which lead McCuen to say that "intelligence finally achieved its rightful place as a principal counter-revolutionary war weapon."[104]

It is important to note that there are a few writers, like John Keegan, that believe that intelligence do not play such a pivotal role in enabling military operations. He

---

[100] John McCuen. *The Art of Counter-Revolutionary War: A Psycho-Politico-Military Strategy of Counter-Insurgency*. (Harrisburg: Stackpole Books, 1965), 113.

[101] *Ibid*, 114.

[102] *Ibid*,, 115.

[103] *Ibid*., 118.

[104] *Ibid*., 119.

believes that the ability to use force remains, even without proper intelligence, the best way to counter any type of threats. Keegan adds that:

> Foreknowledge is no protection against disaster. Even real-time intelligence is never real enough. Only force finally counts…The ability to strike sure will remain the best protection against the cloud of unknowing, prejudice and ignorance that threatens the laws of enlightenment.[105]

Keegan's position may seem very different from the other point of view presented earlier but does still represent the position of some of the more conservative hard-core intellectuals and military officers. This perspective is often associated with maneuver warfare and the advance to contact concept. Moreover, this approach is sometimes a reflection of the intelligence versus operations' approaches to a problem where some operations officers go as far as saying that "intelligence is too important to be left to intelligence officers."[106] Napoleon's own words also seem to support this approach to warfare when he said that "*On s'engage, et alors on voit* (You engage and then you wait and see)."[107] The difficulties with this approach in a COIN context like Afghanistan is that the risks of casualties strongly outweighs any other benefits that operating blindly can procure. In Afghanistan, if you don't see before you engage, you risk of becoming a casualty dramatically increases.

Canadian and U.S. COIN doctrine strongly support the concept of intelligence driven operations. The Canadian COIN doctrine stipulates that good intelligence is vital to support any COIN campaign from the beginning to the end and that sound intelligence

---

[105] John Keegan, Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda. (Toronto: Key Porter Books, 2003), 399.

[106] Michael I. Handel, *Intelligence and Military Operations*. (Portland: Frank Cass, 1990), 21.

[107] *Ibid.*, 8.

supports continuing success that over time will wear down the insurgent movement.[108] The U.S. COIN doctrine categorizes the role of intelligence similarly to the Canadian version of COIN doctrine. COIN is an intelligence-driven endeavor…in COIN operations, the ultimate success or failure of the mission depends on the effectiveness of the intelligence effort.[109] Without good intelligence, a counterinsurgent is like a blind boxer wasting energy flailing at an unseen opponent.[110] This section of this dissertation has demonstrated that intelligence is viewed by most experts on COIN as a critical element to the success of such operations. The following section will now describe the way that the coalition intelligence system is organized in Afghanistan.

TRANSPOSING COIN THEORIES TO INTELLIGENCE ORGANIZATIONS IN AFGHANISTAN

Operations in Afghanistan, defined by the "Three Block" warfare concept[111] (also commonly known as full spectrum operations) calls for military forces to be involved simultaneously in a myriad of tasks such as Humanitarian Assistance (HA), Peace Support/Framework Operations (PSO) and Direct Action (DA). Modern military intelligence organizations must demonstrate a high level of flexibility and adaptability in order to satisfy the commander's intelligence requirements in the "Three Block" warfare

---

[108] B-GL-323-004/FP-003, Counter-Insurgency Operations, July 2007, 7-1.

[109] U.S. Department of the Army and U.S. Department of the Navy. The U.S. Army and Marine Corps Counterinsurgency Field Manual – U.S. Army FM-3-24 – Marine Corps Warfighting Publication No.3-33.5. Chicago: The University of Chicago Press, 2007, 79.

[110] Eliot Cohen, LCol Conrad Crane, LCol Jan Horvath and LCol John Nagl "Principles, Imperatives and, Paradoxes of Counterinsurgency" *Military Review* (March-April 2006): 50.

[111] After operations in Somalia, General Charles Krulak, Commandant of the Marines Corps, spoke of future conflicts and stated it would not imitate the sweeping armoured manoeuvre of Desert Storm, but resemble the chaos of Somalia and Chechnya. He labelled these conflicts 'Three Block wars.' They consist of three major operations occurring simultaneously within an urban environment: humanitarian assistance, peace operations and combat operations. (see General Charles C. Krulak "The Strategic Corporal: Leadership in the Three Block War" *Marines Magazine,* (January 1999)).

context. Military intelligence organizations in Afghanistan are required to support a multitude of diverse tasks such as studying the impact of flooding on military operations, providing focus for civil-military projects, assisting law enforcement in drug interdiction operations, providing information during hostage-taking situations, hunting down High Value Targets (HVTs)[112] and targeting insurgents.[113]

In addition, the conditions of the post 9/11 era led respective national intelligence organizations, civilian and military, to break down traditional organizational barriers and to share as much information as possible within the overall intelligence community (IC). This drastic shift in mindset is often referred to as the old intelligence system of "*need to know*" being replaced by a new system of "*need to share*" or "*responsibility to provide*".[114]

The new "*need to share*" viewpoint means that intelligence professionals have to write reports with a "write for release" mindset.[115] It sometimes means that intelligence analysts have to produce different versions of the same report using techniques such as a tear line process. This consists of removing the more sensitive data from a report in order to avoid exposing sensitive collection capabilities/techniques or ongoing operations.[116]

---

[112] HVT refers to a target of high importance in the ability to wage war, and therefore a primary objective of offensive and defensive operations. In the Afghan context, HVTs likely include senior Taliban and Al Qaeda commanders.

[113] Lieutenant General Eikenberry, Commanding General Combined Forces Command – Afghanistan, *Defense Department News Briefing*, Washington Post, (21 September 2006).

[114] Final Report of the National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, Executive Summary, & Lieutenant-Colonel G. Jensen CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006.

[115] Lieutenant-Colonel H. Ferguson CD, J2 International CDI, *Interview*, 30 January 2007.

This often results in more time spent on packaging and disseminating intelligence products and less time spent on other important activities of the intelligence cycle such as all source analysis and managing the collection plan.[117]

With coalition operations comes the challenge of effective intelligence sharing among the partners. Important technical advances have been made in recent years and classified IT systems and networks are now in place. The most common networks are NATO's Multi-National Battlefield Information Collection Exploitation System (BICES) and Linked Ops-Intel Centers Europe (LOCE) currently supporting ISAF, SFOR, OEF and KFOR.[118] The US Combined Enterprise Regional Information Exchange System (CENTRIXS) provides the US and its coalition partners, many of which are non-NATO countries, with a classified network to share intelligence and coordinate operations in Afghanistan.[119] These systems are a step in the right direction but they are only as effective as the quality and quantity of the information populating them.

Military intelligence organizations have been clearly identified as a critical contributor to COIN operations in Afghanistan and have increasingly been praised for the importance of their work by commanders in the field.[120] The complexity and magnitude

---

[116] Confidential source 001, Canadian Forces Information Operations Group, Interview, 24 April 2006.

[117] Master Warrant Officer M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[118] Confidential source 001, Canadian Forces Information Operations Group, Interview, 24 April 2006.

[119] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

[120] Colonel, W. Semianiw OMM CD, former Commander Task Force Kabul, OP ATHENA Roto 3 (February 2005-August 2005), *Interview*, 3 March 05 & Major-General A.B. Leslie CMM MSC MSM

of the threats faced in Afghanistan compared to previous expeditionary/peacekeeping operations have forced Western militaries to re-examine the way they do business. COIN operations in Afghanistan have dramatically increased the burden on the intelligence units responsible for supporting military forces waging a non-conventional war while facing a complex, dangerous and unpredictable enemy. The intelligence organizations required to support military forces in these non-conventional theatres have become more sophisticated, complex and innovative. Bruno Delamotte goes as far as saying that Afghanistan has become the first War of Intelligence:

> Ce qui était perçu comme un conflit asymétrique, du fou au fort, maîtrisable à moyen terme par une adaptation rapide de notre posture militaire, est en fait sans doute la première "guerre de l'intelligence". Une guerre sans champs de bataille clairement défini, ou plutôt doté d'un champ de bataille planétaire.[121]

Templates/doctrinal models that could be used to predict how adversary forces would react do not exist in today's modern COIN operations as they did during most of the Cold War period. The unpredictability of the threat has also seen tactical commanders relying a lot more on their intelligence staff's advice in order to conduct effective and safer operations. The idiosyncratic[122] connotation of the threats faced abroad has contributed to highlight the importance of intelligence in the eyes of military commanders. Military operations, and in particular COIN operations, have become more and more intelligence driven.

CD, former Deputy Commander International Security Assistance Force – Kabul, Afghanistan (August 2003- February 2004), *Interview*, 27 April 2006.

[121] Bruno Delamotte. *Questions d'intelligence: le renseignement face au terrorisme.* (Paris: Éditions Michalon, 2004), 62.

[122] In military sense, idiosyncrasy connotes an unorthodox approach or means of applying a capability, one that does not follow the rules and is peculiar in a sinister sense (see Montgomery C. Meigs "Unorthodox Thoughts about Asymmetric Warfare" *Parameters*, (Summer 2003): 4.

Military commanders in Afghanistan are continuously challenged by the intelligence problems they have to overcome in order to achieve mission success. Their intelligence staffs do not have access to templates describing what the insurgents are expected to do or the doctrine and tactics that they are expected to follow. As noted by General Montgomery C. Meigs (Ret) "Templating and predicting the actions of cellular terrorist networks that constantly change and reform from fragments of the old structure becomes a shot in the dark."[123] More than ever, military commanders rely on their intelligence staff analysis and advice to conduct and indeed drive successful military operations in the COIN context presented in Afghanistan.

Furthermore, military commanders often have to conduct "intelligence operations" first in order to develop the actionable intelligence required for the conduct of effects-based operations. Lt General William G. Boykin, former US Deputy Undersecretary of Defense for Intelligence, expressed this reality in very simple terms: "If you want 'Actionable Intelligence', you must take 'Action' first."[124] Canadian Forces elements have conducted major intelligence operations in Afghanistan in late 2007 were battalion and company size manoeuvre elements from the Royal 22^{e} Régiment deployed in hostile territory in order to gain precious intelligence on Taliban elements.[125] Some of these operations were designed to make the insurgents react to coalition troop movement

---

[123] General Montgomery C. Meigs "Unorthodox Thoughts about Asymmetric Warfare", *Parameters*, (Summer 2003): 11.

[124] Lieutenant General William G. Boykin, *Presentation to the 16th Annual SO/LIC Symposium – Strategic Environment for Coalition Warfare*, (3 February 2005).

[125] Canadian Special Operations Command, Confidential Source 009, *Interview*, 26 February 2008.

allowing for cued coalition intelligence organizations to collect invaluable information that would later be used in their favor.[126]

OVERVIEW OF THE MILITARY INTELLIGENCE APPARATUS IN AFGHANISTAN

Coalition forces operating in Afghanistan currently fight as elements of the International Security Assistance Force (ISAF) with the exception of some specialized military elements (mainly SOF)[127] that remain employed by the U.S. Central Command (CENTCOM) under Operation Enduring Freedom (OEF). The backbone of ISAF is based on twenty six (26) NATO countries and twelve (12) others. The non-NATO countries are Albania, Australia, Austria, Azerbaijan, Croatia, Finland, Former Yugoslav Republic of Macedonia, Georgia, Ireland, New Zealand, Sweden and Switzerland.[128]

The senior intelligence officer (J2) for ISAF Headquarter (HQ) is based in Kabul. The ISAF J2 has a truly multinational staff with some limited integral collection capabilities that have been offered to ISAF by some of the contributing nations. HUMINT, CI, Reconnaissance and limited SIGINT capabilities have been at the disposal of the J2 for at least the past three years.[129] Similar to NATO, ISAF depends on the intelligence that every contributing nation is prepared to share with other coalition partners. As a general rule of thumb, every nation agrees that it will share its intelligence

---

[126] *Ibid*.

[127] Some Special Operations Forces are employed in more sensitive operations that require more secretive measures and constant availability of national resources (Intelligence, Surveillance and Reconnaissance (ISR) and mobility) that could not be guaranteed in a multinational organization such as ISAF.

[128] ISAF official Web Page, www.nato.int/isaf

[129] Lieutenant-Colonel G. Eanes USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005 & Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

when there is the likelihood that it could have a direct impact on the safety/security of the ISAF troops or if the lack of it risks compromising the overall mission.[130] However, the overall flow of intelligence is far from being perfect as it is common knowledge that most contributing nations do not make all of their collection capabilities available to ISAF as a whole.[131] Intelligence on force protection is shared openly while intelligence on target development in support of offensive operations is not often readily available.[132] Newly accepted NATO members, mainly countries from Eastern Europe, have been very forthcoming in providing collection assets such as HUMINT teams.[133] Many coalition intelligence officers interviewed during this research believed that this may have been motivated by their intentions to make a good impression on NATO as new members.[134] Their attitude contrasted with that of long-established NATO members that have remained less open to the idea of dedicating their collection assets to ISAF.

Subordinate to ISAF HQ are five Regional Commands (RC) covering the north, east, south, west and centre of the country with their own multinational intelligence apparatus. These multinational intelligence organizations are elements of Divisional HQs

---

[130] Captain J. Callacott, CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

[131] National regulations preclude some intelligence collected by sensitive technical means from being available to all ISAF participating nations. Intelligence sharing agreements are often based on bilateral agreements among nations and have little to do with ISAF. It is common knowledge that most ISAF nations have undeclared intelligence assets in Afghanistan that provide national-level intelligence to the various national commanders on the ground.

[132] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

[133] Canadian Special Operations Command, Confidential Source 007, *Interview*, 31 October 2007.

[134] Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 2 November 2007 & Major, D. Zegarac Deputy Chief Assessments, International Security Assistance Force Kabul Afghanistan, *Interview*, 20 November 2007.

and are based on the continental staff model (J2). This paper will focus on RC South based in Kandahar, where American, British, Canadian, Australian, Dutch, Danish and Romanian soldiers are engaged in COIN operations.

RC South intelligence organizations include a multinational J2 staff at the Divisional HQ based at Kandahar Airfield, a four eyes (Australia/Canada/Great Britain/United States) fusion centre called the Kandahar Intelligence Fusion Center (KIFC), national all-source intelligence units and tactical level intelligence cells.[135] Since the beginning of coalition operations based out of Kandahar in late 2001, the intelligence architecture has rapidly evolved. In 2006, the handover of this volatile sector from OEF to ISAF required a major reshuffle of the intelligence apparatus. The pre-2006 period had, for the most part, American troops operating with some low-key participation from other coalition forces. Intelligence sharing challenges were not a priority since the vast majority of combat forces were American, allowing them to rely almost exclusively on U.S. only classified systems such as JWICS[136] and SIPRNet[137]. The arrival of large contingents from Canada, Britain and the Netherlands changed this dynamic, forcing a major overhaul in the information flow of the intelligence system.

The passage of intelligence remains a complex task in RC South. The Divisional HQ receives its intelligence from all of the coalition partners via systems such as CENTRIX or the ISAF LAN. The Divisional commander is normally briefed by his J2 at

---

[135] Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 2 November 2007.

[136] The Joint Worldwide Intelligence Communications Systems (JWICS) is the US Department of Defense and Department of State classified interconnected network capable of handling up to Top Secret and sensitive compartmented information (SCI) levels.

[137] The Secret Internet Protocol Router Network (SIPRNet) is similar to JWICS but can handle information up to Secret only.

the ISAF SECRET level, followed by a briefing at the four eyes level if he is part of that community. The commander is also served by his own national intelligence assets, which have the potential to brief him on national intelligence topics with details that cannot be shared with any other nation. This complex and potentially confusing situation forced the creation of the Kandahar Intelligence Fusion Centre (KIFC) in mid-2006. This four eyes intelligence organization is annexed to the RC South J2 staff building. It is responsible for releasing as much Australian, Canadian, British and American intelligence reporting as possible to other coalition partners in order to promote the development of a CIP and reduce the friction that is inherent to the conduct of coalition operations. The KIFC is also an intelligence processing centers that produces consolidated four eyes reports for the four eyes contingents deployed in Afghanistan.[138]

The overall coalition intelligence community in Afghanistan is more than just what has been discussed at the ISAF levels. It also includes civilian intelligence agencies, federal police forces interested in overseas criminal intelligence, Combined Joint Special Operations Task Force (CJSOTF), OEF tier one SOF[139] units and Afghan security organizations (Afghan National Army (ANA), Afghan National Police (ANP) and National Directorate of Security (NDS)). All of these elements play an active role in developing the intelligence picture but, as the next part of this chapter will demonstrate, they still have a long way to go with regards to systematically sharing intelligence.

---

[138] Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 2 November 2007.

[139] Tier one SOF units are the most highly trained SOF such as Delta, Seal Team Six, 22 SAS and JTF2. These units specialize in high risk missions like counter-terrorism and hostage rescue operations. The identity of tier one SOF units operating in Afghanistan remains classified.

EXAMPLES OF COALITION INTELLIGENCE SHARING IN AFGHANISTAN

Intelligence related to force protection is easier to make available to the largest possible audience because it is relatively simple to take away details and reduce the level of potentially compromising information. However, intelligence relating to target development and future offensive operations requires the maximum amount of details in order to properly support the planning process.[140] For example, the level of sensitivities of the sources and methods used by SOF Intelligence personnel would often preclude them from sharing the information with forces outside a very small community (circle of trust) in order to prevent compromise and maximize operational security (OPSEC). This also means that intelligence collected by the SOF community and the follow-on analysis would not automatically be available to conventional forces, even to the ones from the same nationality. Canadian Special Operations Command personnel also added that there existed circles within circles even within SOF forces and that it was based on credibility, capabilities and the establishment of trustworthy personal relationships.[141] This fact highlights that the intelligence sharing problem within a coalition environment remains complex and that it is not limited to inter-state relationships only. Barriers also exist within intelligence organizations from a same nation.

The presence of a large number of civilian intelligence agencies in Afghanistan and their ambiguous role has presented a legacy of unanswered questions to many military intelligence officers. Some of these agencies have been operating in support of

---

[140] Canadian Special Operations Command confidential source 006, *Interview*, 27 April 2006.

[141] *Ibid*.

the overall military coalition effort while others have been operating autonomously[142]. It is difficult to assess the level of openness of the civilian agencies towards their military counterparts without entering into the classified realm, but, it is fair to say that coordination with other military coalition partners could be improved significantly.[143]

On some occasions, intelligence reports from U.S. civilian agencies were made available to Canadian military intelligence organizations before they had reached some of their U.S. recipients.[144] The presence of Canadian Security Intelligence Service (CSIS) officers with the Canadian military facilitated the passage of those reports.[145] This fact highlights the importance of trust when the time comes to share intelligence. In this case, long-time established sharing mechanisms between two civilian security intelligence organizations expedited the passage of information. Notwithstanding, civilian intelligence agencies maintained a reasonably good relationship with national all-source intelligence organizations and SOF intelligence staff.

The danger of creating and encouraging different circles of trust is that this has the potential to seriously impede the development of a truly CIP. The absence of a CIP has led to problems in the conduct and coordination of operations and has increased the risk of fratricide among coalition partners. One of the measures taken by the coalition intelligence community in Afghanistan was to stress the importance of writing intelligence reports with the intention of releasing them to all coalition partners. This

---

[142] Canadian Security Intelligence Service Confidential source 004, *Interview*, 12 February 2005.

[143] *Ibid*.

[144] *Ibid*.

[145] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

was made difficult because many, within the coalition IC, believed that disseminating reports to the Global Coalition Task Force (GCTF), which included 66 countries (OEF, ISAF and countries such as Pakistan and U.A.E.), was the equivalent of publishing the information to everyone.[146] This resulted in intelligence reports often being deprived of important elements of information in order to protect the sources and methods of collection, and reports that were simply kept within existing circles of trusts.[147]

When ISAF took control of RC South in 2006, it recognized the importance of improving the intelligence sharing system in place.[148] Collaboration between the four eyes community[149] remained easy but the addition of an important contingent from the Netherlands increased the importance of developing new ways of making intelligence available to all involved. The four eyes community therefore stood up the KIFC with the mission of providing as much intelligence as possible to the non four eyes coalition partners. The KIFC has been a notable success in that has provided a new capability in the quest to attain the development of a CIP. The system is not perfect but it has allowed significant improvement in the way intelligence is shared in the Afghan theatre of operations.

---

[146] Canadian Special Operations Command confidential source 006, Interview, 27 April 2006.

[147] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005, Lieutenant-Colonel G. Jensen CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006 & Major-General A.B. Leslie CMM MSC MSM CD, former Deputy Commander International Security Assistance Force – Kabul, Afghanistan (August 2003- February 2004), *Interview*, 27 April 2006.

[148] Lieutenant-Colonel G. Jensen CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006 & Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 29 March 2007.

[149] Includes Australia, Canada, United Kingdom, United States.

Initiatives to improve intelligence sharing in Afghanistan continue to be at the forefront of coalition forces, Afghan and Pakistani preoccupations. Sharing intelligence among the coalition partners is as critical as been able to share it with Afghan and Pakistani security and intelligence agencies. The establishment of a Joint Intelligence Operations Center (JIOC) in Kabul on 25 January 2007 highlights this fact.[150] This new organization was designed to allow for a better exchange of intelligence between ISAF, Afghan and Pakistani authorities on border security related issues. It is currently manned by six Afghan, six Pakistani and twelve ISAF intelligence specialists with the responsibility to facilitate the passage of critical intelligence to the forces deployed at the border between Pakistan and Afghanistan.[151] The creation of the JIOC has been a true success in that it has opened permanent lines of communications between all parties thereby improving trust and directly contributing to intelligence-driven COIN operations.

SUMMARY

Military intelligence organizations have had to adapt and find ways to improve their methods and procedures in order to remain relevant in the eyes of the commanders. The unpredictability and lethality of the threats have clearly contributed to bring this function to the forefront of military operations conducted in Afghanistan. This chapter has highlighted the importance of the role of the intelligence function in places like Afghanistan. The participation of civilian intelligence agencies, even if they potentially do not share everything with their military counterparts, remains critical in order to leverage their capabilities and to improve the level of coordination in the theatre of

---

[150] Captain Stacie Shafran, "Joint Intelligence Operations Center opens in Kabul" Air Force Link (29 January 2007). http://www.af.mil/news/story.asp?id123039140 consulted 30 January 2009.

[151] *Ibid*.

operations. Coalition intelligence organizations rely strongly on their capabilities and their interoperability with other Task Force units, coalition partners and other government departments/agencies. The next logical step should be to transpose these national and multinational successes such as the KIFC and JIOC to intelligence collection organizations.

Furthermore, the establishment of effective intelligence sharing agreements among coalition partners will likely continue to face challenges in the future. Constant efforts by all coalition partners and a strong will to change old overprotective mindsets will be required in order to make significant progress in this area. The following chapter will take a closer look at the obstacles to a more efficient way to share intelligence within a coalition such as the one operating in Afghanistan.

CHAPTER 4 – IDENTIFYING THE HURDLES TO EFFECTIVE INTELLIGENCE SHARING IN AFGHANISTAN

> The fallout over U.S. intelligence support to coalition operations…is centered on the continued use of U.S.-only information systems, the lack of coalition dissemination architecture, under-utilization of commercial assets, and the impact that speed and success on the battlefield had with regard to the existing dissemination procedures.[152]

Previous chapters have provided the background information necessary to gain a better understanding of the field of military intelligence and on the impact of this very important function on coalition operations in Afghanistan. The aim of this chapter is to focus on the causes of the intelligence sharing problems that modern military intelligence organizations currently face in Afghanistan. Multinational intelligence organizations and national all-source intelligence organizations continue to develop the intelligence picture with various accesses to sources and agencies. These organizations continue to encounter important challenges when comes the time to develop a CIP that is accepted by most. This is normally predicated by the fact that they don't have access to the same quantity and quality of intelligence but, it is also based on cultural differences which tend to influence the way situations are perceived. The complexities associated with the conduct of multinational COIN operations in theatres like Afghanistan continue to challenge national and coalition intelligence organizations to their limits. It emphasizes the importance of developing a commonly accepted perception of the threat (CIP) in order to insure that operations are planned and conducted by all participating nations with a common focus. The following example highlights some of the challenges.

---

[152] Lieutenant-Colonel Steve Manning (USMC) "Improved Intelligence Support to our Coalition Partners at the Operational Level" *Naval War College* (9 May 2004): 11.

The Kabul Multinational Brigade (KMNB) was faced with an awkward situation following the arrival of a new commander, a Turkish general accompanied by his brigade staff, in early 2005. The new KMNB commander's evaluation of the threat was drastically different from the way that it had been painted by other KMNB contingents such as the Germans, the French, the British, the Italians, the Norwegians and the Canadians.[153] Turks did not perceive the threat to be as high as others and wanted to develop a "walking out policy"[154] that would allow KMNB troops to spend some time outside of the protected camps for non-official purposes. This radical change in force protection measures was intended to send a positive message to the local population about the improved level of security in the Afghan capital. Intense pressure from the coalition intelligence apparatus combined with a wave of insurgent's attacks contributed to stop this initiative before it could receive the final blessing from the ISAF command structure.[155] In this case, the development of a CIP became a key element in the success of KMNB's mission in that it allowed for the development of a common understanding of the threats necessary for the efficient planning of current and future operations.

This chapter will underline a series of issues that have been identified as having the potential of being a major obstacle to effective intelligence sharing among coalition

---

[153] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[154] During previous rotations where KMNB was under the command of the Canadians and of the Germans, troops were not allowed to leave the camp to spend time in the city in order to buy souvenirs or for other non-official activities. This policy was based on the evaluation of the threats and on the risks that commanders were prepared to take at the time.

[155] Colonel, W. Semianiw OMM CD, Commander Task Force Kabul, OP ATHENA Roto 3 (February 2005-August 2005), *Interview*, 3 March 05.

partners.[156] They are defined as *trust, national interest, organizational culture, policies and information technology (IT).* These issues are by no way inclusive of all of the elements that may affect the efficiency of intelligence sharing between coalition partners but they are assessed by the author as the ones that pose the prevailing impact on this important mechanism. It is also important to note that, even if the focus of the thesis is on the exchange of intelligence at the tactical[157] level that strategic issues continue to play a significant role on the exchange of intelligence in a theatre of operations such as Afghanistan.

TRUST

"The most sensitive touchstone of trust between individuals, as well as nations, is how far they are prepared to share secrets."[158] As mentioned by BGen Nordick, former Canadian Chief of Defense Intelligence, "trust dictates the level of risks that you are prepared to take when sharing intelligence with a coalition partner."[159] It has also been identified by every intelligence and commanding officers interviewed during this research as the number one factor that contributes to successful intelligence sharing among coalition partners. The basis of a trustworthy relationship is however difficult to isolate only at the tactical and operational levels since intelligence professionals

---

[156] These issues have been identified separately to the author by a myriad of the primary sources interviewed in direct support of this thesis.

[157] The tactical level is referred to as the lowest level of military planning, involving small units deployed in a specific theatre of operations. It is also where military intelligence officers are asked to directly support maneuver units and where they normally have the opportunity to meet intelligence counterparts from other nations with who they often develop professional relationships in order to share and receive intelligence.

[158] David Stafford and Rhodri Jeffreys-Jones (Eds.). "*American-British-Canadian Intelligence Relations 1939-2000*" (London: Frank Cass, 2000), 36.

[159] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

operating at that level are subject to national level regulations. These national directives are based on national security imperatives that are restrictive in nature when the time comes to share intelligence with coalition partners.

This fact suggests that the development of a trustworthy relationship between coalition intelligence officers at the tactical and operational levels, even if it is deemed essential by all, is not enough to guarantee that the appropriate level of intelligence will be shared among the different coalition partners.[160] A special relationship based on trust must necessarily be developed at the national level first before intelligence exchanges can be performed at the tactical level. In other words, trust among nations at the strategic level is defined as essential while trust among intelligence professionals at the tactical and operational levels, is viewed as instrumental.

Trust, within the intelligence field, is generally defined as the ability to pass sensitive information to an allied nation with a negligible risk of compromise. That passage of intelligence often results in that same nation providing intelligence back on issues that a certain nation may be interested in but may not have the capability to collect.

> Some states with particularly close relationships refrain from regular covert collection against each other; much as they might like to know the other's bottom line in many economic and other negotiations, the US and Canada probably does not tap each other's telephones to get it.[161]

Former ISAF Deputy Commander, LGen Leslie described this phenomenon during his time in command as the four intelligence circles of trust: They included the national level (Canadian), the "Four Eyes" community (Australia/Canada/Great

---

[160] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007 & Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 29 March 2006, and Ash, Capt(N), *Interview*, 7 April 2005.

[161] Michael Herman "*Intelligence Services in the Information Age*" (New York: Frank Class Publishers, 2005), 212.

Britain/United States), ISAF and finally Afghan security forces.[162] He added that his daily intelligence briefing on the overall security situation in Afghanistan given to him by his ISAF J2 staff was followed by a "Four Eyes" version with more details and additional information and then followed by a Canadian version based on other national intelligence. According to all the generals interviewed during this research, trust remained the number one factor in exchanging intelligence with other nations.[163]

Former Canadian Chief of Defence Intelligence (CDI), BGen Nordick, noted that there was no difference between sharing strategic and tactical intelligence with coalition partners because the level of trust at the national level dictated the rules that must be followed at the lower levels.[164] He added that one of the premises of joining a coalition was the acceptance of sharing a certain amount of intelligence in order to guarantee the overall success of the mission.[165] This process is defined as the balance between the risks to share intelligence and the risks of not sharing intelligence with those same partners. This reality is particularly evident when dealing with non-traditional coalition partners since their affiliation may not be based on long term alliances, common interests and shared values but only on short term mutual interests based on short to mid-term objectives.

The importance of these non-traditional partners must not be underestimated in the intelligence field because they may have the ability to provide intelligence that

---

[162] *Ibid.*, 212.

[163] Interviews conducted with Lieutenant General Ridgeway, Lieutenant General Natynczyk, Lieutenant General Leslie and Brigadier General Nordick.

[164] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

[165] *Ibid*.

countries with robust intelligence architecture may not be able to obtain through their different national collection assets. The field of HUMINT collection is probably the area where non-traditional coalition members can contribute the most to the overall intelligence efforts based on their knowledge of the terrain, the culture and on their capacity to blend in and infiltrate insurgents or terrorists cells. The role of the Jordanian intelligence services in the death of Al Qaeda leader Abu Musad Al Zarqawi and his associates on June 7th 2006 is a good example of the impressive potential presented by some of the non-traditional coalition partners.[166] Jordanian and U.S. authorities confirmed that cooperation between the nation's intelligence organizations culminated in a Jordanian reconnaissance team locating Al Zarqawi, which allowed for a U.S. air raid to be conducted, resulting in the death of the Al Qaeda leader.[167]

The difficulty in creating a trustworthy relationship also lies with the unreliability of certain countries' security vetting process. Surprisingly, NATO does not have a standardized security process or a loyalty check accepted by all members.[168] The lack of a commonly accepted security vetting process, such as the one used by the Five Eyes Community[169], has seriously hampered the establishment of long term trustworthy relationships between some of the coalition partners in Afghanistan. Moreover, the participation of 50 plus nations in the GWOT has impacted negatively on the quantity

---

[166] BBC News, "*Zarqawi killed in Iraq air raid*" (June 8, 2006). http://news.bbc.uk/2/hi/middle_east/5058304.stm, consulted on 12 Oct 2008.

[167] Michael Slackman and Shane Scott. "Terrorist Trained by Zarqawi Went Abroad, Jordan Says" *The New-York Times*, 11 June 2006, http://www.nytimes.com/2006/06/11/world/middleeast/11jordan.html, consulted on 12 Oct 2008.

[168] Lieutenant-Colonel N. Bigras CD, J2 Intelligence Production CDI, *Interview*, 24 April 2006.

[169] Australia, Britain, Canada, the United States and New Zealand share a common security vetting process that guarantee that individuals receiving access to highly classified intelligence have been with similar levels and codeword's for special compartmentalized intelligence.

and quality of the intelligence made available to all coalition partners since it has historically been based on the lowest level of trust within the coalition.[170]

The reality is also that some of the countries taking part in coalition operations in Afghanistan will never be trusted by some of the partner countries in any other another capacity than that coalition. For these countries, sharing intelligence with unreliable countries and with the rest of the coalition will remain difficult based on a generalized lack of trust.[171] Other specific circles of trust within circles, such as the Special Operations Forces (SOF), SIGINT and HUMINT communities also exist and will be discussed further in this chapter.

NATIONAL INTEREST

Decisions to share sensitive intelligence with another nation are made with the mindset that it is in the national interest of the state and that they are viewed as advantageous. National interest is the main reason why extensive protective measures are utilized by modern government in order to protect information that is sensitive in nature. In Canada, official documentation such as the Canadian Government Security Policy (GSP) and the National Defense Security Instructions (NDSI) emphasize the importance of protecting information in order to safeguard the national interest. The GSP prescribes the application of safeguards to reduce the risk of injury. It is designed to protect employees, preserve the confidentiality, integrity availability and value of assets,

---

[170] Lieutenant-Colonel G. Eanes USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005 & Mass Communication Specialist 1st Class Jessica M. Bailey "CENTRIXS Provides Vital Communication" *Navy NewsStand* (16 July 2007): 1.

[171] Colonel D.H.N Thompson OMM, CD, Director Intelligence Operations at CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 24 April 2006.

and assure the continued delivery of services.[172] According to the NDSI information should be classified when it is harmful to the National Interest and compromises government information that concerns the defense and maintenance of the social, political and economic stability of Canada.[173] The existence of these protective mechanisms coupled with policies on how to protect information and intelligence received from a foreign nation are important enablers in supporting effective intelligence sharing agreements. The bottom line is that safeguarding foreign intelligence is as important as protecting your own since its compromise would undoubtedly be harmful to the national interests.

National interests tend to change from time to time based on the political context. These interests may even come into conflict with long-term traditional allies views of a situation. The case of the 2003 war in Iraq and the relationship between Canada and the United States is a classic example of this fact.[174] Canada's decision not to support the US military efforts in Iraq resulted in an important decrease in the quantity and quality of U.S. intelligence passed to Canada.[175] This also affected other sectors of intelligence that were not directly linked to the Iraq context. Canadian Forces Lieutenant General Walter Natyncyk, in his capacity as former Deputy Commanding General III Corps (U.S.), confirmed that he was cut out of every aspect of U.S. intelligence on Iraq after the

---

[172] Government of Canada, *Government Security Policy*, http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/gsp-psg1_e.asp#acc, consulted 12 Nov 2007.

[173] Government of Canada, *National Defence Security Instructions, NDIS 27 – Classification and Designation of Information*, (15 September 2005). *http://vcds.mil.ca/cfpm/pubs/pol-pubs/ndsi/intro_e.asp*, consulted 12 Nov 2007.

[174] Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Viking Canada, 2007), 56.

[175] Colonel J.G.A.J.C. Rousseau CD, Intelligence Branch Advisor and J2X CDI, *Interview*, 2 November 2007.

Canadian government announced that it would not send troops to support the U.S.-led coalition but he added that he still continued to receive intelligence on Afghanistan.[176] According to the former Canadian Forces Intelligence Branch Advisor, Colonel Christian Rousseau, the deterioration of the Canada-U.S. intelligence relationship demonstrated that interests are stronger than relations.[177] However, the Canada-U.S. special intelligence relationship rapidly improved once again following the change of government in Canada in January 2006 and with Canada's new role in southern Afghanistan.

ORGANIZATIONAL CULTURE

Organizational culture is viewed by many observers as the most important factor impeding effective sharing of intelligence between intelligence organizations nationally. Edgar Schein, one of the foremost experts on the topic, offers this definition of organizational culture:

> A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, to be thought to new members as the correct way to perceive, think, and feel in relation to those problems.[178]

In the case of intelligence organizations, the most distinctive feature of the organizational culture is intelligence's secrecy and the sense of difference and mystique it produces.[179]

---

[176] Lieutenant-General W.J. Natynczyk CMM MSC CD, former Deputy Commanding General of the Multi-National Corps Iraq (Iraqi Freedom), *Interview*, 27 April 2006.

[177] Colonel J.G.A.J.C. Rousseau CD, Intelligence Branch Advisor and J2X CDI, *Interview*, 2 November 2007.

[178] Edgar H. Schein, *Organizational Culture and Leadership* (San Francisco: Jossey-Bass Publishers, 1992), 12.

[179] Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press 1996), 384.

This sense of secrecy is based on the sensitivity of the information processed, coupled with the obstacles that security guidelines pose to the passage of information. It is fair to assume that the phenomenon of secrecy does not help in improving communication among the different intelligence organizations, even within the same country.

Since 9/11 many papers such as Special Agent Chase H. Boardman's and Colonel Terence J. Hildner's have been written about the role that organizational culture played with regards to problems between national intelligence agencies the U.S., the U.K. and Australia[180]. The 9/11 Commission in the U.S., the Butler Report in the U.K. and the Flood Report in Australia have all recently highlighted the difficulties experienced by national intelligence organizations in effectively sharing intelligence. Michael Herman adds that "Professional cultures mix cooperation with rivalry."[181] Like any other governmental organization, intelligence agencies, departments and services are often known to be competing for resources while still cooperating at the same time.[182] Many different cultures exist and they are for the most part based on the specialty in which they are employed. Even if high level managers often openly compete for resources and credit, professional intelligence operators are known to quietly make things happen on

---

[180] Special Agent Chase H. Boardman, "Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction" *Joint Forces Staff College – Joint Advanced Warfighting School*, (31 May 2006) and Colonel Terence, J. Hilder, "Interagency Reform: Changing Organizational Culture Through Education and Assignment" *United States Army War College*, (30 March 2007).

[181] Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press 1996), 308.

[182] Recognition of intelligence successes by governmental authorities is often associated with a positive impact on the overall status of the organization within the community (i.e. increased resources or reduced cuts in the case of decreased government spending).

the front lines. "Turf fights between front offices coexist with unspectacular backroom cooperation."[183]

The organizational culture of intelligence organizations has also contributed to the phenomenon of over-classifying and excessive secrecy. This trend was very much present during the Cold War where national intelligence organizations were mostly focused on strategic issues. The support to the warfighter operating within a coalition in Afghanistan has required significant changes in the way intelligence reports are classified. In simple terms, classifying intelligence reports at the TOP SECRET[184] level or with restrictive national caveats[185] would not be of any use to the soldiers in the field who would normally operate at lower level of classification such as the SECRET[186] level.

> Recent moves away from excessive secrecy over satellite collection were summarized by the responsible member of the in the U.S. Administration in mid-1998. The NRO (National Reconnaissance Office) has significantly reduced the classification of the overhead product. Today, over 99 per cent of this operational data is available at the SECRET level for direct use by the warfighter.[187]

The excessive use of national caveats has seriously hindered the effectiveness of coalition intelligence efforts in Afghanistan and the development of a CIP. A recent shift

---

[183] Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press 1996), 308.

[184] TOP SECRET intelligence is normally related to strategic issues or to topics that could cause extremely grave harm to the national security in case of compromise.

[185] National caveats are what limit the distribution of information to other nations. In the U.S. the NOFORN or U.S. Only caveats are used when the information is not releasable to any other nation. In Canada and in the UK, a similar caveat exists in order to protect releasing information to another nation. i.e. UK Only and Canadian Eyes Only. Caveats are also permissive in that they can identified to which selected nations a national reports can be distributed to. i.e. AUS-CAN-GBR-USA allows for the dissemination of these report to the ABCA nations.

[186] SECRET intelligence is often intelligence related to tactical collection or from strategic collection assets that has been downgraded by the releasing authority in order to make the information available at the tactical level.

[187] Michael Herman, *Intelligence Services in the Information Age* (New York: Frank Class Publishers, 2005), 53.

in this mindset has been witnessed in the U.S. intelligence community (IC). In a memorandum sent to senior Pentagon officials in May 2005, Stephen Cambone, the undersecretary of intelligence of the time alleged that:

> Restrictions on international disclosure – classifying documents as "Not releasable to foreign nationals", or NOFORN in Pentagon jargon – have been excessive. Incorrect use of the NOFORN caveat on DoD[188] information has impeded the sharing of classified national defense information with allies and coalition partners. For intelligence under the purview of the DoD, originators shall use the 'Releasable to' marking…to the maximum extent possible.[189]

National directives, such as the one presented above, have been numerous since 9/11 but they have, for the most part, not resulted in rapid changes to the quantity and quality of new U.S. intelligence made available to all coalition partners.[190] This is in fact due to the magnitude of these directed changes in the organizational culture of the U.S. IC.

Some of the closest U.S. allies, such as Australia and Canada, continued to face difficulties in acquiring key intelligence for their respective theatre of operations. Australian Former Prime Minister John Howard appealed directly to President Bush in 2005 when U.S. intelligence agencies had restricted his country's access to key intelligence on the war in Iraq. This was done more than a year after President Bush had signed an order in July 2004 granting Australia and Britain special access to intelligence for use in planning combat and counter-terrorism operations.[191] According to Premier

---

[188] DoD stands for the U.S. Department of Defense.

[189] Peter Spiegel "Pentagon Chief Orders Staff to Give Allies Better Access to Classified data" *Financial Times*, 3 June 2005. www.ft.com/cms/s/03b2c382-d3cd-11d9-ad4b-00000e2511c8.html, consulted 25 Nov 2008.

[190] Lieutenant-Colonel G. Eanes USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005 & Major M. Green, SO2, Officer Commanding UK National Intelligence Centre, Kabul Afghanistan (February 2005-August 2005), *Interview*, 8 April 2005.

Howard, U.S. agencies initially resisted the order because of their inherent reluctance to share information. Restrictions were finally lifted later in 2005 and efficient intelligence sharing mechanisms have been instituted.[192]

Another example of over classifying reports is the case of Afghan prisoners who had been captured by Canadian Forces elements in 2003 and 2004.[193] These prisoners were captured during raids based on a mix of coalition and Canadian intelligence.[194] Prisoners were transferred to the Afghan authorities for further processing and interrogation and finally ended up in U.S. custody. The problem that followed was that U.S. interrogators did not release any of their reports to the Canadian Task Force in Afghanistan because they had been classified as NOFORN[195] which did not allow for the content to be passed to anyone other than a cleared U.S. citizen with the required need to know. An official request from Canada finally succeeded in obtaining access to these reports following many months of discussions on the issue.

POLICIES

Since intelligence remains an issue of the highest importance for a state, it is understandable that the policies responsible to guide this critical function are, for the most part, exclusively national. These policies, which have been influenced by the national IC's organizational culture, have often been viewed as bureaucratic obstacles to

---

[191] Agence France Presse. "Australian PM: US Intelligence Agencies Reluctant to Share Information on Iraq" *Agence France Presse*, 4 October 2006. http://www.globalsecurity.org/intell/library/news/2006/intell-061004-voa01.htm, consulted 12 Nov 2008.

[192] *Ibid*.

[193] Canadian Special Operations Command, Confidential Source 006, *Interview*, 27 April 2006.

[194] *Ibid*.

[195] NOFORN means that no foreign national other than U.S. citizens have access to the information.

the true exchange of intelligence among nations. Policies and directives responsible to legislate how intelligence is safeguarded have been fairly successful to date but the aspect of how policies allow intelligence to be shared between nations remains to be modernized.

The classification of information which is responsible to safeguard national security related subjects is based on the originator's responsibility to assign a level of protection to the information. For example, in Canada, the policy in the NDSI 27 document stipulates that:

> Originators of departmental information are required to assess the content of their documents to determine if a security classification must be assigned. This process eliminates the over-classification of departmental information, which could impose impractical administrative or operational restrictions and degrade the efficiency and usefulness of the classification system. Conversely, under-classification, could fail to provide adequate protection of such information.[196]

This mechanism is however far from faultless in that it is based on the originator's judgement, experience and also on the way that he has been trained and influenced by his own organization.

In 2005, Canadian ASIC personnel deployed in Afghanistan were instructed to classify their reports based on the "write for release"[197] principle. This directive presented internal challenges among the most restrictive intelligence specialties[198] but it also allowed for the vast majority of the reports to be disseminated to all of the coalition

---

[196] Government of Canada, *National Defence Security Instructions, NDIS 27 – Classification and Designation of Information* (15 September 2005) *http://vcds.mil.ca/cfpm/pubs/pol-pubs/ndsi/intro_e.asp*, consulted 13 Nov 2008.

[197] Write for release makes reference to the philosophy of writing intelligence reports based on the lowest denominator within a coalition thereby insuring that the product could be disseminated to the largest audience possible without leaving sensitive information unprotected.

[198] Refers to collectors (HUMINT, SIGINT, and IMINT) that have very strict protective mechanisms in place in order to protect their sources and methods.

partners operating in Afghanistan.[199] This method, based on classifying intelligence reports to the lowest denominator possible, contributed to sharing the view of the threat with as many coalition partners as possible.[200] It also allowed for intelligence staff to remain focused on the intelligence cycle rather than the often complex and time-consuming declassifying or foreign disclosure processes.[201] Canadian intelligence collectors and ASIC analysts were directed to provide their reports at the ISAF SECRET level or less so that the daily intelligence summary could be disseminated to all coalition partners including Afghan security forces.[202]

Policies that spell out the methods and mechanisms on how to share intelligence with foreign nations are non-existent in most countries.[203] In Canada, the only policies[204] that guide the business of sharing intelligence are restrictive in nature and do not provide the legal and operational framework that would facilitate such an endeavour. The reality is that intelligence sharing agreements are, for the most part, formed on a multilateral or bilateral basis which is often articulated through a Memorandum of Understanding (MOU) between the nations involved. In the absence of a clear policy, the MOUs are

---

[199] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[200] Colonel, W. Semianiw OMM CD, former Commander Task Force Kabul, OP ATHENA Roto 3 (February 2005-August 2005), *Interview*, 3 March 05.

[201] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[202] *Ibid*.

[203] Jorgen Kruger, Director Intelligence Policies and Programs, CDI, *Interview*, 2 November 2007.

[204] The Security of Information Act and the Government Security Policy dated 24 December 2001are the two main documents in Canada that legislate how intelligence is handled. These documents do not directly handle methods of how to share intelligence with a foreign nation.

used as technical enablers.[205] MOUs provide some mechanism on how to share but they also present some important disadvantages. According to Jorgen Kruger, Director of Intelligence Policies and Program within the CDI organization in Canada, MOUs are not timely, they require significant staff efforts at the strategic level, they have to be reviewed periodically and they do not provide any flexibility for the intelligence staff deployed in the field.[206] If a subject is not clearly covered by a MOU, then it will be impossible for the deployed intelligence staff to share it with a partner nation even if it seems to make sense to everyone involved.

The U.S., which is clearly the largest contributor to the coalition in Afghanistan, has a robust program in place to allow for disclosure of intelligence to a foreign nation.[207] Studying the U.S. model is therefore that much important because it has such an impact on what intelligence becomes available to other coalition partners. In his paper entitled *Optimizing Intelligence Sharing in a Coalition Environment*, Colonel George Gramer Jr. describes how U.S. intelligence should be made available to other coalition partners:

> Clearly everything should not be releasable – the coalition or alliance does not need 100 percent of the available U.S. national intelligence. The coalition requires tailored, viable, timely, sharable tactical and operational intelligence information. Sanitized information should safeguard and protect lives, information sources and operations.[208]

---

[205] Jorgen Kruger, Director Intelligence Policies and Programs, CDI, *Interview*, 2 November 2007.

[206] *Ibid*.

[207] The National Defense Policy (NDP-1) and the Intelligence Disclosure Policy (DCID 6/7) governs how the U.S. releases military information to foreign governments and international organizations and establishes eligibility criteria to receive releasable information. Detailed procedures for handling, processing, downgrading, release and sanitization of these material exist (exerts from Joint Publication 2-01).

[208] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 11.

The principle of "need to know" is also considered in the U.S. system and the evaluation of that requirement sits with the senior intelligence Officer often referred as the Combined Joint Senior Staff Officer for intelligence (CJ2). Moreover, the U.S. requires that nations receiving U.S. intelligence have a security protection program comparable to the U.S. model in order to mitigate the risks of compromise.[209] Modern coalitions do not have policies and doctrine in place which directs how intelligence can be shared among the partners. No coherent multinational intelligence doctrine currently exists outside of NATO parameters and even less with non-traditional partners such as many involved in coalition operations in Afghanistan.[210]

INFORMATION TECHNOLOGY (IT)

The last factor presented in this chapter is the impact that information technology has on effective intelligence sharing among coalition partners. Experts in the field agree that IT plays an important role in all of the four phases of the intelligence cycle but that this role becomes critical and essential during two of those phases: processing and dissemination. During the processing phase, IT is undoubtedly a key enabler. CCIRM requires powerful and agile database management IT tools in order to allow the collators and analysts to work seamlessly through huge amounts of data. One of the constant challenges with regards to database management remains the methodology used to handle the data, the advances in technologies and how these advances impact on the evolution and relevancy of the data.

---

[209] United States Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations Joint Publication 2-01*, (October 7, 2004): E-4.

[210] Lieutenant-Colonel Steve Manning (USMC) "Improved Intelligence Support to our Coalition Partners at the Operational Level" *Naval War College* (9 May 2004): 7.

Creating databases that can be used by follow-on coalition rotations is as important as creating the database in the first place. There have been many cases where new rotation of troops had to start from nothing because they did not have a compatible IT system to transfer the data or because they did not speak the language of past rotations.[211] Even though English is the language of choice for Western coalition forces, there have been cases where other languages have been used during certain rotations. A good example of this is Canada's participation in coalition operations in Bosnia.[212] Canada's contribution ended in 2006 after 27 six-month rotations, with data scattered on 158 different CDs, some in French, some in English, all using incompatible software and formats.[213] This is also happening in Afghanistan where some countries use languages other than English to populate their important databases.[214] The reality is that the information contained in the database would now be extremely difficult to re-use or share with other potential coalition partners. There is no common standard, no common language, and no common software, and insufficient efforts were undertaken to upgrade the software used over years. Hence, efficient information sharing could only be achieved if a common information structure was adopted based on one semantic.[215]

---

[211] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[212] Canada contributed to UN and NATO led Coalitions in Bosnia.

[213] Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

[214] Master Warrant Officer, M. Thibault MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[215] Gaétan Thibault, Lieutenant-Colonel M. Gareau and François Le May "Intelligence collation in asymmetric conflict: A Canadian armed forces perspective" *System of Systems Section, Defence R&D Canada Valcartier, Canada*, (July 2007): 4.

Advances in technologies represent an important asset to modern intelligence organizations. New software has been developed in order to support the analysis process and to better understand how networks of insurgents or extremists are organized and function.[216] Link analysis software such as the I2 analyst notebook[217] is employed by a large number of coalition partners in Afghanistan. Some countries choose to purchase only certain variants of the software while others use different languages or methodology to input the data. The lack of standardization seriously diminishes the potential advantage that such interoperable software could provide if available to all coalition partners.

The development of biometrics software designed to identify individuals by using exclusive physiological[218] or behavioral[219] signatures has also provided opportunities for intelligence organizations in Afghanistan to build databases of individuals using these characteristics. Biometric technology has the potential to be particularly useful in the CI field, although releasibility, lack of standardization and legal issues continue to reduce the potential that this type of technology represents for coalition forces in Afghanistan.

Within the dissemination phase, many experts believe that IT is the most important factor because it allows for large files (text, video or graphical) of classified information to be disseminated through long distances in a safe and effective way. The creation of a classified network that can be used by all coalition members and that is

---

[216] *Ibid.*, 6.

[217] I2 analyst notebook (Copyright © 2008 i2 Ltd. All Rights Reserved) is a link analysis software used to graphically represent extremist networks and insurgent's relationships to one another in support of target development associated tasks.

[218] Physiological is related to the shape of the body (fingerprints, iris, palm, face and DNA).

[219] Behavioural makes reference to behaviour of an individual (Signature, voice, keyboard).

populated by all is an essential element for the creation of a relevant and precise CIP. Systems such as CENTRIX and the ISAF LAN have been developed to take on this role in order to allow for the passage of information and intelligence between all coalition partners. In Afghanistan, there is no doubt in anyone's mind that the proper IT networks are now in place.[220] The problem was, for the longest time, that they were not used to their projected potential. The classified IT networks have been in place for many years now but nations such as Canada, the UK and the United States have just recently been using them more extensively. The reality is that these systems are only as good as the information that populates them. U.S. forces continue to predominantly use SIPRNet and JWICS[221] even though they have made significant efforts towards migrating to CENTRIX and the ISAF LAN.[222] The less sensitive reports are known to be published on the coalition networks while the more sensitive ones remain on national or ABCA networks.[223]

New technologies that have been developed on the internet have made their way to the classified intelligence networks. Coalition forces in Afghanistan have access to chat rooms, classified video-teleconference and web-based programs in order to facilitate

---

[220] Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 15 November 2007, Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007, Major M. Green, SO2, Officer Commanding UK National Intelligence Centre, Kabul Afghanistan (February 2005-August 2005), *Interview*, 8 April 2005 & Lieutenant-Colonel G. Eanes USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005.

[221] SIPRNet and JWICS are two NOFORN U.S. only systems not available to other coalition. members. Britain, Australia and Canada have recently been allowed access to certain sectors of SIPRNet.

[222] Major J.Y. Belzile CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 15 November 2007.

[223] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

the passage of sensitive information in a timely and secure fashion. These new technologies have drastically increased the size of the bandwidth required to support such systems. Canadian intelligence organizations in Afghanistan were responsible for the use of over 80% of all the bandwidth available to all of the Task Force users.[224] The size of the encrypted files and the level of detail required explain the increase in the bandwidth requirement over the years. Chat rooms have also contributed to increase the level of situation awareness for the soldiers deployed outside of the security of the camps.

> People who go out on patrol can enter a chat room and let everyone know what they saw. There might be a lucrative target out there, whether a truck or a car or a group of people or a building or something else. And chat rooms help effectively coordinate the time-sensitive targeting process.[225]

SUMMARY

This chapter has presented five of the most important factors that have affected the exchange of intelligence between coalition partners in one way or another. It has also demonstrated that many of the issues facing tactical and operational intelligence organizations on sharing originate from the national level and that many of the problem areas are intermingled. Based on the importance of intelligence for any nation and the direct relationship to its national interests, it is fair to believe that solutions to significantly improve the current intelligence sharing agreements will have to continue to be developed with the key support at the national level. The following chapter will propose some recommendations on how to improve the current coalition intelligence system and to strive towards the development of a true CIP.

---

[224] Master Warrant Officer, M. Thibault, MMM, CD. Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005.

[225] Dona Miles "Information Access Key in Terror War, CENTCOM General Says" *American Forces Press Service*, 31 March 2005.

CHAPTER 5 – RECOMMENDATIONS

> …the focus must be on regional collectors, unclassified sources and staying away from national assets and associated restrictions and that coalition intelligence sharing successes are based on the establishment of policies, keeping the focus on using tactical collectors and creating an efficient dissemination IT network.[226]

The previous chapter demonstrated that national policies and strategic decisions have a direct impact on the way intelligence is shared by coalition partners at the strategic, operational and tactical levels. It also highlighted the fact that it is impossible to address the intelligence sharing problems faced by coalition forces in Afghanistan by focusing exclusively at the tactical and operational levels. Chapter four also recognized the importance that five factors (trust, national interests, organizational culture, policies and information technology) have had on the way that intelligence is being shared by coalition's members in Afghanistan. These factors will be used as a guide by the author in presenting recommendations on how to improve intelligence sharing within coalition operations.

IMPROVING TRUST THROUGH THE ALIGNMENT OF NATIONAL INTERESTS

Trust has been previously defined as the most important factor impacting on how intelligence is shared between nations. This factor is closely intermingled with the notion of national interest since countries often base their trust on common values and mutual interests. It would be utopia to believe that all coalition partners would be capable of trusting each other in current or future coalition operations, and would be prepared to share all of their intelligence seamlessly. Furthermore, the role played by each coalition

---

[226] Lieutenant-Colonel Steve Manning (USMC) "Improved Intelligence Support to our Coalition Partners at the Operational Level" *Naval War College* (9 May 2004): 15.

partner within a coalition tends to dictate how these nations are perceived by other partners and, sometimes, how intelligence is made available to them.[227] National "caveats" within an operation/campaign can also negatively affect the development of trustworthy relationships between coalition partners. These limitations included Germany's refusal to ferry soldiers from other NATO countries in its helicopters, prohibitions on the use of tear gas and refusal to permit soldiers to operate at night.[228]

The author sees only one way to improve the current level of trust among coalition partners in Afghanistan. It is through the creation of formalized multinational objectives that coalition partners would adhere to. Every coalition partner would have to be prepared to contribute forces to the overall effort and be prepared to take equal levels of risk in doing so. The creation of the U.S. – U.K. intelligence cooperation model (which later became the four eyes community) during the Second World War, was been based on the necessity to better cooperate and share intelligence in the face of great peril.[229] These special relationships assisted in the creation of an intelligence sharing model that continues to be relevant 68 years later. Coalition partners must agree, at the strategic level first, on multinational interests that will lead current and future actions of a coalition. NATO, as the leading multinational organization in Afghanistan, has the responsibility to take the lead on the issue of intelligence sharing by formalizing

---

[227] Colonel Paul J. de B. Taillon, "Coalition Special Operation Forces: Building Partner capability" *Canadian Military Journal*, 8.3 (Autumn 2007): 46-47.

[228] Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Viking Canada, 2007), 202.

[229] Jeffrey T. Richelson and Desmond Ball, *The Ties that Bind: Intelligence Cooperation between the UKUSA Countries* (Boston: Allen & Unwin, 1985), 1.

processes and procedures and, by soliciting the participation of all nations in order to improve trust between partner nations.

CHANGING THE ORGANIZATIONAL CULTURE OF INTELLIGENCE ORGANIZATIONS

National intelligence organizations, all over the world, must continue to work on changing their organizational culture towards a mindset of cooperation and of a "need to share". They must adapt their operating procedures and methods to the realities of integration and of cooperation between services, agencies and states. The U.S. 500 Day plan for integration and collaboration, presented by the U.S. Director of National Intelligence Mike McConnell on 10 October 2007, emphasized the importance of changing the old culture of secrecy and competition often reported within the U.S. IC.[230] This model is a good example to follow for the coalition intelligence community in that most, if not all, of the founding principles of this plan could easily be transposed to a coalition intelligence apparatus. The focus of the U.S. plan is clearly based on creating a culture of collaboration and on accelerating information sharing.[231] It advocates the establishment of a new philosophy based on the "obligation to provide" versus one that had been almost exclusively based on the "need to know".

The role of education

This study agrees wholeheartedly with one of the enabling initiatives presented in the U.S. 500 day plan in that the best way to modify the organizational culture of national ICs is by placing emphasis on education at the earliest stages in the career of intelligence

---

[230] U.S. Intelligence Community. "500 Day Plan: Integration and Collaboration" (10 October 2007): 1. http://www.dni.gov/500-day-plan/500-day-plan.pdf

[231] *Ibid*., 2.

professionals. The U.S. plan recognizes the importance of formalizing a National Intelligence University program where new members of the U.S. IC would be trained with their colleagues from other intelligence fields before continuing to more specialized training within their respective agencies.[232]

Similarly in Canada, many discussions have been taking place between military intelligence stakeholders about the creation of a Defence Intelligence Academy. This academy's principal objective would be to create a new Canadian Defence Intelligence organizational culture by providing common training to every member of the Defence Intelligence Community (DIC) and by encouraging contacts between members from different intelligence specialties early in their careers.[233] As with the U.S. model, this academy would provide a core program that would be pursued by every new member of the DIC followed by specialized training for each of the specialties i.e. SIGINT, IMINT, HUMINT, GEOINT, etc. Such an Academy would provide the ideal medium required to model an effective DIC organizational culture based on cooperation and integration, one which would eventually translate its successes to the strategic, operational and tactical levels. Other recommendations presented later in this chapter, such as the development of coalition intelligence training opportunities, will also contribute to support the development of a new organizational culture.

CREATING MULTINATIONAL INTELLIGENCE ORGANIZATIONS

---

[232] *Ibid*., 4.

[233] Colonel, J.G.A.J.C. Rousseau CD, Intelligence Branch Advisor and J2X, *Interview*, 2 November 2007 & Brigadier-General G.W. Nordick OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006.

Policies on how intelligence operations must be conducted within coalitions must be developed under the leadership of a multinational organization such as ABCA or NATO. As noted earlier in this thesis NATO relies only on voluntary release of national intelligence from its participating members and does not have formed intelligence organization other than one very small counter-intelligence unit. One of the solutions for NATO would be to create its own intelligence collection capabilities in areas such as HUMINT, unmanned aerial vehicles (UAV), SIGINT and IMINT.[234] Existing commercial technologies and experienced nations could contribute to forming these new multinational tactical intelligence organizations that would provide NATO with the integrated intelligence support required during deployments such as ISAF in Afghanistan. The creation of such multinational organizations would also significantly reduce the level of dependence on national intelligence organizations and provide NATO's intelligence apparatus with a true sense of interoperability. NATO currently has one truly multinational unit called the NATO Airborne Early Warning Force based on a fleet of 17 E-3 Sentry AWACS[235] aircraft. Future NATO intelligence units could be formed under a similar model.

NATO remains the best possible alliance within which Western countries could form multinational intelligence organizations, based on the existing AWACS model. It is the author's opinion that member states would be interested in such endeavours if the requirement for nations to divulge technical advances remained minimal and if the

---

[234] Colonel J.G.A.J.C.Rousseau CD, Intelligence Branch Advisor and J2X CDI, *Interview*, 2 November 2007.

[235] AWACS stands for Airborne Warning and Control System. It is an aircraft platform responsible to conduct surveillance related tasks and provides command and control services.

benefits would greatly surpass the associated cost and risks. Member states would have to provide the funding required for these collection assets and base their capabilities on commercially available technologies and procedures.

> The coalition commander must strengthen unity of effort through the establishment of combined joint intelligence elements and intelligence processing center in order to foster intelligence cooperation and sharing and create a central focus for all multinational intelligence requirements… By making the command's intelligence processing center multinational in character, the intelligence contributions of all multinational partners will be enhanced, and many dissemination problems may be resolved.[236]

Over the years, the existence of multinational intelligence organizations has been described as one of the key elements required to conduct successful coalition operations. NATO's after action reports (AAR), dating back to the mid-1990s, highlight the importance of creating such organizations in order to ensure the appropriate passage of information to all of the participating nations as well as to provide the level of integrated analysis required by coalition forces.[237] Based on the fact that HUMINT capabilities are often viewed as the most important in a COIN environment, and because it does not rely on the transfer of sensitive technical data, it is assessed as the capability of choice to be developed at the multinational level.

IMPROVING THE COORDINATION OF INTELLIGENCE CAPABILITIES

Another way to improve intelligence sharing policies is by focusing on the coordination of the vast majority of national and multinational intelligence organizations involved in a theatre of operation. This option centers on coalition forces making the best

---

[236] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 13.

[237] Melissa Patrick "Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operations Joint Endeavour" *Army War College* (10 April 2000): 7-8.

use of the intelligence capabilities each coalition partner brings.[238] The U.S. Joint publication 2.0 supports this approach. It emphasizes that the coalition commander must adjust for differences and adapt to the differing capabilities of each coalition partner.[239] In other words, a coalition commander must demonstrate strong leadership and persuasive qualities early in the planning stages of coalition operations in order to maximize the intelligence resources that could potentially be made available to him or her. Some of the most advanced coalition partners may provide more technical intelligence capabilities such as UAVs, SIGINT and IMINT assets while other less technically advanced partners could provide HUMINT, counter-intelligence (CI) and special reconnaissance[240] capabilities.

Another option requires a drastic augmentation in the use of commercially available intelligence capabilities. This is specifically feasible in the field of IMINT where commercial satellites are more accessible than ever and where U.S. security caveats have historically limited the wider dissemination of products originating from the U.S. military satellite constellation.[241] The development of commercially available technologies in the fields of surveillance and reconnaissance functions has also

---

[238] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 13.

[239] United States Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations Joint Publication 2-01*, (October 7, 2004).

[240] Special reconnaissance capabilities make reference to special units that are formed to conduct reconnaissance in all type of settings, in the most demanding conditions and in support of tactical to strategic objectives.

[241] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 15.

progressed extensively allowing for their easy application to military functions.[242] It is assessed that the most important obstacles to this option remains linked to availability of resources, to the associated financial commitments required from coalition partners, and to the assignment of a champion (nation or multinational organization) that would lead such projects.

INCREASING LIAISON

The use of intelligence liaison teams is another way to improve intelligence exchanges between coalition partners. Intelligence liaison teams greatly assist in providing a better understanding of national intelligence capabilities to other coalition partners as well as serving as a stepping stone in establishing trust, confidence, and interoperability.[243] Moreover, the presence of intelligence liaison officers brings direct access to national and component[244] specific intelligence resources and directly contributes to the development of an integrated evaluation of the threat through a CIP.

Intelligence liaison can also be provided to a theatre level coalition HQ by the creation of national intelligence centers (NICs). NICs are normally formed into a "village"[245] in proximity to the coalition HQ. In Afghanistan, the NIC village is established directly besides the main building housing ISAF HQ in Kabul.[246] NICs have

---

[242] Ibid., 13-14.

[243] Major Michele H. Brendenkamp (U.S. Army) "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces?" *School of Advances Military Studies – U.S. Army Command and General Staff College* (AY 2002-2003): 45.

[244] Refers to: special operation forces (SOF), Army, Navy, Air force and Marines.

[245] NIC village makes reference to the sector where NICs are set up. Under the NATO construct, the NIC village is standard operating procedures when setting up a theatre level HQ.

[246] Major, D. Zegarac Deputy Chief Assessments, International Security Assistance Force Kabul Afghanistan, *Interview*, 20 November 2007.

been developed exclusively as national intelligence organizations but their proximity to the main coalition HQ allows them the access to overall coalition affairs as well as providing access back to national intelligence organizations in return. Their contribution is essential in order to develop a theatre level CIP and maintain connectivity with various national intelligence organizations: military and civilian.

DEVELOPING COMMON POLICIES AND PROCEDURES

Despite the lack of a single intelligence doctrine for non-NATO and ABCA multinational operations, standardization is essential.[247] The role of an intelligence sharing procedures is to facilitate the passage of information by standardizing the mechanisms that coalition partners are expected to follow. These procedures include details such as the formats, timings and means used to disseminate intelligence reports. Intelligence sharing procedures also dictate whether the coalition sharing mechanisms will be based on a "push" or a "pull" system.[248] Most experts agree that the best system is a mix of the two which is often referred to as the "smart push" or the "smart pull" system. This allows users to know when a product is available (push system) while it also provides access to a standardized database accessible to every other partners (pull system).[249]

---

[247] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 12.

[248] With regards to a typical coalition intelligence apparatus, the term "push" systems makes reference to the fact that the intelligence is "pushed" to organizations that require it through the systematic use of classified e-mails, while the "pull" method sees intelligence reports posted on a web page or a portal requiring the client to search for the intelligence themselves.

[249] J.R. Wilson "Expanded use of advanced communications technology is enabling nearly instantaneous delivery of vital military information" *Aerospace America Online*, October 2003, http://www.aiaa.org/aerospace/Article.cfm?issuetocid=418&ArchiveIssueID=43

Efficient intelligence sharing procedures are critical in that they contribute to significantly improving the interoperability of intelligence organizations, processes and associated technologies.[250] These policies have to be accepted well in advance of a coalition being deployed in order to have all intelligence staff intimately involved with the mechanisms that will be in place during their time in a specific theatre.[251] Procedures cannot be left to the last minute or until a coalition is deployed because there will be very little time to troubleshoot after arriving in a theatre of operations. Commanders will expect to receive sufficient intelligence support immediately. As noted by Major Barret Peavie:

> Intelligence sharing procedures must be established in the planning process of a multinational operation, a concept that magnifies in difficulty with coalitions due principally by its ad hoc nature.[252]

These procedures will also have to be tested by intelligence coalition partners during pre-deployment training in order to be validated by the contributing nations and to allow intelligence staff to become proficient with them.

INTEROPERABILITY THROUGH TRAINING

In order to efficiently support knowledge-centric coalition forces, the intelligence apparatus needs to be well-organized and operational long before they start to operate in their theatre of operations. As depicted by Major Michelle Bredenkamp, intelligence organizations must have opportunities to train together in order to facilitate the exchange

---

[250] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 11.

[251] *Ibid*., 12.

[252] Major Barret K. Peavie (US Army) "Intelligence sharing in Bosnia" *United States Army Command and General Staff College* (AY 00-01): 17.

of intelligence and guarantee a certain level of interoperability.[253] Coalition intelligence personnel follow their own national pre-deployment training plans prior to deploying overseas. In most countries, this pre-deployment training is focused on individual skills[254] required to operate in a war zone, and complemented by collective training with the emphasis on national task force level operations. National contingents focus on the interoperability of their national assets, with very little emphasis placed on intelligence sharing mechanisms with other coalition partners.[255]

Coalition intelligence training must be organized and coordinated between all coalitions partners involved prior to the deployment of forces into a theatre of operations. This training would provide coalition partners with opportunities to practice how they would effectively share intelligence and interact during the duration of their tour of duty. Such exercises would require extensive communications and IT support but could be conducted without involving large number of troops in the field. The use of simulated troops would significantly reduce the cost and the logistical complexity associated with these exercises. Coalition intelligence exercises would also contribute to develop a high level of interoperability between coalition members and would contribute to increase the level of trust between coalition members. Interoperability between units is known to

---

[253] Major Michele H. Bredenkamp (U.S. Army) "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces?" *School of Advanced Military Studies – U.S. Army Command and General Staff College* (AY 2002-2003): 28.

[254] Individual training is mostly focused on weapons, first aid, mine awareness, Improvised Explosives Devices (IED) and immediate actions expected to be conducted by every soldier.

[255] Major, S. Neveu CD, J2 Plans 2, CDI, *Interview*, 2 November 2007.

effectively diminish compartmentalization and increase intelligence sharing between the organizations involved.[256]

INFORMATION TECHNOLOGY (IT)

As underlined previously, information technology had the potential to become one of the key enablers to efficient intelligence sharing within a coalition such as the one in Afghanistan. However, it is important to note that IT also has the potential to become one of the biggest obstacles to efficient information sharing. For example, IT tools must be fully interoperable among coalition partners. Intelligence software such as I2 Analyst Notebook and biometric programs must be made available to all coalition partners. Databases must also be standardized in order to make the intelligence more easily accessible and available to all concerned.[257] In addition to non-standardized input formats, there is an issue with the difference in manual entry and input capability among coalition members.[258] Coalition partners would remain responsible for classifying the information populating their national databases to the appropriate level based on the

---

[256] Anthony H. Cordesman "The Ongoing Lessons of Afghanistan: Warfighting, Intelligence, Force Transformation, and Nation Building" *Center for Strategic and International Studies* (6 May 2004): 47.

[257] Gaétan Thibault, Lieutenant-Colonel M. Gareau and François Le May "Intelligence collation in asymmetric conflict: A Canadian armed forces perspective" *System of Systems Section, Defence R&D Canada Valcartier, Canada,* (July 2007): 6-7.

[258] Captain J. Callacott CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007.

"write for release" principle.[259] Moreover, standardizing the processes would make the intelligence more easily retrievable and exploitable by all coalition partners.

Standardizing these IT tools is clearly a colossal task but it is assessed as a critical element of successful intelligence sharing for any coalition. Coalition partners have to agree, in advance, to a common information technology language and a standardized way of processing the information. It is the author's opinion that this would only be feasible if one country of a group of countries, such as ABCA or NATO, took on the task of making these tools interoperable for all coalition partners. The idea would be that coalition partners would all have advanced, efficient and interoperable IT tools to work with, as well as the classified network architecture required to share intelligence efficiently. The author realizes that applying this recommendation would likely take a lot of time and resources but the expected results would outweigh the benefits of the status quo.

Coalition classified networks such as CENTRIXS and the ISAF LAN must be the networks of choice for everything that has to do with coalition operations and intelligence related information in Afghanistan. National and multinational intelligence organizations, at the strategic and tactical levels, must recognize the importance of these networks and regulate their use systematically. These classified coalition networks must become handy to all coalition partners. Coalition networks, and the information they contain must be the primary systems used by coalition partners, while national systems must be complementary in nature. Colonel George K. Gramer supports the development

---

[259] As alluded earlier (footnote 197), the "write for release" principle makes reference to the philosophy of writing intelligence reports so as to make them accessible to as many coalition partners as possible.

of multi-level secured IT networks which would allow coalition and national intelligence to be available on the same system.[260] The information would be protected through the use of firewalls allowing access only to the information for which the user is cleared and has a need to know. It would allow large providers of intelligence such as the U.S. military to have access to national and coalition IT architecture on the same system.

The coalition intelligence apparatus is dependant on a robust IT system available to all of the partners. This is a critical aspect of successful coalition operations.[261] It is clear to everyone who has studied coalition operations that they will not be fully interoperable unless the participating nations have all of the necessary mechanisms in place required to disseminate information and intelligence to all of their partners.[262] Anti-hacking mechanisms would have to be in place in order to guarantee the security and integrity of the more sensitive data. .

DEVELOPING A COALITION INTELLIGENCE COLLECTION PLAN

This is probably the most important recommendation of all the ones presented at the tactical and operational levels in that it has the potential to maximize the intelligence assets available to a coalition as well as allowing a unified effort in developing the vital theatre wide CIP. The development of a coalition intelligence collection plan, synchronized with the overall theatre coalition campaign plan, is a critical element.

---

[260] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 15 & Major Barret K. Peavie (US Army) "Intelligence sharing in Bosnia" *United States Army Command and General Staff College* (AY 00-01): 28.

[261] Colonel George K. Gramer Jr (U.S. Army) "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College* (17 May 1999): 13.

[262] *Ibid*., 12.

McCuen supports this concept when he writes that the joint exchange of intelligence is essential in fighting an insurgent effectively and that all intelligence-gathering agencies must be closely co-coordinated.[263] "Perhaps nearly as bad as no intelligence to organization, or a multiplicity of intelligence organizations, is an overloaded one."[264] This plan must also be synchronized with all coalition elements and not limited to conventional forces. It must include SOF elements as well as civilian intelligence agencies to the maximum extent possible. Coordinating theatre intelligence requirements through the development of a theatre intelligence campaign plan would avoid duplication of efforts and it would maximize the overall use of scarce intelligence resources.

The development of such a plan would also fulfill the requirement of the first phase of the intelligence cycle (direction) and facilitate the rest of the process for the coalition. A proper intelligence collection plan would provide the focus required by tactical collectors as well as leveraging the maximum amount of effort out of every coalition partner's intelligence capabilities. It would also provide the right type of environment required in order to develop target packages necessary for deliberate offensive planning which has been so important in conducting COIN operations. The development of an intelligence collection plan would also direct a strict allocation of intelligence areas of intelligence responsibilities (IAOR) between the coalition partners in order to focus their efforts geographically based on the overall limitations in resources and the location of the different national contingents.[265] The development of a coalition

---

[263] John McCuen. *The Art of Counter-Revolutionnary War: A Psycho-Politico-Military Strategy of Counter-Insurgency*. (Harrisburg: Stackpole Books, 1965), 115.

[264] Robert Thompson. Defeating Communist Insurgency: The Lessons of Malaya and Vietnam. (London: Chatto and Windus, 1966), 86.

intelligence collection plan would allow for a coalition intelligence apparatus to be focused, proactive and synergetic.[266]

The absence of such a plan would likely negatively impact the overall theatre campaign plan and provide significant obstacles to the effective coordination of the overall intelligence effort. Moreover, the absence of such a plan would also be counterproductive in that it would impede the intelligence coordination effort and deprive the establishment of critical coalition intelligence priorities. Coordinating the intelligence collection efforts by using all of the available intelligence assets remains the key objective in developing such a plan.

SUMMARY

This chapter has demonstrated that coalition intelligence sharing problems have to be tackled simultaneously at the strategic, operational and tactical levels. The coalition intelligence apparatus requires a major overhaul of its mechanisms and the solutions to the problems do not seem to lie in the conservative realm but through innovative changes that require a major change in the organizational culture and in the way that this function is perceived by other partners of the Defence team. The recommendations presented in this final chapter also indicated that a minimum level of trust and interoperability must be developed at all levels in order to guarantee the proper coordination of intelligence assets for the benefit of all of the coalition partners. Recommendations presented in this chapter call for the establishment of trust between coalition partners, for the use of an efficient classified IT network, for the development of policies and procedures, for the

---

[265] Canadian Special Operations Command, Confidential Source 009, *Telephone interview*, 26 February 2008.

[266] Lieutenant-Colonel G. Eanes USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005.

establishment of integrated multinational intelligence organizations, and for the development of a thorough intelligence collection plan.

CONCLUSIONS

This dissertation has demonstrated that tactical and operational intelligence sharing in modern military coalition is problematic but that solution exists in order to mitigate the problems. It has also highlighted that coalition intelligence organizations have attempted to adapt to the challenges of the COIN operations in Afghanistan with limited successes.

Taking today's operations in Afghanistan as a case study, the paper next examined how the battle situation had allowed for the development of a robust but complex coalition intelligence apparatus. The thesis highlighted the fact that the current intelligence system, despite admitted weaknesses, had many strengths that could not be ignored by future planners. Study of the specific ISAF and OEF intelligence architecture made it clear that although different versions of evaluating the security situation existed and true integration of intelligence assessments was still far from being achieved, effective progress towards a CIP had been one of the most important successes in intelligence sharing between coalition partners in Afghanistan. The development of a CIP can clearly be seen to require excellent communication between national contingents' intelligence organizations, and a genuine desire to contribute to the overall coalition intelligence effort.

This thesis also explored the many hurdles which can obstruct the creation of a CIP. Restrictive national regulations, old habits of over-classifying reports, IT limitations, lack of trust between some countries and/or individuals as well as a lack of vision on the part of some participating nations can all contribute to hampering the development of a CIP within a coalition environment. Proven solutions in the

Afghanistan case included the creation of intelligence liaison officer positions and of multinational intelligence organizations. It did not include an accepted coalition intelligence collection plan that could have greatly contributed to improve the level of coordination of the overall intelligence effort in country.

This research noted the fact that intelligence structures were directly linked to the concept of national interest. This implies that military and civilian intelligence organizations are both generally managed at the highest levels of government in order to avoid compromising national capabilities or exposing vulnerabilities. This dissertation also demonstrated that intelligence policies were driven at the strategic level and that these policies directly impacted how intelligence could be shared at the operational and tactical levels among coalition partners. The inevitable conclusion from this finding is that most of the problems identified with regards to intelligence sharing at the lower levels must involve strategic entities in the search and implementations of the solutions.

The existence of multinational organizations such as NATO and ABCA has allowed for some coalition intelligence doctrine and policies to be written. However, research revealed that these guidelines have not been followed religiously by nations comprising the current coalition in Afghanistan. On the contrary, nations such as the United States, Canada and Great Britain have continued to use their own classified national IT networks for the bulk of their operations instead of using the available coalition IT systems that were to join them with all other coalition partners. A lack of integration and interoperability between intelligence organizations complicated the development of an efficient coalition intelligence apparatus.

The concept of trust has been discussed throughout the paper and could arguably be acknowledged as the most important factor affecting intelligence sharing within a coalition. Trust must exist at the strategic level first in order for intelligence to be shared effectively with other partners. National level decision makers will normally dictate to what extent intelligence can be shared to another nation all the way down to the tactical level. Trust can also be developed during operations as well as during exercises, but intelligence organizations often support only their own national contingents on exercises. They rarely practice coalition intelligence procedures, much less train as part of a coalition intelligence organization. Such multinational exercises would have the potential to contribute significantly to establishing trust between the participating nations.

As shown by the research of this thesis, trust at the tactical and operational levels is also very important because the business of intelligence remains fundamentally based on individuals and not on machines or technical capabilities. Trust at the tactical and operational levels can be developed over time, based on personalities and affinities between individuals as well as on the level of openness allowed by the respective authorities. Trust is a critical aspect of intelligence sharing as much as intelligence sharing is a key element of trust. Sharing intelligence at the tactical and operational levels demonstrates shared interests and often goes a long way in creating strong relationships between coalition partners.

This paper highlighted the importance that the intelligence organizational culture has had on sharing intelligence with other coalition partners over the years. The events of 9/11 changed the way western intelligence organizations saw their role with one another and how they viewed the importance of effectively sharing intelligence. The old

organizational culture driven by secrecy and the "need to know" concepts have currently been overtaken by the principles of "write for release" and "need to share". Intelligence organizations found out they must adapt their operating procedures and methods to the realities of integration and of cooperation between services, agencies and states. These new principles are slowly taking root in places like Afghanistan but there remains a lot of work to be done.

Many intelligence officials interviewed during the research for this thesis argued that the best way to change the culture of an organization was through education. The U.S. and Canadian IC are currently looking at the creation of integrated all-source intelligence academies and universities. This approach to the problem, coupled with shorter-term solutions such as the creation of more exchange positions between agencies and the establishment of coalition intelligence procedures and policies would greatly contribute to improving interaction and exchanges between intelligence organizations.

This thesis has presented solutions to improve coalition intelligence sharing at the strategic, operational and tactical levels. In order to make these happen, somebody has to take the lead. Multinational initiatives exist between NATO and ABCA members but it seems that much remains to be done to integrate other potential coalition partners. The way ahead for intelligence sharing within the context of COIN and coalition warfare requires the more active countries to take the lead on the most important issues. NATO has been engaged through initiatives such as the Multinational Interoperability Council (MIC) but has few results to show for. The five ABCA countries have developed a coalition intelligence handbook, but have been unable to fully implement it during recent coalition operations in Afghanistan.

One option for further improvement sees the nations more prone to lead current and future coalitions taking the lead on these issues and developing the guidelines and the IT backbone required in order to conduct successful coalition operations. Members of the ABCA organization are arguably among the best organized and the most experienced nations with regards to intelligence sharing, and their expertise should be used to the fullest extent in order to allow for the development of universally accepted guidelines, policies, and methods for efficient coalition intelligence sharing. These guidelines also need to be exercised and practiced with the traditional and non-traditional partner countries who compose today's coalitions.

It is important to note that this thesis did not answer every aspect of the problems of intelligence sharing within the Afghan coalition. It also raised some questions that were outside the scope of the present research but would definitely need to be looked at in more detail in the future if one hoped to definitely improve intelligence sharing between coalition partners. Nonetheless, the research presented here offers viable and practical solutions to many of the most crucial problems of coalition intelligence sharing, based on a thorough exploration of the causes and nature of the difficulties. Most if not all of the suggestions outlined above could be put into practice in the near term, with an immediate positive effect on today's ongoing coalition operations in Afghanistan and potentially elsewhere. It is hoped that this vital area of warfare will receive the attention it deserves.

BIBLIOGRAPHY

PRIMARY SOURCES - INTERVIEWS

Belzile, Major J.Y. CD, Canadian Intelligence Liaison Officer to CENTOM HQ, *Interview*, 29 March 2007, Tampa Bay, United States. Subsequent interviews conducted by telephone on 2, 8 and 15 November 2007.

Bigras, Lieutenant-Colonel N. CD, J2 Intelligence Production CDI, *Interview*, 24 April, Ottawa, Canada.

Callacott, Captain J CD, Senior Analyst, All Source Intelligence Centre, Kandahar Airfield, (Jul 06-March 07), *Interview*, 24 May 2007, Bagotville, Canada.

Canadian Forces Information Operations Group

Confidential Source 001, *Interview*, 24 April 2006, Ottawa, Canada.

Canadian Forces Joint Task Force X

Confidential Source 008, *Interview*, 12 February 2005, Kabul, Afghanistan.

Canadian Security Intelligence Service

Confidential Source 004, *Interview*, 12 February 2005, Kabul, Afghanistan.

Canadian Special Operations Command,

Confidential Source 006, *Interview*, 27 April 2006, Ottawa, Canada.

Confidential Source 007, *Interview*, 31 October 2007, Ottawa, Canada.

Confidential Source 009, *Telephone interview*, 26 February 2008

Eanes, Lieutenant-Colonel G. USAF, Deputy CJ2X Combined Forces Command Afghanistan (February 2005-August 2005), *Interview*, 5 March 2005, Kabul, Afghanistan.

Ferguson, Lieutenant-Colonel H. CD, J2 International CDI, *Interview*, 30 January 2007, Ottawa, Canada.

Green, Major M., SO2, Officer Commanding UK National Intelligence Centre, Kabul Afghanistan (February 2005-August 2005), *Interview*, 7-8 April 2005, Kabul, Afghanistan.

Jensen, Lieutenant-Colonel G. CD, J2 Plans CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 27 April 2006, Ottawa, Canada.

Kruger, Jorgen, Director Intelligence Policies and Programs, CDI, *Interview*, 2 November 2007, Ottawa, Canada.

Leslie, Major-General A.B. CMM MSC MSM CD, former Deputy Commander International Security Assistance Force – Kabul, Afghanistan (August 2003-February 2004), *Interview*, 27 April 2006, Ottawa, Canada.

Natynczyk, Lieutenant-General W.J. CMM MSC CD, former Deputy Commanding General of the Multi-National Corps Iraq (Iraqi Freedom), *Interview*, 27 April 2006, Ottawa, Canada.

Neveu, Major S. CD, J2 Plans 2, CDI, *Interview*, 2 November 2007, Ottawa, Canada.

Nordick, Brigadier-General G.W. OMM MSM CD, Chief of Defence Intelligence (CDI), *Interview*, 24 April 2006, Ottawa, Canada.

Rigeway, Lieutenant-General A. OBE, United Kingdom Chief of Defence intelligence (CDI), *Interview*, 15 April 05, Kabul, Afghanistan and 22 March 2006, London, United Kingdom.

Rousseau, Colonel J.G.A.J.C., CD, Intelligence Branch Advisor and J2X CDI, *Interview*, 2 November 2007, Ottawa, Canada.

Semianiw, Colonel, W. OMM CD, former Commander Task Force Kabul, OP ATHENA Roto 3 (February 2005-August 2005), *Interview*, 3 March 05, Kabul, Afghanistan.

Thibault, Master Warrant Officer, M. MMM CD, Senior Analyst ASIC OP ATHENA Roto 3, *Interview*, 15 May 2005, Kabul, Afghanistan.

Thompson, Colonel D.H.N., OMM, CD, Director Intelligence Operations at CDI and former Canadian Forces Intelligence Liaison Officer detached to MOD UK, London, *Interview*, 24 April 2006, Ottawa, Canada.

Zegarac, Major D. CD, Deputy Chief Assessments, International Security Assistance Force Kabul Afghanistan, *Interview*, 20 November 2007, Bagotville, Canada.

PRIMARY SOURCES - GOVERNMENT AND MILITARY DOCUMENTS

ABCA (Armies of America, Britain, Canada and Australia, with New Zealand as an associate member)

Coalition Intelligence Handbook, Quadripartite Advisory Publication (QAP) Number 325, Edition 2, Dated July 2003.

Official Web page
http://www.abca-armies.org

Canadian Forces Publications

B-GJ-005-200FP-000, Joint Intelligence Doctrine, November 11, 2002.

B-GL-323-004/FP-003, Counter-Insurgency Operations, July 2007.

National Defence Security Instructions, NDIS 27 – Classification and Designation of Information,
http://vcds.mil.ca/cfpm/pubs/pol-pubs/ndsi/intro_e.asp

Government of Canada Publications

Government of Canada, *Government Security Policy*,
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/gsp-psg1_e.asp#acc

North Atlantic Treaty Organization (NATO)

NATO Allied Administrative Publication (AAP) 6 NATO Glossary of Terms and Definitions.
http://www.dtic.mil/doctrine/jel/other_pubs/aap_6v.pdf

ISAF Home Page
http://www.nato.int/isaf

United Nations

Resolution 1386 (2001), Adopted by the Security Council at its 4443rd meeting, 20 December 2001.

United States Government Publications

National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report" 22 July 2004.
http://www.9-11commission.gov/report/911Report.pdf

U.S. Department of the Army and U.S. Department of the Navy. *The U.S. Army and Marine Corps Counterinsurgency Field Manual – U.S. Army FM-3-24 – Marine Corps Warfighting Publication No.3-33.5*. Chicago: The University of Chicago Press, 2007.

U.S. Intelligence Community. "500 Day Plan: Integration and Collaboration" 10 October 2007. http://www.dni.gov/500-day-plan/500-day-plan.pdf

U.S. Joint Chiefs of Staff, "Joint and National Intelligence Support to Military Operations" Joint Publication 2-01, 7 October 2004.

SECONDARY SOURCES – BOOKS

Allen, R.E. ed. *The Concise Oxford Dictionary of Current English*. Oxford: Oxford University Press, 1990.

Becket, Ian et al. *Modern Counter-Insurgency*. Burlington: Asgate Publishing Limited, 2007.

Clausewitz, Carl Von. *On War*. New Jersey: Princeton University Press, 1976.

Delamotte, Bruno. *Questions d'intelligence: le renseignement face au terrorisme*. Paris: Éditions Michalon, 2004.

Galula, David. *Counter-Insurgency warfare: Theory and Practice*. New York: Frederick A. Praeger, 1964.

Gross Stein, Janice and Eugene Lang. *The Unexpected War: Canada in Kandahar*. Toronto: Viking Canada, 2007.

Handel, Michael I. ed. *Intelligence and Military Operations*. Portland: Frank Cass, 1990.

Haycock, Ronald et al. *Regular Armies and Insurgency*. London: Croom Helm, 1979.

Herman, Michael. *Intelligence Power in Peace and War*. Cambridge University Press, 1996.

------. *Intelligence Services in the Information Age*. New York: Frank Class Publishers, 2005.

Jones, Seth. *Counterinsurgency in Afghanistan*. Santa Monica, CA: RAND Corporation, 2008.

Keegan, John. *Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda*. Toronto: Key Porter Books, 2003.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Hamden: Anchon Books, 1965.

McCuen, John. *The Art of Counter-Revolutionnary War: A Psycho-Politico-Military Strategy of Counter-Insurgency*. Harrisburg: Stackpole Books, 1965.

Scales, Major-General Robert H. Jr. *Future Warfare Anthology*. Carlisle's Barracks, PA: U.S. Army War College, 2000.

Schein, Edgar H.. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass Publishers, 1992.

Shulsky, Abram N. & Schmitt, Gary. *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. Washington D.C.: Potomac Books, 2002.

Stafford, David and Rhodri Jeffreys-Jones (Eds.). *American-British-Canadian Intelligence Relations 1939-2000*. London: Frank Cass, 2000.

Steele, Robert David, *The New Craft of Intelligence. Personal, Public and Political. Oakton*, Virginia: OSS International Press, 2002.

Sun, Tzu. *The Art of War*, (trans. Samuel B Griffith), Oxford: Oxford University Press, 1971.

Thompson, Leroy. *The Counterinsurgency Manual*. London: Greenhill Books, 2002.

Thompson, Robert. *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam*. London: Chatto and Windus, 1966.

Trinquier, Roger. *Modern Warfare: A French View of Counterinsurgency*. New-York: Praeger, 1964.

Weale, Adrian. *Secret Warfare*. London: Hodder & Stoughton, 1997.

SECONDARY SOURCES – ARTICLES, BOOK CHAPTERS AND OTHER WORK

Agence France Presse. "Australian PM: US Intelligence Agencies Reluctant to Share Information on Iraq" *Agence France Presse*, 4 October 2006. http://www.globalsecurity.org/intell/library/news/2006/intell-061004-voa01.htm

Andres, William, Wills, Craig, and Griffith, Thomas E. Jr. "Winning with Allies: The Strategic Value of the Afghan Model" *International Security*, Vol 30, no.3 (Winter 2005/2006):124-160.

Aylwin-Foster, Brigadier Nigel, "Changing the Army for Counterinsurgency Operations" *Military Review*, (November-December 2005):2-15.

Bailey, Mass Communication Specialist 1st Class Jessica M., "CENTRIXS Provides Vital Communication" *Navy NewsStand*, 16 July 2007.

Bialos, Jeffrey P. and Koehl, Stuart L. "The NATO Response Force: Facilitating Coalition Warfare Through Technology Transfer and Information sharing" *Center for Technology and National Security Policy – National Defense University*, September 2005.

Boardman, Special Agent Chase H. "Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction" *Joint Forces Staff College – Joint Advanced Warfighting School*, 31 May 2006.

Boykin, Lieutenant-General William G. (USA) "Intelligence Support to Allied and Coalition Operations" *16th Annual SO/LIC Symposium on Strategic Environment for Coalition Warfare*, 3 Feb 2005.

Brendenkamp, Major Michele H. (U.S. Army). "How Can the U.S. Army Overcome Intelligence Sharing Challenges Between Conventional and Special Operations Forces?" *School of Advanced Military Studies – U.S. Army Command and General Staff College*, AY 2002-2003.

British Broadcasting Corporation "*Zarqawi killed in Iraq air raid*" *BBC News* (June 8, 2006) http://news.bbc.uk/2/hi/middle_east/5058304.stm. consulted on 15 November 2009.

Bumiller, Elisabeth. "Petraeus Warns About Militants' Threat to Pakistan" New York Times (1 April 2009) http://www.nytimes.com/2009/04/02/washington/02military.html. consulted on 12 April 2009.

Clough, Chris. "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation" *International Journal of Intelligence and CounterIntelligence*, Vol 17 (2004):601-613.

Cody, General Richard A. and Maginnis, Robert. "Coalition Interoperability: ABCA's New Focus" *Military Review*, (November-December 2006):65-68.

Cohen, Eliot, Crane, LCol Conrad, Horvath, LCol Jan and Nagl, LCol John. "Principles, Imperatives and, Paradoxes of Counterinsurgency" *Military Review*, (March-April 2006):49-53.

Cordesman, Anthony H. "The Ongoing Lessons of Afghanistan: Warfighting, Intelligence, Force Transformation, and Nation Building" *Center for Strategic and International Studies*, 6 May 2004. http://www.csis.org/media/csis/pubs/afghanlessons.pdf

de B. Taillon, Colonel, Paul J. "Some of the Challenges of Multinational Force Command" *New Zealand Journal of Defence Studies*, Vol 1, March 2007.

------. "Coalition Special Operation Forces: Building Partner Capacity" *Canadian Military Journal*. Vol 8, no.3 (Autumn 2007):45-54.

Eikenberry, Lieutenant-General, Karl. "Lt. Gen. Eikenberry Holds Defense department News Briefing" Washington Post, 21 September 2006. www.washingtonpost.com/wp-dyn/content/article/2006/09/21/AR2006092100915.html

Gerleman, David and Stevens, Jennifer E. "Operation Enduring Freedom: Foreign Pledges of Military & Intelligence Support" *Report to the Congress*, 17 October 2001.

Gramer, Colonel George K. Jr (U.S. Army). "Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders have an Intelligence Dissemination Challenge" *Naval War College*, 17 May 1999.

Hilder, Colonel Terence, J. "Interagency Reform: Changing Organizational Culture Through Education and Assignment" *United States Army War College*, 30 March 2007.

Howcroft, James R.. "Technology, Intelligence and Trust" *Joint Forces Quarterly*, Vol 46, no.2 (2007):20-26.

Jones, Seth. "The Rise of Afghanistan's Insurgency: State failure and Jihad" *International Journal*, Vol. 32, no 4 (Spring 2008), 8.

Kilcullen, David. "Counterinsurgency *Redux*" *Small War Journal* (July 2006) http://www.smallwarsjournal.com/documents/kilcullen1.pdf

Krulak, General Charles C. "The Strategic Corporal: Leadership in the Three Block War" *Marines Magazine* (January 1999).

Lefebvre, Stéphane. "The Difficulties and Dilemmas of International Intelligence Cooperation" *International Journal of Intelligence and CounterIntelligence*, Vol 16 (2003):527-542.

Maginnis, Robert. "ABCA: A Petri Dish for Multinational Interoperability" *Joint Forces Quarterly*, Vol 37, no.2 (2005):53-58.

Manning, Lieutenant-Colonel Steve (USMC). "Improved Intelligence Support to our Coalition Partners at the Operational Level" *Naval War College*, 9 May 2004.

McLuhan, Stephanie. "One Issue, Two Voices. Intelligence Sharing between Canada and the United States: A Matter of National Survival" *International Journal of Intelligence and CounterIntelligence,* Issue 6 (January 2007):1-15.

Meigs, Montgomery C. "Unorthodox Thoughts about Asymmetric Warfare" *Parameters,* (Summer 2003):4-18.

Metz, Steven and Millen, Raymond. "Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response" *US Army War College - Strategic Studies Institute* (November 2004).

Metz, Steven. "New Challenges and Old Concepts: Understanding 21st Century Insurgency" *Parameters,* Vol 37, Issue 4 (21 December 2007):20-32.

Miles, Dona. "Information Access Key in Terror War, CENTCOM General Says" *American Forces Press Service*, 31 March 2005.

Norton-Taylor, Richard. "Coalition of the unwilling" *The Guardian,* 7 November 2007. http://www.guardian.co.uk/afghanistan/comment/story/0,,2206425,00.html

Patrick, Melissa, Intelligence "Intelligence in Support of Peace Operations: The Story of Task Force Eagle and Operations Joint Endeavour" *Army War College,* 10 April 2000.

Peavie, Major Barret K. (US Army). "Intelligence sharing in Bosnia" *United States Army Command and General Staff College* (AY 2000-2001).

Rexton Kan, Paul. "Counternarcotics Operations within Counterinsurgency: The Pivotal Role of Intelligence" *International Journal of Intelligence and CounterIntelligence*, Vol 19 (2006):586-599.

Ricassi, Robert. "Principles for Coalition Warfare" *Joint Forces Quarterly,* Vol 1, no.1 (1993):58-71.

Rudner, Martin. "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism" *International Journal of Intelligence and CounterIntelligence*, Vol 17 (2004):193-230.

Shafran, Captain Stacie. "Joint Intelligence Operations Center opens in Kabul" Air Force Link (29 January 2007). http://www.af.mil/news/story.asp?id123039140

Sherwood-Randall Elisabeth. "The Case for Alliances" *Joint Forces Quarterly*, Issue 43, (2006):54-59.

Sims, Jennifer E. "Foreing Intelligence Liaison: Devils, Deals, and Details" *International Journal of Intelligence and CounterIntelligence*, Vol 19 (2006):195-217.

Slackman, Michael & Shane, Scott. "Terrorist Trained by Zarqawi Went Abroad, Jordan Says" *The New-York Times*, 11 June 2006. http://www.nytimes.com/2006/06/11/world/middleeast/11jordan.html

Spiegel, Peter. "Pentagon Chief Orders Staff to Give Allies Better Access to Classified data" *Financial Times*, 3 June 2005. www.ft.com/cms/s/03b2c382-d3cd-11d9-ad4b-00000e2511c8.html

Steele, Robert David, "The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats". *Strategic Studies Institute – Army War College* (February 2002).

Thibault, Gaétan & Gareau, Lieutenant-Colonel M., & Le May, François, "Intelligence collation in asymmetric conflict: A Canadian armed forces perspective" *System of Systems Section, Defence R&D Canada Valcartier, Canada* (July 2007).

Wilson, J.R. "Expanded use of advanced communications technology is enabling nearly instantaneous delivery of vital military information" *Aerospace America Online* (October 2003). http://www.aiaa.org/aerospace/Article.cfm?issuetocid=418&ArchiveIssueID=43