Help a brother out : a case study in multinational intelligence sharing, NATO SOF

Ara, Martin J.; Larsse, Brage Andreas.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HELP A BROTHER OUT: A CASE STUDY IN MULTINATIONAL INTELLIGENCE SHARING, NATO SOF

by

Martin J. Ara
Thomas Brand
Brage A. Larssen

December 2011

Thesis Advisor:	David Tucker
Second Reader:	Timothy Doorey

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2011	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Help a Brother Out: A Case Study in Multinational Intelligence Sharing, NATO SOF	5. FUNDING NUMBERS
6. AUTHOR(S) Martin J. Ara, Thomas Brand, and Brage A. Larssen	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis examines how to optimize intelligence sharing in a coalition by a thorough literature review and site visits to intelligence sharing organizations in order to establish best practices for multinational intelligence sharing. The newly established NATO SOF Headquarters (NSHQ) in Mons, Belgium was treated as a test case to validate their intelligence sharing procedures and structures in reference to the authors' identified best practices: mutual gains and benefits; trust; direct control; and accessibility and interoperability.

Intelligence support to SOF is a *decisive* factor, when in conventional operations it often is not; therefore intelligence support to SOF is special - NATO SOF is no exception. The level of intelligence support to SOF normally only exists at the national level, due to bureaucratic obstacles, a need to protect sensitive sources and capabilities, and lack of trust. The NSHQ is experimenting with several innovative methods to enhance trust and streamline intelligence capability amongst NATO SOF forces. There are structural and organizational lessons learned from the establishment of the NSHQ that can be applied to future operations and coalitions.

14. SUBJECT TERMS NATO SOF, NSCC, NSHQ, Special Operations Interoperability, Military Networks, NATO Transformation, European Common Threats, NATO Training and Education Program-NSTEP, BICES Network, Afghanistan Special Operations, ISAF SOF, Intelligence Sharing, Multinational Operations, Intelligence, Coalitions.	15. NUMBER OF PAGES 72
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HELP A BROTHER OUT: A CASE STUDY IN MULTINATIONAL INTELLIGENCE SHARING, NATO SOF

Martin J. Ara
Lieutenant, United States Navy
M.S., London School of Economics, 1999

Thomas Brand
Lieutenant Colonel, German Army
B.S., University of the German Federal Armed Forces Munich, 1995

Brage Andreas Larssen
Major, Norwegian Army
B.S., Norwegian Military Academy, Oslo, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Martin J. Ara
Thomas Brand
Brage A. Larssen

Approved by: David Tucker
Thesis Advisor

Timothy Doorey
Second Reader

John Arquillia
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines how to optimize intelligence sharing in a coalition by a thorough literature review and site visits to intelligence sharing organizations in order to establish best practices for multinational intelligence sharing. The newly established NATO SOF Headquarters (NSHQ) in Mons, Belgium was treated as a test case to validate their intelligence sharing procedures and structures in reference to the authors' identified best practices: mutual gains and benefits; trust; direct control; and accessibility and interoperability.

Intelligence support to SOF is a *decisive* factor, when in conventional operations it often is not; therefore intelligence support to SOF is special - NATO SOF is no exception. The level of intelligence support to SOF normally only exists at the national level, due to bureaucratic obstacles, a need to protect sensitive sources and capabilities, and lack of trust. The NSHQ is experimenting with several innovative methods to enhance trust and streamline intelligence capability amongst NATO SOF forces. There are structural and organizational lessons learned from the establishment of the NSHQ that can be applied to future operations and coalitions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BICES	Battlefield Information, Collection, and Exploitation System
C4I	Command, Control, Communications, Computers, and Intelligence
CIA	Central Intelligence Agency
CJFSOCC	Combined Joint Forces Special Operations Component Command
COTS	Commerical Off the Shelf
CSOF	Coalition Special Operations Forces
DA	Direct Action
FID	Foreign Internal Defense
HUMINT	Human Intelligence
ISAF	International Service and Assistance Force
JIATF-South	Joint Interagency Task Force-South
JIOC	Joint Intelligence Operations Center
JFC	Joint Force Command
MILDEC	Military Deception
MOOTW	Military Operations Other Than War
NATO	North Atlantic Treaty Organization
NIC	National Intelligence Cell
NSCC	NATO SOF Coordination Center
NSTEP	NATO SOF Training and Education Program
OPSEC	Operational Security
PIFC	Pentagon Intelligence Fusion Center
PSYOPS	Psychological Warfare
SACEUR	Supreme Allied Commander, Europe

SIGINT	Signals Intelligence
SOF	Special Operations Forces
SOIB	Special Operations Intelligence Branch
SOTG	Special Operations Task Group
SOCOM	(United States) Special Operations Command
SOCEUR	(United States) Special Operations Command Europe
TTPs	Tactics, Training, and Procedures
UW	Unconventional Warfare
VSO	Village Stability Operation

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to thank our supervisor, Dr. David Tucker, for his thorough knowledge of intelligence and support throughout this project, CAPT Tim Doorey, USN (ret.), whose insight inspired our research. We would also like to thank Dr. Chris Lamb of the National Defense University for the generous amount of time he granted us, and the staffs at the Pentagon Intelligence Fusion Center (PIFC) and the NATO SOF Headquarters for showing us a way ahead. This thesis would not have been possible without their support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> The foundation of United States, regional, and global security will remain America's relations with our allies, and our commitment to their security is unshakable. These relationships must be constantly cultivated, not just because they are indispensible for U.S. interests and national security objectives, but because they are fundamental to our collective security. Alliances are force multipliers: through multinational cooperation and coordination, the sum of our actions is always greater than if we act alone… we will continue to mutually benefit from the collective security provided by strong alliances.
>
> President Barack Obama[1]

> The changing security environment requires the Joint Force to deepen security relationships with our allies.[2]
>
> National Military Strategy of the United States

A. OVERVIEW

NATO's essential purpose is to safeguard the freedom and security of all its members via political and military means in accordance with the North Atlantic Treaty and the principles of the United Nations Charter.[3] "There is a common perspective among a variety of defense and security establishments around the world that the nature of the current and future security environment we face presents complex and irregular challenges that are not readily apparent and are difficult to anticipate."[4] SOF is being singled out and recognized as a key

---

[1] President Barack Obama, "The National Security Strategy," Washington, 2010, 41, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed November 4, 2011).

[2] Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," Washington, February 8, 2011, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed February 24, 2011).

[3] North Atlantic Treaty Organization, "NATO's New Strategic Concept," November 19, 2010, 18, http://www.nato.int/strategic-concept/index.html (accessed February 24, 2011).

[4] North Atlantic Treaty Organization Special Operations Coordination Centre (NSCC), "The North Atlantic Treaty Organization Special Operations Forces Study," December 4, 2008, ii. http://www.nshq.nato.int/NSHQ/GetFile/?File_ID=29 (accessed February 24, 2011).

component of the North Atlantic Treaty Organization (NATO) alliance in the fight against contemporary and future threats, because SOF is "ideally suited to [the] ambiguous and dynamic irregular environment" facing NATO.[5]

SOF has traditionally been considered a national asset. NATO had no history of utilizing SOF in the Alliance when NATO nations first assumed responsibility for the conflicts in the Balkans. However the lessons learned during those conflicts were not applied due to a lack of a central NATO SOF entity until the NATO Riga summit of 2006. On December 22, 2006, Admiral William McRaven was appointed Director of the NATO SOF Coordination Center (NSCC) and ordered to start the transformation process. Three years later, on March 1, 2010, the NATO SOF Headquarters (NSHQ) was formally established as a three-star headquarters within the Alliance in Mons, Belgium.[6]

According to its mission statement, the purpose of NSHQ is twofold. First, it must optimize the employment of SOF by the Alliance. NSHQ further describes this as "the intention to make the employment of SOF as perfect, efficient, and effective as possible, so as to deliver to the Alliance a highly agile Special Operations capability across the range of military operations."[7] Second, it must provide a command capability when so directed by Supreme Allied Commander Europe (SACEUR). NSHQ further describes this as "the ability to deploy a robust C4I capability and enablers for the support and employment of SOF in NATO operations."[8] To be able to carry out successful special operations in support of the current and future operating environments, the Alliance needs adequate interoperability, command and control, and intelligence structures.

Even amongst the closest allies, challenges in intelligence sharing remain. During the early years of Operation Iraqi Freedom, British operators were denied access to intelligence fused by the U.S. that the British had gathered themselves.

---

5 NSCC, "The North Atlantic Treaty Organization Special Operations Forces Study," ii.

6 NATO Special Operations Headquarters, "Biennial Review," January 2010, 6.

7 Ibid., 1.

8 Ibid., 1.

The issue became so contentious that it had to be raised by British and Australian Prime Ministers with the U.S. President to be resolved.[9] Having realized that intelligence sharing is always a compromise between the need to share and the need to protect (even with the best-designed organizations, much less a large, multinational, bureaucratic organization), the NSHQ has developed an innovative approach to solving its intelligence deficiencies. It has created its own organic intelligence collection, analysis, and exploitation capability. It has also acquired its own equipment and created a robust NATO SOF training facility and training program to supplement intelligence flow to NATO SOF forces. !

B. BACKGROUND

Special operations often test the limits of both equipment and personnel. This extremity introduces a significant degree of uncertainty or "fog of war." Success in special operations dictates that the uncertainty associated with the enemy, weather, and terrain must be minimized through access to best available intelligence.[10] Most special operations conducted nationally benefit from access to the best national intelligence available. However, because of classification issues, special operations by international coalitions often lack access to the best available intelligence. This absence increases the likelihood of operational failure and further risks the personal safety of the operators.

NATO (and many of the individual member states) foresees a future threat environment shaped by unconventional threats such as transnational crime, terrorist attacks, and the proliferation of weapons of mass destruction.[11] There are so many similarities in threats projected by the NATO member states and by official NATO strategy it is easy to conclude that a common enemy exists: transnational problems require transnational solutions. The complexities in the international order and the "significant challenges to the intelligence system [that]

---

[9] Bob Woodward, *State of Denial* (New York: Simon and Schuster, 2006), 318–319.

[10] William McRaven, *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice* (Novato, CA: Presidio Press, 1996).

[11] North Atlantic Treaty Organization, "NATO's New Strategic Concept," 18.

arise in targeting groups such as al-Qaeda due to their networked and volatile structure"[12] make multinational intelligence sharing requisite. There is much to gain from multinational cooperation. The expected continued decline in military budgets and limited SOF human resources make burden-sharing and proper division of labor even more appropriate.

C. PURPOSE AND SCOPE

Intelligence is a decisive factor, sometimes *the* decisive factor, in special operations. As such, the NSHQ's ultimate success will rely on its ability to solve some of the perennial problems related to intelligence sharing within coalitions. The newly established NSHQ in Mons, Belgium serves as an excellent testing ground to analyze SOF intelligence sharing issues within a coalition. NSHQ is attempting to streamline and optimize the intelligence available to NATO SOF units.

The scope of this research will be limited to NATO SOF nations, with particular emphasis on why the NSHQ has created its particular organizational structures, procedures, manning requirements, and training programs to improve the intelligence picture available to the SOF operator. We will focus on the headquarters element, not the tactical or operational levels in current operations in Afghanistan.

D. RESEARCH QUESTION

As depicted in Figure 1, NATO SOF has a detailed doctrine for inputs into the intelligence process for operational units arriving from a variety of sources both NATO and national.

[12] Lawrence E. Cline, "Special Operations and the Intelligence System," *International Journal of Intelligence and Counterintelligence* 8, no. 4 (2005): 579.

Figure 1. Current NATO SOF Intelligence Support Architecture for Operations[13]

NSHQ realizes that there are limits to the intelligence that can or will be shared in a large coalition environment. Because there are limitations to the doctrinal approach, the NSHQ is developing procedures, acquiring equipment, and creating a NATO SOF intelligence curriculum. This work facilitates an intelligence-sharing framework that does not rely exclusively on national or NATO structures to supplement intelligence support to NATO SOF operations.

In this thesis, the authors will examine whether the NSHQ is optimized for intelligence sharing in a coalition environment. The goal of this thesis is to determine the most effective way for NATO SOF to enhance operational performance and increase operator safety through intelligence sharing.

[13] NATO SOF Coordination Center, *Special Operations Task Group Manual v1.0*, December 2009, 6-2.

E. CONCEPTUAL AND RELEVANT LITERATURE

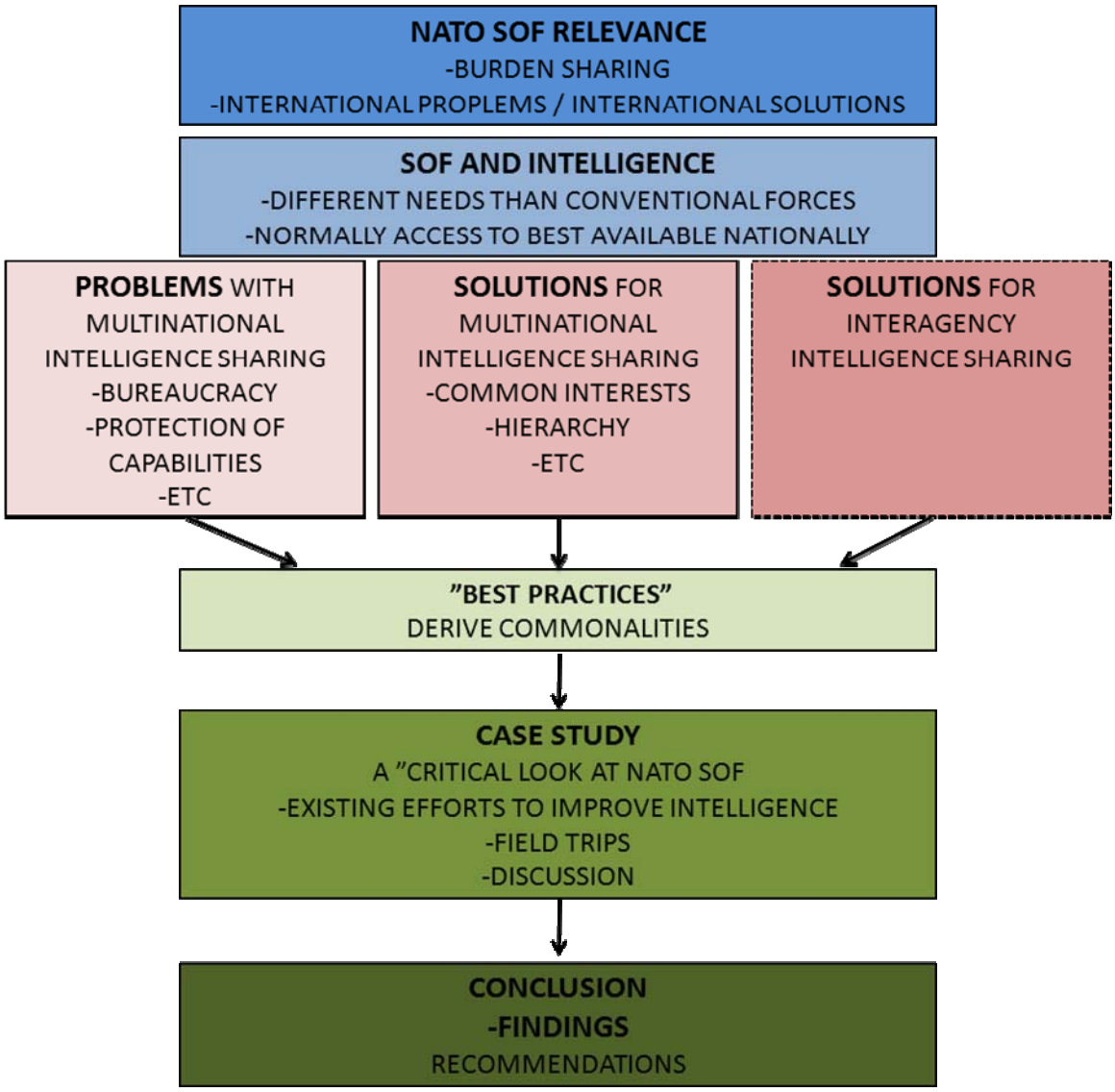
There is little unclassified literature measuring the effectiveness of international intelligence sharing on military operations, and almost no literature on international intelligence sharing in SOF operations. There is no body of scholarly literature available on intelligence sharing in NATO. For this thesis, the authors will draw on organizational design literature and examine several types of multinational and intelligence organizations and U.S. interagency operations to draw parallels and lessons learned in order to recommend best practices.

F. THEORETICAL FRAMEWORK AND METHODOLOGY

We will identify best practices by conducting a literature review and field studies of intelligence sharing and by conducting a gap analysis with observed NSHQ procedures to determine whether the NSHQ is operating optimally, and if not, we will make recommendations for improvement.

The theoretical framework for this research seeks to understand the critical role that intelligence plays in special operations, how intelligence sharing facilitates successful coalition special operations, and the best structures and conditions for intelligence sharing. To do this, we will look at some historical examples. The "Five Eyes" agreement among the U.S., UK, Australia, Canada, and New Zealand dating from the early Cold War is the first significant historical multinational intelligence-sharing agreement.[14] In the post-Cold War era, NATO countries have been operating in a multinational framework for conflicts, such as those in Somalia, the Balkans, and Afghanistan. The literature review, field studies, and discussions with subject matter experts will be the foundation for our analysis. This foundation describes problems and solutions for intelligence sharing. Figure 2 demonstrates our framework and methodology.

[14] The National Security Agency, "Declassified UKUSA Signals Intelligence Agreement Documents Available," The National Security Agency, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml (accessed November 4, 2011).



!

Figure 2. Theoretical Framework and Methodology

!

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTELLIGENCE SUPPORT TO SPECIAL OPERATIONS: WHY SOF IS DIFFERENT

> The nature of many SOF objectives and tactics requires intelligence support that is frequently more detailed than that needed in conventional operations.[15]
>
> Joint Publication 3-05

> SOF need intensive and comprehensive study of their targets. U.S. SOF prepared for Grenada with maps roughly on a par for inadequacy with those used by the British in Gallipoli. The contrast between the excellent intelligence available to French forces in Algeria and the almost always inadequate, or just nonexistent, intelligence available in Indochina illustrates the point. Special operations cannot succeed without good intelligence; in common with tactical surprise it is close to constituting an absolutely necessary condition for operational success.[16]
>
> Colin Gray

A. INTRODUCTION

In February 1942, Allied intelligence learned that Germany had stepped up production of heavy water in a heavily guarded facility in occupied Norway. Heavy water is used in the production of nuclear material. Afraid that Germany was developing an atomic weapon, the British drew up plans to destroy the plant after conventional bombing operations failed. Nine Norwegian commandos trained by the British Special Operations Executive, under cover of night, surreptitiously entered the facility, went to the exact location of the heavy water cylinders and destroyed the stockpile. Because they had precise intelligence, the commandos knew exactly where to go; they had trained on full-scale mock-ups of the facility. Their intelligence was so accurate that they even knew the

[15] U.S. Joint Chiefs of Staff, Joint Publication 3-05, 1998, V-2.

[16] Colin Gray, "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *Parameters*, Spring 1999, http://www.carlisle.army.mil/USAWC/parameters/Articles/99spring/gray.htm (accessed March 14, 2011).

location of the keys needed to lock up the night watchman.[17] Upon conclusion of the mission, the team reported back to their headquarters in London: "Operation carried out with complete success. High-concentration plant completely destroyed. No suspicions aroused and no shots exchanged. Greetings."[18]

As with many special operations, intelligence was the *decisive* factor in this operation. Without access to the critical intelligence about the facility, even the best-trained and equipped operators would have faced a significantly higher probability of failure. This chapter describes why special operations forces have special intelligence requirements for success.

B. BACKGROUND

It is commonly stated that intelligence support to SOF operations is critical for mission success, yet the literature never discusses in detail why this is so. Most accept that intelligence is critical for SOF is self evident.[19] Is intelligence for special operations different from intelligence for conventional units? In other words, is intelligence for special operations "special?" If intelligence for SOF (and NATO SOF by extension) is "special," then it is imperative that the NSHQ develop the proper tactics, training, and procedures (TTPs) and acquire the correct intelligence equipment and systems to create the most appropriate possible intelligence support. Intelligence support to special operations is "special" in that intelligence is often a *decisive* factor in the planning and execution of a special operation, where in conventional operations it is not.

Special operations are high-risk ventures with the expectation of a high payoff in return. Often a nation's prestige is also at stake. The operations are frequently conducted on the margins of what is possible, and therefore, the

---

[17] Russell Miller, *Behind the Lines: the Oral History of Special Operations in World War II* (New York: St. Martin's Press, 2002), 107–15.

[18] Ibid., 115.

[19] Even the Army Field Manual for intelligence support to Army SOF spends only two short paragraphs discussing why intelligence is critical for SOF operations. See Army Field Manual 3-05.102, *Army Special Operations Forces Intelligence*, 2001, v.

operational environment is often uncertain. In these situations, "successful special operations are dramatically influenced by the commander's ability to make the right decision, at the right time."[20] To reduce uncertainty and to facilitate decision making, intelligence plays a key role. If a commander can get access to timely, relevant, accurate, and detailed intelligence, it will simplify decision-making and increase the possibility of mission success. Lawrence E. Cline describes SOF as "voracious consumers of intelligence."[21] SOF normally needs access to best available intelligence during planning and operations.[22]

There are two broad categories of special operations: direct special operations and indirect special operations. This chapter will examine intelligence support to both types, but will focus on the direct type, sometimes called commando operations. While the types of intelligence support to SOF required for both operations are different, SOF has unique intelligence requirements for each in the granularity of detail and focus, which are distinct from conventional intelligence requirements.

Intelligence support to special operations is different from intelligence support to conventional operations. According to the U.S. Army Special Operations Forces Intelligence Manual (FM 3-05.102), there are three main differences, as follows:

First, the complex missions, the intricate planning, and the decentralized execution of SOF missions require a greater level of intelligence detail than does a conventional operation. Due to their small footprint, for SOF the "mission hinges upon having a key bit of knowledge at a specific time or event."[23] The relatively small size and autonomy of SOF forces requires intelligence inputs to the planning, training, and execution portions of an operation.

---

[20] Army Field Manual 3-05.102, 2-1.

[21] Cline, "Special Operations and the Intelligence System," 576.

[22] See McRaven, *Spec Ops: Case Studies in Special Operations Warfare.*

[23] Army Field Manual 3-05.102, 2–5.

Second, given the high risk of strategic consequences of failure and the uncertainty of the operational environment, timeliness and accuracy of the information for special operations are more crucial than for a conventional operation. SOF commanders need extremely detailed intelligence to help make the go/no go decision.

Third, the sensitivity of and need for very detailed information requires direct interface between the personnel conducting a mission and the intelligence personnel. Due to the reliance on relative superiority (see below for an elaboration of this term) in most SOF operations, intelligence collection and analysis must support efforts to maintain surprise, military deception (MILDEC), and operational security (OPSEC).[24]

C. RELATIVE SUPERIORITY AND THE THEORY OF SPECIAL OPERATIONS

For commando operations, "relative superiority" is a critical concept. According to Admiral William McRaven, "relative superiority is a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well-defended enemy."[25] McRaven argues that relative superiority is brought about by several factors, which allow a mission to overcome, for a limited period of time, the "frictions of war" at the pivotal or decisive moment in an engagement. SOF forces with cutting edge technology, national level intelligence, and high-quality training can minimize the frictions of war and achieve relative superiority. McRaven defines the frictions of war as chance, uncertainty, and will of the enemy. According to McRaven, six principles of special operations allow SOF to achieve relative superiority: simplicity, security, repetition, surprise, speed, and purpose. The principles work because they reduce warfare to its simplest level and limit chance, uncertainly, and the

[24] Army Field Manual 3-05.102, 2-4–2-5.

[25] McRaven, *Spec Ops: Case Studies in Special Operations Warfare*, 4.

enemy's will. Achieving relative superiority is possible for small but not for large forces, as large forces are unlikely to be able keep all of the principles in balance.[26]

To achieve relative superiority, SOF must take into account the principles during the three phases of an operation: planning, preparation or training, and execution. Good intelligence is important during all phases of an operation and affects all of the principles. Without good intelligence, it is impossible to develop a plan that maximizes the probability of achieving relative superiority. Without a good plan, the likelihood of achieving relative superiority during the execution phases is lessened.

The inherent weakness of SOF is their lack of firepower relative to a larger, conventional force.[27] A larger force, by definition, does not require relative superiority to succeed since by its sheer numbers it cannot be overwhelmed by a smaller force. Therefore, a smaller force must look for other factors that will allow it to succeed. The smaller the attacking force, the greater the level of intelligence required for inputs into the planning process. A smaller force cannot rely on just firepower to overcome an opponent. This is where SOF must look for competitive advantage, such as through technology and surprise, over the numerically larger and better-defended force. All things being equal, both a large force and a small force would like to have perfect intelligence, but without high quality intelligence, the chances of failure rise more rapidly for the smaller force. A larger attacking force generally requires less detailed intelligence, because they are not relying on the principle of relative superiority to overcome a size deficit; a larger force is relying on numerical superiority. Even if a SOF force is relying on technology or specialized training to overwhelm a larger force, intelligence is critical for the design of the technology or training program. Figure 3 depicts this phenomenon. Operations on the left-hand side require intelligence with a higher degree of detail for success. As an operation moves

[26] McRaven, *Spec Ops: Case Studies in Special Operations Warfare*, 5–8.

[27] Ibid., 6.

further to the right and becomes larger, it needs less detail and lower intelligence fidelity to succeed because it will not rely on relative superiority to overcome a size deficit. Therefore, if a force is small and relying on relative superiority, it had better have good intelligence to use in the planning, training, and execution phases.

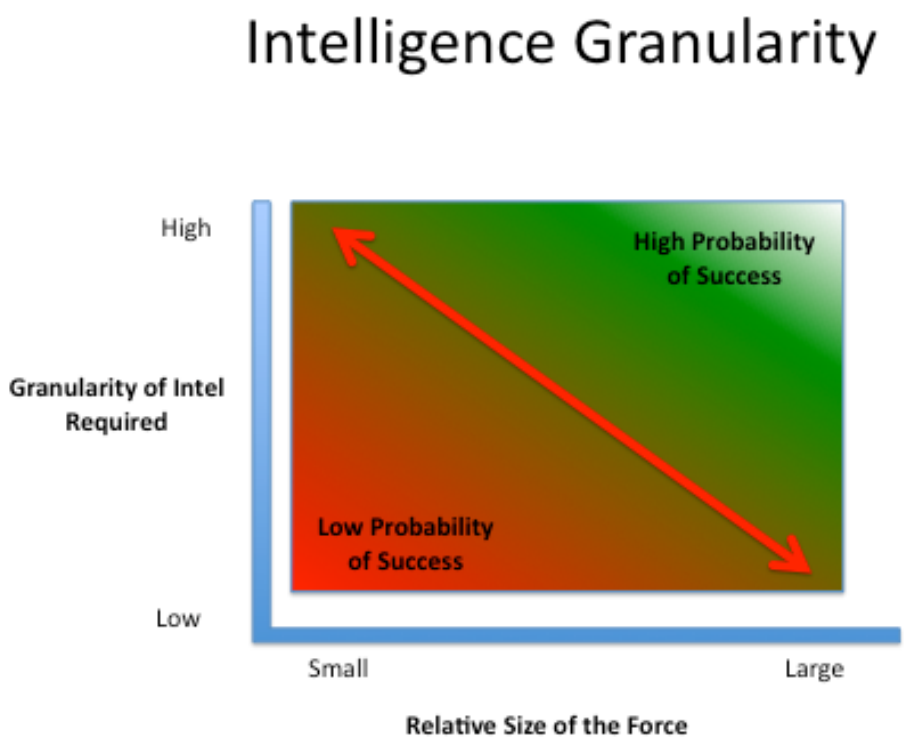


Figure 3. Intelligence Granularity

D. THE DIRECT APPROACH

The Italian manned torpedo attack in Alexandria Harbor, Egypt in 1941 is an example of why intelligence is critical to the successful conduct of special operations. Six Italian frogmen were able to destroy two of the most important ships in the British fleet, a feat the Italian and German navies and air forces were unable to accomplish. The Italians were aware from previous failed manned torpedo strikes at Gibraltar and Malta that they needed to have detailed

intelligence for the mission to succeed. During this previous operation in Malta, they did not have an agent on the ground to provide supporting intelligence. On the other hand, agents in Alexandria reported on harbor patrols and other harbor defenses. With the detailed intelligence on the harbor, the Italians were able to tailor their mission rehearsals to the mission profile required for the harbor. Commenting on the realistic training, one of the frogmen recalled that the mission seemed like "an exercise."[28] The operators were able to examine aerial photos, maps, and human intelligence (HUMINT) reports from Alexandria. The detailed intelligence picture helped to determine a route to bring the host submarine, *le Scire*, to within 1.3 miles of the harbor entrance and to plot a safe and direct route for the manned torpedoes.[29]

The intelligence picture was also critical in determining a go/no go decision point for the mission. Due to poor weather and lack of location data on the targets for the mission, the Italians postponed the operation for twenty-four hours. They received a final operational intelligence update the day of the operation, allowing for precise targeting. The final intelligence update allowed intelligence to play a role in the execution phase, in addition to the planning and training phases of the mission.

Detailed intelligence made the 1940 assault on Eben Emael in Belgium possible for a small German force. The Germans knew they could not neutralize the fort with a conventional parachute, air bombardment, infantry, or armored assault before artillery from the fort was able to destroy the bridges the Germans needed. Having available only a small force outnumbered ten to one, the Germans had to plan carefully. They had excellent intelligence, which reduced the planning considerations. A German subcontractor who helped build the fort

[28] McRaven, *Spec Ops: Case Studies in Special Operations Warfare*, 90.

[29] J. Valerio Borghese, *Sea Devils*, trans. James Cleugh (Chicago: Henry Regnery Co., 1954), 135, 138–143.

provided blueprints of the structure, allowing the planners to know the exact location of the large guns and fields of fire.[30] Additionally, they had detailed photo intelligence from flyovers.

All of the detailed intelligence allowed for tabletop models of the facility to be constructed. The Germans knew where to expect counterattacks, which casemates and cupolas to attack, and had specially designed shaped charges to destroy the casemates. All of this fed into the training cycle. The Germans conducted their demolition training against similar casemates and the gliders landed in an area comparable to the layout of the fort. The physical training was also based on intelligence.[31] In this case, the intelligence provided critical inputs to the planning and training phases vice the execution phase. The detailed intelligence helps explain how sixty-nine German commandos could seize the most expensive and hardened fort of its day.

The 1943 operation against the Vermork Heavy Water facility in Norway demonstrates the interplay between intelligence and targeting. The British deemed the facility strategically important and devoted considerable resources to attempting to destroy it, but failed. The Norwegian commando team that later assaulted the facility had intimate knowledge of it. Without previously seeing the facility, the operators knew where the buildings were in relation to each other and knew the best locations for concealment and cover.[32] The operators carried the exact weapons load to conduct their mission. Without the precise intelligence, a small team would not likely have been able to enter the facility as quickly and without firing any shots. The intelligence played a critical role in the planning and training portion of the mission.

The role that intelligence played in the 1970 Son Tay prisoner of war rescue operation is critical, but unfortunately the intelligence was also flawed. In

---

[30] McRaven, *Spec Ops: Case Studies in Special Operations Warfare*, 43.

[31] Ibid., 61.

[32] Miller, *Behind the Lines*, 110.

some tactical aspects of the operation, the intelligence was nothing less than superb. In other aspects, the intelligence failed the team. The operators had access to the best technical intelligence, allowing them to develop a plan to ingress deep into North Vietnam without being detected.[33] They also had access to a scale mock-ups of the facility built for use in planning and had a detailed assessment of the conditions of the Prisoners of War (POWs).[34]

If the planners had decided to take the risky step of using a HUMINT source to verify the presence of the POWs, they might have learned that the facility was empty. The failure to correctly determine that there were no prisoners at the camp was both a product of wishful thinking and the desire to avoid signaling to the North Vietnamese their intention to conduct a raid.[35] The intelligence at the unit level was superb and allowed for the mission planners to develop a highly innovative plan that was nearly flawless in its execution.

E. THE INDIRECT APPROACH

Intelligence required for Special Operations using the indirect approach is also very distinct from both the direct approach and from conventional unit intelligence needs. Joint Doctrine states "intelligence support to SOF in [Military Operations Other Than War] MOOTW requires an expanded focus of the standard scope of intelligence functions."[36] The intelligence must discuss political, economic, cultural, and family and tribal relationships, in addition to traditional military data. Unconventional warfare (UW), psychological operations (PSYOPS), and foreign internal defense (FID) are mission types that center on understanding the population, key tribes, and personalities in a region. The more

---

[33] Lucien S. Vandenbroucke, *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy* (New York: Oxford University Press, 1993), 55–56.

[34] McRaven, *Spec Ops: Case Studies in Special Operations Warfare*, 293, 297.

[35] Vandenbroucke describes several of the reasons for going ahead with the raid even though intelligence was beginning to suggest that the POWs might have been moved: the windows for conducting an operation were closing for the year; POWs were beginning to die in captivity; and the team was in Thailand and ready to go. Vandenbroucke, *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy*, 64–66.

[36] Joint Publication 3-05, V-2-3.

information available on the particular groups and their grievances, culture, vulnerabilities, and religion, the more effective the indirect force will be. Tools such as network analysis are designed to provide insight into the wider group or tribal structure.

The intelligence requirements for the indirect approach contrast with intelligence requirements for SOF direct-action missions and conventional forces that are tasked to attrite enemy forces. For example, conventional forces, when attempting to destroy an enemy tank, don't need to understand the religious background or the language of the tank commander. They need only to understand what type of round will penetrate the tank's armor.

The Bay of Pigs invasion, while not a classic indirect case, provides a clear example of what happens when intelligence about the attitudes of local populations is misunderstood or not taken into account. The key assumption of the invasion force was that an invasion and initial success would cause a chain reaction of uprisings throughout the country due to the unpopularity of the Castro government. The invaders also assumed that low morale among Castro's forces would prevent them from putting up a good defense. Both assumptions turned out to be very wrong. Significant amounts of HUMINT were available that demonstrated the level of motivation and effectiveness of Castro's forces and should have provided a more realistic assessment of the level of resistance.[37]

The Village Stability Operations (VSO) program in Afghanistan conducted by SOF demonstrates the need for a very different type of intelligence capability. Understanding the tribal and ethnic dynamics in an area is critical for success in stability operations. Each new VSO site is chosen after a detailed review of the project's goals in a specific area. For example, in some areas SOF may choose to set up a VSO near a minority tribe's village to provide protection. In other areas, SOF may set up the VSO in the district center to support a local governor

[37] Vandenbroucke, *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy*, 153–154.

who has been deemed competent.[38] Only by closely monitoring the intelligence picture by using both unclassified open-source and classified intelligence collection can a detailed and current understanding of the human environment be gained and maintained.

F. CONCLUSION

While the requirements for both the direct and indirect methods vary from the intelligence requirements for conventional forces, they also vary from each other. The intelligence for the direct approach is very detailed, specific, and usually highly classified. The intelligence for the indirect approach is more general and usually unclassified or lowly classified.

It is not surprising that in a war such as Afghanistan in which special operations have played such a prominent role, intelligence has also played a critical part. It is a change from previous conflicts; previously, intelligence was important, but not the decisive factor. Former Central Intelligence Agency (CIA) Director Michael Hayden observed:

> [T]he Soviet Union's most deadly forces -- ICBMs, tank armies -- they were actually relatively easy to find, but they were very hard to kill. Intelligence was important, don't get me wrong, but intelligence was overshadowed by the need for raw, sheer fire power. Today the situation is reversed. We're now in an age in which our primary adversary is easy to kill, he's just very hard to find. So you can understand why so much emphasis in the last five years has been placed on intelligence.[39]

Intelligence is now a decisive factor in the current conflicts. With the emphasis on counterinsurgency operations in Afghanistan, some of the facets of special operations intelligence have made it into the larger military intelligence

---

[38] Stephen N. Rust, “The Nuts and Bolts of Village Stability Operations,” *Special Warfare*, July-September 2011.

[39] Michael Hayden, “Prepared Remarks at the Council of Foreign Relations,” New York, September 7, 2007, https://www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html (accessed March 13, 2011).

scheme. Former International Security Assistance Force (ISAF) CJ2 Major General Michael Flynn argued in 2010 that:

> [B]ecause the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade.[40]

He essentially argued for military intelligence in Afghanistan to resemble the intelligence required for indirect operations. This trend will likely continue, as the current conflicts lend themselves to a special operations model.

Almost every publication states that intelligence is critical for special operations success. No publication discusses the reasons in detail. For direct operations, intelligence must help determine what is necessary to gain relative superiority due to SOF's smaller size and limited firepower. Once that is determined, intelligence must be considered in the planning, rehearsal, and execution phase of an operation. For indirect operations, intelligence must describe the political, cultural, and economic environment of the battle space. Special operations rely on aspects of intelligence that conventional forces, due to their size advantage and mission, can afford to overlook. In this respect, intelligence support to SOF is a *decisive* factor, when in conventional operations it usually is not; therefore intelligence support to SOF is special.

[40] Major General Michael Flynn, Captain Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (accessed December 3, 2010).

III. INTELLIGENCE SHARING CHALLENGES AND WAYS TO MASTER THEM

> Although the literature on international intelligence cooperation is sparse and largely historical there is hardly any doubt that all intelligence services perform some kind of liaison function. None has all the resources—financial, human, and technical—to be entirely self-sufficient in all areas. Furthermore, the transnational nature of security threats makes isolation an impossible option.[41]
>
> Stéphane Lefebvre

A. BACKGROUND

SOF is a valuable tool in contemporary conflicts around the world. We have already established that SOF has special needs in intelligence to be effectively employed with minimal operational risk. Stéphane Lefebvre argues that no nation will have all the resources to be self-sufficient in all intelligence areas, yet intelligence sharing and cooperation has proven to be difficult even within a long-standing alliance like NATO. This chapter will first describe some of the challenges for multinational intelligence sharing and then suggest possible mitigations to these challenges, understanding that intelligence sharing, especially in an international context, will be problematic.

B. CHALLENGES AND SHARING OBSTACLES

1. Lack of Mutual Interest and Cost/Benefit

The cost/benefit analysis is the crucial starting point for countries to join an intelligence sharing collaboration, either on the battlefield or in crisis prevention. For multinational intelligence sharing to work, states must have strong mutual

[41]Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence* 16, no. 4 (Summer 2010): 536.

interests. Lefebvre describes these mutual interests as “a common enemy and great gains of sharing.”[42] If these are lacking, the cost versus benefit analysis will normally keep states from sharing intelligence.

The maxim “the enemy of my enemy is my friend” has guided countries to share intelligence throughout history. Many authors belong to the “common interest school” to explain why intelligence sharing on the international level sometimes works and sometimes does not work.[43] James I. Walsh, in his recent book *The International Politics of Intelligence Sharing*, argues that states will share intelligence with each other when they have a common interest and when there are possible gains in sharing.[44] In cases where mutual interests are strong and the value of sharing is high, the flow of information and intelligence is normally not a problem.[45]

2. Bureaucracies

One school of thought on why intelligence sharing does not happen as readily as it should in an international context is that while it may be official state policy to share intelligence, intelligence bureaucracies in individual countries actively resist direction to share intelligence. Authors who argue in favor of this reach a conclusion similar to ”mutual interests” authors as Walsh and LeFebvre, but for different reasons.

Björn Fägersten is one of the scholars arguing for bureaucratic resistance as one of the key challenges of intelligence sharing. Building on Graham Allison’s studies of bureaucratic roles in policymaking, Fägersten doubts policy

---

[42] Stephane Lefebvre, “The Difficulties and Dilemmas of International Intelligence Cooperation,” 528.

[43] For examples, see Lefebvre, “The Difficulties and Dilemmas of International Intelligence Cooperation;” Jennifer Sims, “Foreign intelligence liaison: devils, deals, and details,” *International Journal of Intelligence and Counter Intelligence* 19, no. 2 (2006); and J.T. Richelson, “The calculus of intelligence cooperation,” *International Journal of Intelligence and Counter Intelligence* 4, no. 3 (1990).

[44] James I. Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2010), 8.

[45] Lefebvre, “The Difficulties and Dilemmas of International Intelligence Cooperation.”

makers' ability to direct outcomes in intelligence sharing. Fägersten uses the example of Europol to demonstrate that while European policy makers repeatedly stated that they wanted intelligence shared among Europol members, intelligence and security services refused to provide valuable intelligence.

The two main roadblocks are bureaucratic interests and bureaucratic culture. Bureaucratic interests are essentially turf-wars in which actors in organizations resist sharing due to the desire to control the intelligence they generated and in which they lack incentive to give up sole authority. The old adage "information is power" is appropriate here. Intelligence organizations are reluctant to give up their secrets because it is not in their self-interest to do so. According to Fägersten, "self-interest is inherent in any political actor . . . bureaucratic actors pursue their own rational goals such as increased budgets, more power in the decision-making process or personal advancement."[46] Each organization wants to be the one organization whispering secrets in their president's or prime minister's ear.

Equally persuasive is the bureaucratic culture argument. Fägersten states that intelligence and security organizations are essentially conservative and resistant to change. Intelligence staffs have little contact with and rarely cooperate with outside agencies. As such, they are naturally suspicious of outside organizations, especially foreign organizations. Intelligence organizations are generally established to collect and keep secrets from foreigners and thus they are wary that sharing exposes the organization to the risk of a leak. The examples that Fägersten gives are persuasive. He lists repeated attempts by the European Union after 9/11, the Madrid bombings, and again after the London bombings to force multilateral intelligence sharing with Europol. Each instance proved futile.[47]

---

[46] Björn Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol," *Intelligence and National Security* 25, no. 4 (2010): 502.

[47] Ibid., 507–513.

A third explanation as to why international intelligence sharing is problematic is the bureaucratic process itself. U.S. Army COL George Gramer gives an example of the bureaucratic process preventing intelligence sharing at the operational and tactical level. He describes the confusion created by various rules and contradictions in doctrine that made intelligence sharing for NATO difficult during Operation JOINT ENDEAVOUR in Bosnia. While joint doctrine states that intelligence dissemination is an operational commander's responsibility; it gives little guidance on how to accomplish this task.[48] The confusion resulted in loss of timely intelligence, redundant reporting, and resulted in nations relying on their own exclusive national intelligence systems. "Intelligence collected by exclusively national sources often seemed to be siphoned off into national channels; in most cases, the intelligence was never shared with the coalition," according to Gramer.[49]

Another example of this is outlined in Norwegian media. It states that Norwegian security laws, created during the Cold War to protect Norwegian intelligence, prevent Norwegian soldiers in Afghanistan from sharing intelligence with their partners, ultimately putting soldiers' lives at risk.[50]

The 9/11 Commission Report did not directly address international intelligence sharing, but shed light on why domestic intelligence sharing within the U.S. intelligence community was problematic, as well as the lack of incentive each organization had to share intelligence. Each agency had its own internal rules *against* sharing, and lacked rewards *for* sharing. There were no punishments for not sharing information and no penalties for over-classifying information. In other words, there was no incentive to share for individual

[48] 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* (1999): 1–2.

[49] Ibid., p. 5.

[50] Camilla Wernersen, "Norsk Lov Utsetter Soldater for Livsfare (Norwegian Law Exposes Soldiers to Risk)," Norwegian National Television, November 21, 2011, http://www.nrk.no/nyheter/norge/1.7881332 (accessed November 27, 2011).

analysts, only risks in doing so.[51] In a multinational environment this is even more problematic because release of classified information requires approval from a Foreign Disclosure Officer or an equivalent bureaucrat.

Intelligence agencies are generally embedded in bureaucratic national organizations. These bureaucracies are conservative, resistant to change, and reluctant to share intelligence; furthermore, their staffs have little contact with, and few systems to cooperate with, outside agencies. The "need to know" principle and stove-piping of information persist. The consequence of this behavior is over-classification and excessive compartmentalization.

3. Sharing Enablers

A lack of will or lack of capabilities, or a combination thereof in large part explains the failure to overcome a lack of "Mutual interest" and bureaucratic obstacles to intelligence sharing.[52] In the following section the potential factors to *enable* intelligence sharing and to overcome the systemic resistance to change will be analyzed in four categories: gains, trust, direct control, and accessibility. Although the literature on collaboration in general is broad and extensive,[53] these categories are the authors' attempt to analyze this literature based on our observations[54] of why intelligence sharing occurs when it does.

---

[51] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2004), 417.

[52] Jeanne Hull, ""We´re all Smarter than Any One of U.S.": The Role of Inter-Agency Intelligence Organizations in Combating Armed Groups," *Journal of Public and International Affairs* 2 (2008): 28.

[53] For example, view Robert Axelrod, *The Complexity of Cooperation* (Princeton, Princeton University Press, 1997); Eduard Salas, *Team Cognition* (Washington, DC, American Psychological Association, 2004); and David B. Seaburn, *Models of Collaboration* (New York, Perseus Books Group, 1996).

[54] Authors visit with Dr. Christopher J. Lamb and discussed the work of Joint Interagency Task Force South (JIATF-South), the Pentagon Intel Fusion Center, and the NATO SOF HQ.

4. Gains

Gains or mutual benefits are necessary conditions for intelligence sharing.[55] The members of an intelligence coalition weigh the benefits and costs for contributing before entering into an intelligence sharing relationship.

On an organizational level, a country's investment in a multinational coalition has to be attractive and cost efficient. No one country's intelligence service has all the resources (financial, human, technical) to be entirely self-sufficient in all areas.[56] A state may share collection capabilities with a foreign intelligence service and share the results of the collection, or a country may grant the use of its territory to collect intelligence in exchange for sharing in the information collected.[57] The guiding principle, "the enemy of my enemy is my friend" illustrates one of the purest forms of mutual benefit and common interest. Mutual benefits are essential to maintain desirability for the different members of an intelligence sharing coalition. As with many types of cooperation, the benefits of intelligence sharing increase with the frequency with which the participants exchange intelligence and the range of issues their agreements include.[58]

The Joint Inter Agency Task Force South (JIATF-South) is one example of intelligence-sharing success. According to Dr. Christopher J. Lamb of the National Defense University, one of the most commonly cited reasons for JIATF-South's success is that partner organizations and nations believe they get a great return on their investment. In exchange for intelligence they get credit for drug seizures or prosecutions, making partnering with JIATF-South a productive investment.[59]

---

[55] Walsh, *The International Politics of Intelligence Sharing*, 24.

[56] Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," 536.

[57] Derek S. Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," *Orbis* 50, no. 3 (2006): 455.

[58] James I. Walsh, "Defection and Hierarchy in International Intelligence Sharing," *Journal of Public Policy* 27, no. 2 (2007), 152.

[59] Christopher J. Lamb and Evan Munsing, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success* (Washington, D.C.: National Defense University Press, 2011), 45.

A solid goal-setting process that culminates in a clear mission can drive the intelligence sharing process.[60] JIATF-South is a purpose-built counternarcotic organization, and its narrow mission helps to keep the focus on agreed upon intelligence issues.[61] Another example of a purpose-built intelligence sharing organization is the Pentagon Intelligence Fusion Center (PIFC). PIFC´s target customers and main contributors are countries filling important positions in Afghanistan.[62] This linkage to operations substantiates PIFC´s clear understanding of the goals to be achieved and fosters a belief among its members that the organization is worthwhile.[63]

5. Trust

Trust is based on expectations about how others are likely to behave in the future.[64] Cooperation generally depends on trust. The level of trust is one factor that influences how much intelligence is shared.[65]

One of the most influential factors in the judgment of trust is competence.[66]JIATF-South has a dozen personnel in senior positions who have worked in the field against illicit trafficking for over 20 years, and almost half of the entire command has been on board for six years or more.[67] At JIATF-South, new personnel are mentored by experienced members, but also pass through

---

60 Lamb and Munsing, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*, 45.

61 Ibid., p. 35.

62 Currently the PIFC consists of approximately 20 personnel from the U.S., Germany, Denmark, Poland, Holland, Canada, Spain and Australia; It is a national level intelligence fusion center that brings together U.S. and partner intelligence agencies to fully share and exploit information across issues vital to coalition success in Afghanistan. It reached full operational capability in 2010. PIFC, e-mail to authors, November 1, 2011.

63 Glenn M. Parker, *Cross-Functional Teams: Working with Allies, Enemies, and Other Strangers* (San Francisco: Jossey-Bass, 2003), 88.

64 Barbara D. Adams, "Trust in Small Military Teams," http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/006.PDF, (accessed October 12, 2011).

65 Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," 457.

66 Adams, "Trust in Small Military Teams."

67 Lamb and Munsing, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*, 48.

training programs to establish a common baseline level of competence.[68] Competence is a necessary condition for trust in an intelligence-sharing environment, however it is not sufficient without the existence of a common culture.

A common culture is characterized by shared values, goals, norms, policies and similarities. Collaborative professional training and education programs, as well as shared experiences in general, stimulate a common culture. The deeper the common culture, the better the community's tacit understanding and the more predictable the actions of other coalition members. The derived common culture is a form of social institution that facilitates internal coordination.[69] Increased combined duty builds a deeper sense of trust and community. Trust-building depends inevitably on time.

James Walsh, author of *The International Politics of Intelligence Sharing,* describes the competence/common culture nexus by analyzing the UK-U.S. agreement of 1948 in comparison to the Gehlen organization, the predecessor of the Federal German Intelligence Service. The Gehlen organization provided expert knowledge on the Soviet Union, but the knowledge was less trusted by the U.S. due to the organization's Nazi background. The British, on the other hand, provided expert knowledge on their colonies and former colonies, and the information and intelligence was more trusted by the U.S. because of the UK-U.S. common culture.[70]

Relationships in the SOF community are based primarily on face-to-face contact, which is more information-rich than purely virtual communication and therefore more likely to inspire trust. As relationships develop, increasing knowledge of another person and information about cultural similarities lead to identification with this person, that is, to seeing oneself and another person as

---

[68] Ibid., p. 58.

[69] Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol," 504.

[70] Walsh, "Defection and Hierarchy in International Intelligence Sharing," 171–174.

belonging in the same group. Increased trust is a product of this identification and it encourages trust with the group as a whole. [71]

Both the exchange of information and the openness with which the information is exchanged provide evidence about the assessment of another's trustworthiness.[72] The level of trust needed in an intelligence-sharing environment is achieved when all actors assume that intelligence products are routed to the right consumer by default and regardless of the nationality of the recipient.

6. Direct Control

In any intelligence-sharing agreement there is always a fear that participants will violate the agreements, will not be as responsive as required, or will withhold intelligence and not disseminate it properly. One attractive option to counter these fears and manage the risks is to rely on a clear hierarchy with one leading agency or nation in direct control of the intelligence collaboration framework. Hierarchical agreements include a dominant state, responsible for making the most important decisions and for monitoring compliance. [73] The leading agency's responsibility is to maintain focus and direct efforts.[74] The leading agency or nation can properly be held accountable only if it has the authority to punish those who violate the agreement.

The 9/11 Commission Report, for example, names the lack of a central authority as a fundamental problem of efficiency and intelligence sharing.[75] A hierarchy can deliver the cooperative synergy and intelligence fusion that member states in an alliance desire. The CIA-Gehlen collaboration during the

---

[71] Adams, "Trust in Small Military Teams."

[72] Adams, "Trust in Small Military Teams."

[73] Walsh, "Defection and Hierarchy in International Intelligence Sharing," 152.

[74] Hull, "'We´re all Smarter than Any One of U.S.': The Role of Inter-Agency Intelligence Organizations in Combating Armed Groups," 36.

[75] Ibid, p. 7; and National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 402.

Cold war is a successful example of a hierarchical intelligence relationship, where the CIA was the dominant actor with direct control over the Gehlen organization.[76]

Conversely, participating countries are aware that if they pay lip service to the requirement to share intelligence and instead focus only on their own interests, they will be punished. The PIFC, for example, has clear job requirements for contributing countries. The U.S., as PIFC´s framework nation, reserves the right to vet each country's incoming personnel to make sure they are qualified and not a security risk.[77]

7. Accessibility

Effective intelligence sharing requires accessible and compatible means of secure communications. In a multinational intelligence-sharing environment, the members of the different nations have to be able to connect with each other in order to exchange classified intelligence.

One basic requirement at the individual level is simply to speak the same language. PIFC and the JIATF-South demand adequate language proficiency in English on combined duty positions. Beyond that, JIATF-South (with its clear regional focus) regularly distributes a compendium of "best operational practices" translated into several languages.[78]

The information age created further opportunities to ensure communications and the exchange of intelligence. The PIFC is using the NATO Battlefield Information Collection and Exploitation System (BICES) as a central information system to facilitate communication. JIATF-South is connected to nations by the Cooperating Nations Information Exchange System, which has

---

[76] Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," 460–461; and Walsh, "Defection and Hierarchy in International Intelligence Sharing," 152.

[77] Visit to the Pentagon Intel Fusion Center (PIFC), July 15, 2011.

[78] Lamb and Munsing, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency*, 47.

online chat rooms with real-time translation.[79] Existing compartmentalized practices can be minimized through a liaison infrastructure. The PIFC´s foreign disclosure officer is physically located between the coalition partners using solely BICES and the U.S. personnel using national systems, in addition to BICES to ensure accessibility of intelligence for coalition members.[80]

A solution to avoid classification and policy obstacles is the bottom-up approach.[81] Instead of starting an intelligence process from the "top" with the highest classification, the starting point should be from unclassified and open source and then steadily move up the "classification" ladder. Commercial off-the-shelf technology, which continues to become more and more capable, has the potential to foster accessibility of information since the raw data is unclassified and the analysis can be written for release to foreign partners.

8. Sharing Enablers Nexus

While the enablers we have just discussed are not enough to completely overcome the desire not to share intelligence, they do help overcome the obstacles to sharing and help mitigate the risks associated with sharing. None of the enabling categories described above should be considered in isolation. A majority of the mentioned factors are inevitably interconnected to each other. Policies and standards implemented by a lead nation also can have a positive effect on trust building. Violations of security standards can destroy credibility of one actor or nation, but can increase trust in the system if appropriately handled.

---

79 Lamb and Munsing, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency*, 49.

80 Visit to the Pentagon Intel Fusion Center (PIFC).

81 Gregory F. Treverton, *Intelligence for an Age of Terror* (New York: Cambridge University Press, 2009), 193.

C. CONCLUSION

There are numerous reasons why intelligence sharing is challenging, and nations have significant reasons not to share intelligence even with their closest allies. Bureaucratic interests and states' fears of compromise prevent effective intelligence sharing and there will likely never be complete intelligence sharing among nations. There are specific factors that can mitigate the fears associated with sharing intelligence, however. The factors that facilitate intelligence sharing are mutual gains, trust, direct control by a leading agency or nation, and accessibility. The combination of these factors supports the "trust, but verify" approach in intelligence sharing relationships.[82]

[82] Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," 468.

IV. CRACKING THE CODE: THE NSHQ AND INTELLIGENCE SHARING

> Although the possession of intelligence is a battle-winning factor, the full impact of intelligence cannot be effectively applied unless both the intelligence itself and the information from which it is derived can be shared. Interoperability, in this case the ability to exchange information and intelligence, is the key to successful multinational operations.
>
> NATO Intelligence Doctrine[83]

NATO developed most of its intelligence doctrine during the Cold War.[84] Operations in the Balkans and Afghanistan, demonstrated to the NSHQ leadership the theoretical predictions that intelligence sharing is problematic even under the best of circumstances and would not work well in a SOF environment.[85] NSHQ subsequently developed an innovative approach to solve the problem of intelligence sharing among NATO SOF forces. This approach clearly exemplifies the four pillars we identify in Chapter Three: mutual gains/benefits; trust; direct control; and accessibility and interoperability. By using this approach, the NSHQ addressed most of the factors that make sharing intelligence difficult. In those cases for which sharing is not possible, NSHQ has developed methods to supplement their intelligence collection and analysis.

A. MUTUAL GAINS/BENEFITS: RELEVANCE OF NATO SOF AND INTELLIGENCE FOR THE ALLIANCE

In its new strategic concept, *NATO 2020: Assured Security; Dynamic Engagement,* NATO characterizes the threat of conventional aggression against the Alliance or its members as low. The future threat is more likely to be unconventional and most likely to come from a ballistic missile attack, a terrorist

---

[83] NATO AJP-2 "Allied Joint Intelligence, Counterintelligence and Security Doctrine P 2," 2003, 1-1-1.

[84] Ibid.

[85] NSHQ Chief of Staff briefing, Naval Postgraduate School, Monterey, CA, October 20, 2011.

attack, or a cyber attack.[86] The future threats articulated in the new strategic concept document echo the threats described by several NATO countries in their national strategies, including the U.S. The newly released U.S. *National Military Strategy* emphasizes both the ongoing shifts and increasing interconnectedness in the international order and the threat from non-governmental actors such as terrorists and pirates. Looking at the similarities in future threats among member states and official NATO strategy, it is easy to conclude that a common enemy exists, establishing the critical requirement for the mutual gains that can come from intelligence sharing. The complexities in the international order and the "significant challenges to the intelligence system [that] arise in targeting groups such as al-Qaeda due to their networked and volatile structure" make multinational intelligence sharing a prerequisite.[87] In other words, there is much for all to gain from multinational intelligence cooperation.

SOF has been identified as a key tool in the post 9/11 security environment for solving these contemporary conflicts that the NATO members have in common. Many NATO SOF units have conducted multiple deployments to and operations in Afghanistan over the last ten years. The result is that NATO SOF units are more experienced and combat tested than ever. Yet a 2008 NATO study found that "[A]lliance SOF operational experiences… in Afghanistan have demonstrated gaps in policy, organization, interoperability, and resourcing that have caused these highly valuable forces to operate inefficiently and at times at cross purposes."[88] NATO formally established NSHQ to further transform and integrate NATO SOF; currently, NSHQ provides the operational command capability to the ISAF SOF HQ and its intelligence arm, the Special Operations Forces Fusion Cell (SOFFC) in Kabul, Afghanistan to mitigate the intelligence sharing problems.

---

[86] North Atlantic Treaty Organization, "NATO's New Strategic Concept."

[87] Cline, "Special Operations and the Intelligence System," 579.

[88] North Atlantic Treaty Organization Special Operations Coordination Centre (NSCC),"The North Atlantic Treaty Organization Special Operations Forces Study."

The individual NATO SOF nations will benefit by increasing their intelligence capacity, which gives them an incentive to participate in the NSHQ effort to increase intelligence capacity across the NATO SOF force. NATO SOF cannot afford to rely on national intelligence alone as the primary source of their intelligence as this is too time-consuming, problematic, and unreliable in a tactical SOF environment. The collection and analytical effort by the different nations task forces is fused by the SOFFC. Without this oversight, collection and analysis efforts would be narrowly scoped and might miss the broad picture needed to be effective against a widespread enemy network. This thesis has argued that there is a need for effective multinational intelligence sharing to make NATO SOF relevant to the Alliance in present and future conflicts. Without intelligence sharing, NATO SOF will not be as effective as possible, thus each state should have an incentive to share relevant intelligence within NATO SOF.

B. TRUST, COMMON CULTURE, AND COMPETENCY: INTELLIGENCE STANDARDIZATION, TRAINING, AND EDUCATION

As NATO SOF moves from a "stovepiped," nation-dependent model to a "plug-and-play" model, NATO SOF members benefit from being part of a larger NATO SOF intelligence apparatus as equipment, training, and analytical capability is standardized, trust is built, and intelligence is shared.[89] To enhance trust, competency, and intelligence sharing amongst its members, the NSHQ relies on a robust program of intelligence standardization, training, and education. At the core of the NSHQ's intelligence mission are the NATO SOF Training and Education Program (NSTEP) and training facility at Chievres Air Base near the NSHQ in Mons, Belgium.

When the NSTEP was developed, the basic assumption was that the intelligence education curriculum was a natural starting point. Most nations' SOF were able to conduct the Finish piece in the Find, Fix, and Finish, Exploit, and Analyze (F3EA) cycle described in figure 4. However, very few of the NATO

[89] In the plug-and-play model, the NATO SOF task forces all have similar intelligence requirements and standards; NSHQ COS briefing, October 20, 2010.

SOF nations had the assets, countrywide reach, or the capability to find, fix, exploit and analyze alone. The NSHQ expends most of its intelligence training time in these phases.[90]

Figure 4. F3EA Cycle [91]

Most NATO nations do not have an intelligence sub-specialty or an intelligence Military Occupational Specialty (MOS).[92] Additionally, intelligence personnel with experience in SOF are an even smaller subset of intelligence personnel, so the number of trained SOF intelligence personnel across NATO is small. For this reason, SOF intelligence education was a natural starting point for the NSHQ. A NATO school with intelligence courses exists, but was not focused on SOF requirements. The NSHQ identified new requirements based on the gaps between what was already taught in NATO courses and the training requirements for SOF personnel as described in figure 3.

[90] NSTEP Director, discussion with authors, Chievres Air Base, Belgium, October 26, 2011.

[91] F3EA cycle, NSCC SOTG Manual v 1.0, December 11 2009, 4-17.

[92] Observation from NSHQ site visit, October 25, 2011.

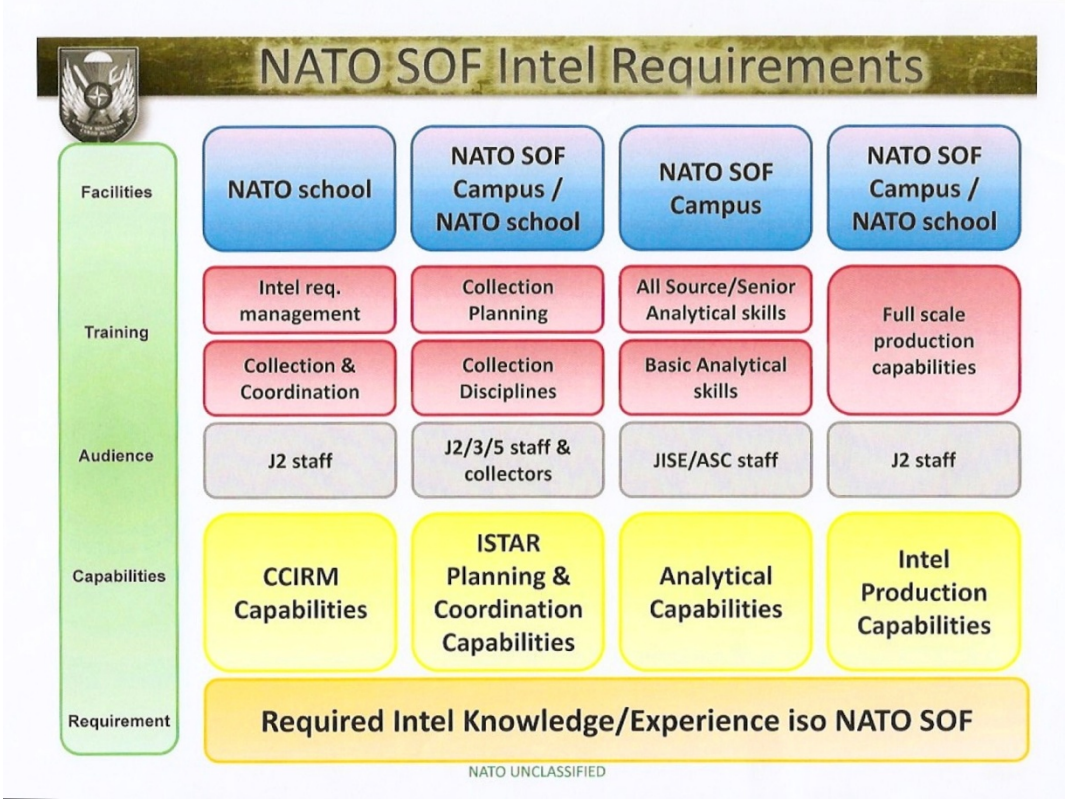


Figure 5. NATO SOF Intelligence Training Requirements[93]

The NSHQ (through NSTEP) offers a wide range of intelligence courses aimed at standardizing NATO SOF intelligence skills for both operators and analysts. . The courses are geared toward SOF at the operational and tactical levels, with a focus on current operations in Afghanistan. Some of the intelligence courses offered by the NSHQ are:

- Basic Intelligence Course
- Threat Network Analysis Course
- ISR Seminar
- Warrior View Course
- Cell Phone Exploitation Course
- Forensic Exploitation Course
- Precision Geo-Location Familiarization Course

[93] NSHQ Intelligence Training briefing, NSHQ, Mons, Belgium, October 27, 2011.

- Maritime Intelligence Course
- Technical Exploitation Operations Course[94]

With trained and qualified SOF intelligence personnel, NATO SOF will be better prepared to integrate intelligence into the planning and conduct of operations, in addition to being more educated consumers of intelligence. Shared training also creates a baseline standard amongst the NATO SOF, which increases trust and competency.

A second key piece of the NSTEP is building personal relationships. The NSTEP program spends 75 percent of the time on coursework, but the other 25 percent of the time is spent developing relationships and learning how to operate in a multinational SOF environment.[95] With relationships thus established, NATO SOF forces arrive in the field with an established, trusted network, since people know each other and have a basic understanding of differing military cultures.

To further the trust amongst the various nations, the NSHQ does not have mobile training teams. The rationale for this decision is to prevent individual nations from suspecting that they have received less thorough training than have other nations and to force members to attend the training at the NSTEP where they meet members from other nations. The practical effect is that all the nations involved receive the same intelligence baseline, thus strengthening competency. In addition, all nations know that they all have received the same training as well as enhanced personal relationships among the members of the NATO SOF community. The participating non-NATO SOF nations (Partnership for Peace members, Australia, New Zealand, Sweden, etc.) that are part of the coalition also receive the same training. There are no exclusions, cutouts, or other

[94] NATO SOF Training and Education Program, "NSTEP Course Offerings," http://www.nshq.nato.int/NSTEP/ (accessed November 1, 2011).

[95] NSTEP Director, discussion with authors.

segregation for participating members. All cleared and vetted participants are treated equally with regards to clearances and access to NSHQ systems. [96]

Over the last few years, NATO SOF personnel have established trusted networks through continuous training exercises (e.g., COLD RESPONSE, FLINTLOCK), training programs (e.g., NSTEP) and operational commitments (e.g., Balkans, Afghanistan). Because the NATO SOF community is fairly small in comparison to any one country's military apparatus as a whole, the personnel tend to encounter the same people on multiple occasions and thus develop close personal ties, which promotes rapid trust building.[97]

C. DIRECT CONTROL: THE U.S. AS THE FRAMEWORK NATION

In March 2006, Supreme Headquarters Allied Forces Europe (SHAPE) suggested establishing an SOF Component Command "on par with the Joint Force Commands."[98] The proposal was turned down. However, at the Riga Summit later that same year, the NATO heads of State approved a U.S. initiative to start the process of transforming NATO SOF with the purpose of optimizing SOF within the Alliance. On December 22, 2006, Admiral McRaven was appointed Director of NSCC and ordered to start the transformation process. Three years later, on March 1, 2010, NSHQ was formally established as a three-star headquarters within the Alliance, with the U.S. as the framework nation.[99]

The U.S. as the framework nation has been pivotal in the stand-up phase of the NSHQ. It is unlikely that any country other than the U.S. would have had the capabilities to foster the transformation from a three-man special operations office headed by a Colonel to a functional headquarters, headed by a three-star

---

[96] NSTEP Director, discussion with authors.

[97] Authors' observation.

[98] NATO Special Operations Headquarters, "Biennial Review,"

[99] The other members of the May 2006 joint initiative were Norway, Holland, and Poland. See NATO correspondence, May 15, 2006, provided by NSHQ. Within NATO, a framework nation is the lead nation supporting a NATO unit. It is responsible for providing the command leadership, key resources, and infrastructure. Refer to http://www.aco.nato.int/page208301014.aspx for more information.

general officer, of over 150 staff members in a time period of just four years.[100] The U.S. is currently manning 40 percent of NSHQ´s positions and more than 30 percent of the positions in the Special Operations Intelligence Branch (SOIB) and the SOFFC.[101] The main financial burden for NATO SOF falls on the U.S., with USSOCOM alone contributing $300 million of its fiscal year 2010 budget to NSHQ.[102] A crucial responsibility is to dedicate strong leadership to the command level. The U.S. is manning the most important positions such as the commander, chief of staff, and the directors of the SOIB and SOFFC. Finally, NSHQ doctrines are largely modeled on U.S. doctrine.[103]

The SOIB and the SOFFC are the primary mechanisms within NATO SOF charged to ensure that intelligence is shared with NSHQ and the operational elements. The SOIB is "designed to provide timely and relevant multi-source and multinational SOF specific intelligence to the full spectrum of NATO SOF missions to meet Supreme Allied Commander, Europe (SACEUR) requirements."[104] The SOIB, located in Molesworth, England, has three analytical teams that serve in Afghanistan on a rotating basis to maintain currency in the threat environment. The SOFFC, located in Kabul, is "focused on garnering information from a multitude of sources, fusing that information with operational requirements to produce, and then disseminate, actionable intelligence to NATO Special Operations Task Groups (SOTGs) in Afghanistan."[105]

---

[100] NATO Special Operations Headquarters, "Biennial Review."

[101] Ibid., 3, and NATO Special Operations Headquarters. "Special Operations Intelligence Branch," November 2010, 2-5.

[102] Andrew Freikert, "U.S. Special Operations Forces: Background and Issues for Congress," March 2011, 5, http://www.fas.org/sgp/crs/natsec/RS21048.pdf (accessed November 10, 2011).

[103] For example, see NATO AJP 3-5, "Allied Joint Doctrine for Special Operations," 2009, and U.S. Joint Publication 3-05 Doctrine for Joint Special Operations, 2011.

[104] NATO Special Operations Headquarters. "Special Operations Intelligence Branch," November 2010, 5.

[105] Ibid., 3.

The U.S. decisively influences the most important decisions of the NSHQ. In terms of its capabilities and responsibilities, the U.S. is powerful and credible enough to hold other countries accountable if they do not fulfill required and agreed-upon benchmarks. For example, nations will not receive BICES terminals until they have fulfilled NSHQ requirements and participated in necessary training.

D. ACCESSIBILITY AND INTEROPERABILITY: USING TECHNOLOGY TO FILL GAPS AND FACILITATE INTELLIGENCE SHARING

A key pillar of NSHQ's intelligence sharing strategy is to use technology to facilitate sharing and fill the gaps where national intelligence is not shared in a timely manner. When the NSHQ's precursor agency, the NATO SOF Coordination Center (NSCC), was established, the commander (Admiral McRaven) did not even have a way to securely communicate with the NATO SOF units and was forced to rely on unclassified email and unsecured phones. Most NATO SOF units did not have NATO systems in their headquarters or at the tactical level.[106] This single deficiency highlighted the challenges NATO SOF had in trying to create secure mechanisms from scratch to share intelligence.

The first challenge for the NSCC began with a search for a Command, Control, Communications, Computer, and Intelligence (C4I) network. NSCC decided to leverage the NATO BICES network as their baseline network.[107] The system is scalable and rapidly deployable to NATO SOF units, both in national headquarters and in the field.

The second challenge for NATO SOF was bureaucratic: intelligence was often held in national channels due to classification and bureaucratic resistance and was not being disseminated down to multinational units in the field in a timely

[106] NSHQ COS briefing, October 20, 2010, and Alan Dron, "Special Network—Alliance Aims to Improve Cooperation among Special Operators," September 1, 2009, http://www.c4isrjournal.com/story.php?F=4211503 (accessed November 14, 2011).

[107] See NSHQ BICES Communications & Information Systems Strategy, August 2011, 3, and Dron, "Special Network—Alliance Aims to Improve Cooperation among Special Operators," 1.

manner—or in some cases at all. Analyses from completed NATO SOF operations in Afghanistan were not forwarded back to the relevant task forces or to the NATO SOF units in the field. The NSHQ's approach to this problem is unique and needs to be explored in detail.

The NSHQ realized that the resistance from individual nations' intelligence services to releasing intelligence in a timely manner would be significant, so they decided to supplement intelligence that came from national intelligence services and NATO structures for tactical intelligence support. They acquired Commercial Off the Shelf (COTS) technical exploitation equipment to collect and analyze the data on their own such as biometric, cell phone exploitation, and forensic systems.[108]

The main advantage of using COTS equipment is that NATO SOF units can classify the data at a level that is releasable to NATO or ISAF instead of to national levels. Since the data is releasable to NATO, it still is accessible by national systems, but NATO SOF units can analyze the data themselves. Having the data rapidly and readily available to the NATO SOF task forces facilitates a rapid turnaround in the intelligence cycle. With an intelligence baseline standard established by the NSTEP, NATO SOF relies less on NATO intelligence or national intelligence structures for intelligence support. Armed with these intelligence skills, NATO SOF can generate intelligence at a classification level appropriate to the force. There is no waiting for a Foreign Disclosure Officer (FDO) to release or downgrade the intelligence in a timely manner; they have access to the raw intelligence from the start.

An example of the use of COTS technology is the tactical biometric systems fielded by NSHQ. The NSHQ owns the systems, trains the operators on their use, and hand-receipts the kits to the NATO SOF units when they arrive in Afghanistan. Before the kits are issued, the NSHQ verifies that the recipients have been appropriately trained on the kits' use. NSHQ maintains the kits, and

[108] For example, see NATO SOF Technical Exploitation Operations Course. https://www.nshq.nato.int/NSTEP/page/login/?ItemTempID=12 (accessed November 10, 2011).

when the units leave Afghanistan, the kits are returned to NSHQ for servicing and maintenance. The raw biometric data collected is stored on a secure, but unclassified server. NATO SOF intelligence analysts with the task forces or at the SOFFC and who have a valid reason to access the data will be granted access to the raw data. The analysts in the field will then be able to turn the data around into the intelligence cycle with a classification appropriate to NATO SOF.

The NSHQ is following this pattern with SIGINT collection, cell phone exploitation, forensic analysis equipment, and a BICES intelligence toolkit.[109] Use of these procedures furthers interoperability by standardizing the equipment, data collection, and data storage across the NATO SOF. Even if a task force is replaced by a task force from another NATO SOF nation, there is consistency in NATO SOF operations regardless of the task force's origin.

The NSHQ has the leeway and has been granted the authority to produce its own best practices manuals and to update their Tactics, Training, and Procedures (TTPs). Unlike NATO doctrine, which takes several years for approvals, the NSHQ can update the manuals as changes become necessary.[110] The ability to rapidly update manuals streamlines interoperability and synchronization, so all units arriving in theater use the latest procedures.

E. CONCLUSION

The NSHQ has "cracked the code" for intelligence sharing. It has avoided many of the potential pitfalls inherent in intelligence sharing arrangements (those pitfalls identified in Chapter 3) and developed a method for increasing the amount of intelligence available to the task forces. The NSHQ developed its intelligence organization and structures with the understanding that it will never have complete access to all available intelligence, but its structures, practices, and procedures mitigate intelligence sharing problems. By standardizing training, improving competency across NATO SOF, using unclassified or NATO classified

[109] NSTEP Director, discussion with authors.

[110] Ibid.

information, and acquiring their own C4I systems, the NSHQ has bypassed obstacles that complicate intelligence sharing. With SOIB and SOFFC, the NSHQ retains proximity to the end user. Feedback in the form of lessons learned from end users in Afghanistan influences intelligence-sharing policies and are applied to the NSTEP training and the technological infrastructure. In continuing to do so, the NSHQ is able to put pressure on the national intelligence organizations to review their own policies of sharing to avoid becoming irrelevant to NATO SOF.

The operational impact of intelligence sharing within NATO SOF can be demonstrated by former ISAF commander General David Petraeus' words on August 2010 to the NATO Secretary General:

> Over the past three months, SOF elements carried out more than 4,000 total operations that captured or killed 235 insurgent leaders and more than 2,500 lower-level fighters – likely an unprecedented number in the history of SOF. . . . The increase in SOF successes also results from improved ISR capabilities, our improved abilities to fuse intelligence, increased partnering efforts with Afghan Special Forces, and improved capabilities of our Afghan SOF partners.[111]

[111] NATO Special Operations Headquarters. "Special Operations Intelligence Branch," November 2010, 4.

V. CONCLUSIONS AND RECOMMENDATIONS, A WAY AHEAD

A. SUMMARY

Chapters One and Two of this thesis argue that SOF is a valuable tool in contemporary conflicts and that SOF relies on accurate and current intelligence to ensure that training, planning, and execution of SOF operations precisely address the situation in an intended target area. SOF normally employs multiple intelligence disciplines, and mission success relies on access to coherently fused all-source products delivered to the SOF operator. Intelligence support to SOF is different from intelligence support to conventional units because more and different detail is required and because it has to be disseminated all the way down to the operator for planning and mission execution.

Chapter Three of this thesis argues that intelligence with the granularity demanded by SOF historically has existed mainly at the national level. Because of bureaucratic obstacles, the need to hide capabilities and sources so as to avoid their compromise or loss, and lack of trust this kind of intelligence has historically not been shared with alliance or coalition partners. Realizing that intelligence sharing will never be perfect, Chapter Three of this thesis argues that however problematic, there are specific factors that can mitigate the fears associated with sharing intelligence. The factors that facilitate intelligence sharing are mutual gains; trust and competence; direct control by a leading agency or nation; and accessibility and technology. A balanced combination of these factors supports the "trust, but verify" approach in intelligence sharing relationships.[112]

This thesis set out to examine whether NATO SOF is optimized for intelligence sharing in a coalition environment. In Chapter Four, this thesis explores both the current status of the NSHQ intelligence structure, and practices

[112] Derek S. Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," *Orbis*, 50, 3 (Summer 2006), p. 468.

and procedures in NATO SOF, and concludes that NATO SOF addresses all of the factors that mitigate the potential pitfalls in intelligence sharing arrangements.

B. CHALLENGES AND RECOMMENDATIONS

The NSHQ has “cracked the code” for intelligence sharing. They have established an organization that mitigates the problems related to intelligence sharing. However, the NSHQ faces the challenge of maintaining consistency for optimized intelligence sharing conditions. The thesis has recognized that NATO SOF is a successful intelligence sharing organization; it might therefore be disrupted by the tendency of successful organizations to grow larger.

One danger related to enlargement is that the NSHQ might become more bureaucratic, increasing the likelihood that bureaucratic obstacles will appear. Another danger related to expansion is that successful organizations attract people--everyone will want to participate and send personnel to learn, but not to contribute. This lack of common competence will undermine trust, one of the crucial factors for intelligence sharing to occur. It is therefore crucial that the NSHQ continue to uphold the standards of personnel working in intelligence related positions.

The U.S. as a framework nation has been crucial in establishing the current intelligence sharing relationship within the NSHQ. While having a strong framework nation in direct control is important, it is also crucial to be aware of the dangers. Unilateral or unbalanced actions by the U.S. could result in partner nations questioning the current perceived benefits of the intelligence sharing relationship.

Operations in Afghanistan are a driving factor for the current intelligence-sharing framework within the NSHQ. Most of the intelligence training, education, and SOPs are based on lessons learned from the SOFFC. SOFFC is a purpose-built intelligence sharing organization with the sole purpose of optimizing the flow of timely and accurate intelligence to the different taskforces on the ground. With operations being the centerpiece for optimized intelligence sharing, it is

imperative for the NSHQ to look “beyond” current operations in Afghanistan and toward future operations. The SOIB is one mechanism through which the NSHQ can institutionalize future SOFFCs with the lessons from Afghanistan and prevent the NSHQ from having to rebuild a functional intelligence sharing structure for future requirements. It is much easier to adjust the target set than to rebuild the entire intelligence sharing mechanism.

At the core of the NSHQ’s intelligence sharing program is capacity building through education at the NSTEP. The current courses, with one exception, are all Afghanistan centric. The recently added Maritime Intelligence Course is a step in the right direction for potential future operational challenges. One of the SOF truths states, “Competent Special Operations Forces cannot be created after emergencies occur.”[113] As such, the NSTEP needs to be looking forward. It is important that the courses at the NSTEP reflect the entire spectrum of SOF capabilities and missions and go beyond the scope current operations in Afghanistan.

C. NATO SOF: AN EXPORTABLE MODEL OF INTELLIGENCE SHARING

The intelligence-sharing model that NSHQ developed fits its needs and organizational structure. The NATO structure presents a ready-made bureaucracy with delineated command relationships, IT and support infrastructure, and manning procedures. Yet the natural advantages of a long-standing operational alliance alone were not enough to create the conditions for intelligence to be shared amongst the NATO SOF members without significant challenges.

Structural changes, facilitated by the creation of the NSHQ, have helped to enhance intelligence sharing among NATO SOF members. A long-standing structure is not a prerequisite for creating a multinational intelligence sharing institution. In this respect, the NSHQ had unique access to a preexisting NATO

[113] U.S. Army Special Operations Command, SOF Truths. http://www.soc.mil/USASOC%20Headquarters/SOF%20Truths.html (accessed December 7, 2011)

framework, but lessons can still be applied to other coalition intelligence sharing partnerships, whether law enforcement, regional and international, or even economic intelligence agreements.

The most important enabler is for all members of the partnership to feel that they gain a mutual benefit from membership. While some members may contribute more intelligence than they gain from the intelligence exchange, they may gain other political, diplomatic, or economic benefits from memberships. All members must have a stake in the successful exchange of information.

Second in importance is that a basic level of trust and competency must be established among the members. The NSHQ realized there was a large gulf in *intelligence* capability amongst the NATO SOF forces, despite a smaller gap between the *operational* capabilities of the units. By creating a standard intelligence skill set via the NSTEP, the units had a smaller gap in intelligence capability, which increased the credibility of forces. As the credibility of the forces increases, so does the trust. Other organizations trying to replicate NSHQ's success should concentrate on capacity building across the force.

The NSHQ chose a model of direct control to centralize decision making for its structure. Using direct control in a diverse military organization is a natural fit, but in other intelligence sharing models, direct control may not be necessary. If another model of authority is chosen, it must clearly delineate the roles and responsibilities of each member, and it must have a way to punish violators. If the agreement doesn't have enforcement mechanisms, solving the "free-rider problem" will be difficult.[114]

The increased capability of COTS intelligence equipment and availability of open source information has a big potential to change restrictions against sharing. Historically, intelligence sources and methods were amongst a nation's most guarded secrets. Now, for a very modest investment, intelligence collection

[114] The free-rider problem, in this context, refers to a situation when an intelligence service receives intelligence, but does not provide intelligence in return. See Walsh, *The International Politics of Intelligence Sharing*, 134.

platforms are commonly available. With information collected at unclassified or lowly classified levels, nations have less to fear in exposing national intelligence capabilities and should be more forthcoming in sharing intelligence.

Secure communication systems need to be established in any intelligence sharing apparatus. Secure communications support trust, and without a secure communications, there will always be the risks of a leak. The NSHQ chose a system that they could scale rapidly and could push out to the headquarters, various operational units, and deploying units. Each organization will have different requirements, but lack of secure communications will hinder sharing and significant thought should go into selecting the appropriate C4I network.

This thesis examined several coalition intelligence sharing organizations. One common theme in successful (or partly successful) intelligence sharing organizations is that they were purpose-built. JIATF-South (counter-drugs), the NSHQ (tactical SOF operations in Afghanistan), and the PIFC (strategic intelligence in Afghanistan) all have a clear mission and mandate. Europol (transnational crime) is an example of an organization with a large scope and broad mandate; it has struggled to have its members share intelligence in a meaningful manner. Future multilateral intelligence sharing organizations should try to keep the scope of the cooperation narrow and focused to help achieve success.

While the conditions under which the NSHQ was created are unique due to its status a NATO organization, the lessons learned from its approach to intelligence sharing are valuable. Former British Prime Minister Winston Churchill once remarked, “It is no use saying ‘We are doing our best!’ You have got to succeed in doing what is necessary.”[115] In this respect, the NSHQ is doing what is necessary and has created a blueprint for other intelligence sharing organizations to follow.

[115] The Quotations Page, http://www.quotationspage.com/special.php3?file=w980510 (accessed December 1, 2011).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, Barbara D. “Trust in Small Military Teams.” http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/006.PDF, (accessed October 12, 2011).

Army Field Manual 3-05.102. *Army Special Operations Forces Intelligence*, 2001.

Axelrod, Robert. *The Complexity of Cooperation*. Princeton, Princeton University Press, 1997.

Borghese, J. Valerio. *Sea Devils*. Translated by James Cleugh. Chicago: Henry Regnery Co., 1954.

Chairman of the Joint Chiefs of Staff. “The National Military Strategy of the United States of America.” Washington, February 8, 2011. http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf (accessed February 24, 2011).

Cline, Lawrence. “Special Operations and the Intelligence System.” *International Journal of Intelligence and Counterintelligence* 8, no. 4 (2005): 575–592.

Dron, Alan. “Special Network—Alliance Aims to Improve Cooperation among Special Operators.” September 1, 2009. http://www.c4isrjournal.com/story.php?F=4211503 (accessed November 14, 2011).

Fägersten, Björn. “Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol.” *Intelligence and National Security* 25, no. 4 (2010): 500–520.

Flynn, Major General Michael, Pottinger, Captain Matt and Paul D. Batchelor. “Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.” Center for a New American Security. http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (accessed December 3, 2010).

Freikert, Andrew. “U.S. Special Operations Forces: Background and Issues for Congress.” March 2011. http://www.fas.org/sgp/crs/natsec/RS21048.pdf (accessed November 10, 2011).

Gramer, Jr., Colonel George K. “Optimizing Intelligence Sharing in a Coalition Environment: Why U.S. Operational Commanders Have an Intelligence Dissemination Challenge.” *Naval War College Thesis* (1999).

Gray, Colin. “Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?” *Parameters*. Spring 1999. http://www.carlisle.army.mil/USAWC/parameters/Articles/99spring/gray.htm (accessed March 14, 2011).

Hayden, Michael. “Prepared Remarks at the Council of Foreign Relations.” New York, September 7, 2007. https://www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html (accessed March 13, 2011).

Hull, Jeanne. “’We´re all Smarter than Any One of U.S.’: The Role of Inter-Agency Intelligence Organizations in Combating Armed Groups.” *Journal of Public and International Affairs* 2 (2008): 28–50.

Lamb, Christopher J., and Evan Munsing. *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*. Washington, D.C.: National Defense University Press, 2011.

Lefebvre, Stéphane. “The Difficulties and Dilemmas of International Intelligence Cooperation.” *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527–542.

McRaven, William. *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice*. Novato, CA: Presidio Press, 1996.

Miller, Russell. *Behind the Lines: the Oral History of Special Operations in World War II*. New York: St. Martin’s Press, 2002.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. New York: W.W. Norton, 2004.

The National Security Agency. “Declassified UKUSA Signals Intelligence Agreement Documents Available.” The National Security Agency. http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml (accessed November 4, 2011).

NATO AJP-2, “Allied Joint Intelligence, Counterintelligence and Security Doctrine P 2,” 2003.

NATO AJP 3-5, “Allied Joint Doctrine for Special Operations,” 2009.

NATO SOF Training and Education Program. “NSTEP Course Offerings.” http://www.nshq.nato.int/NSTEP/ (accessed November 1, 2011).

NATO Special Operations Headquarters. “Biennial Review.” January 2010.

NATO Special Operations Headquarters. "Special Operations Intelligence Branch," November 2010.

NATO SOF Coordination Center. *Special Operations Task Group Manual v1.0*, December 2009.

North Atlantic Treaty Organization. “NATO’s New Strategic Concept.” November 19, 2010. http://www.nato.int/strategic-concept/index.html (accessed February 24, 2011).

North Atlantic Treaty Organization Special Operations Coordination Center (NSCC). “The North Atlantic Treaty Organization Special Operations Forces Study.” December 4, 2008. http://www.nshq.nato.int/NSHQ/GetFile/?File_ID=29 (accessed February 24, 2011).

NSHQ BICES Communications & Information Systems Strategy, August 2011.

Obama, President Barack. “The National Security Strategy.” Washington, 2010. 41. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed November 4, 2011).

Parker, Glenn M. *Cross-Functional Teams: Working with Allies, Enemies, and Other Strangers*. San Francisco: Jossey-Bass, 2003.

The Quotations Page, http://www.quotationspage.com/special.php3?file=w980510 (accessed December 1, 2011).

Reveron, Derek S. “Old Allies, New Friends: Intelligence Sharing in the War on Terror.” *Orbis* 50, no. 3 (2006): 453–468.

Richelson, J.T. “The calculus of intelligence cooperation.” *International Journal of Intelligence and Counter Intelligence* 4, no. 3 (1990): 307–323.

Rust, Stephen N. “The Nuts and Bolts of Village Stability Operations.” *Special Warfare*, July-September 2011.

Salas, Eduard. *Team Cognition*. Washington, DC, American Psychological Association, 2004

Seaburn, David B. *Models of Collaboration*. New York, Perseus Books Group, 1996.

Sims, Jennifer. “Foreign intelligence liaison: devils, deals, and details.” *International Journal of Intelligence and Counter Intelligence* 19, no. 2 (2006): 195–217.

Treverton, Gregory F. *Intelligence for an Age of Terror*. New York: Cambridge University Press, 2009.

U.S. Joint Chiefs of Staff. Joint Publication 3-05, 1998.

U.S. Joint Publication 3-05 Doctrine for Joint Special Operations, 2011.

Vandenbroucke, Lucien S. *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy*. New York: Oxford University Press, 1993.

Walsh, James I. “Defection and Hierarchy in International Intelligence Sharing.” *Journal of Public Policy* 27, no. 2 (2007), 151–181.

Walsh, James I. *The International Politics of Intelligence Sharing*. New York: Columbia University Press, 2010.

Wernersen, Camilla. “Norsk Lov Utsetter Soldater for Livsfare (Norwegian Law Exposes Soldiers to Risk).” http://www.nrk.no/nyheter/norge/1.7881332 (accessed November 20, 2011).

Woodward, Bob. *State of Denial*. New York: Simon and Schuster, 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California