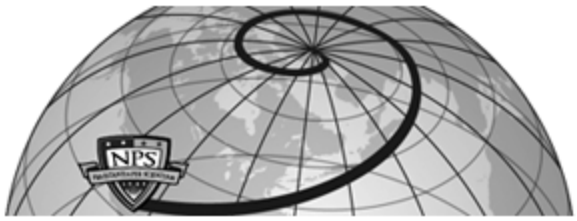

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FUSION NODES: THE NEXT STEP IN COMBATING THE GLOBAL TERRORIST THREAT

by

Timothy R. Shaw
Jason S. Mackenzie
Anthony F. Pollio Jr.

December 2011

Thesis Advisor:	Douglas Borer
Second Reader:	Leo Blanken

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Fusion Nodes: The Next Step in Combating the Global Terrorist Threat		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Timothy R. Shaw, Jason S. Mackenzie, and Anthony F. Pollio Jr.			
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** A	

13. ABSTRACT (maximum 200 words)

Implementing a proactive approach to deny, disrupt, and defeat terrorist networks that threaten U.S. national interests is a critical capability required by the U.S. government. The challenge arising from these threats stems from the semi- and non-permissive environments where U.S. freedom of action is reduced or non-existent. The purpose of this thesis is to propose a system that effectively integrates intelligence and operations in order to conduct a proactive method to global counter-terrorism (CT) operations in these arenas. This system is based on the Network Targeting Cycle- Find, Fix, Finish, Exploit, and Analyze (F3EA) utilized by USSOF most recently in Iraq and Afghanistan, but also in the recent past during the conflict in Vietnam and narco-terrorism operations in South America. The scope of this thesis is to examine how the U.S. military can develop a global CT approach using the F3EA process based on an interagency, allied, and host-nation collaborative environment.

14. SUBJECT TERMS Counter-terrorism, Fusion Node, F3EA			**15. NUMBER OF PAGES** 105
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FUSION NODES: THE NEXT STEP IN COMBATING THE GLOBAL TERRORIST THREAT

Timothy R. Shaw
Major, United States Army
B.S., United States Military Academy, 1996

Jason S. Mackenzie
Major, United States Army
B.A., North Carolina State University, 1998

Anthony F. Pollio Jr.
Major, United States Army
B.S., Hofstra University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Authors: Jason S. Mackenzie

Timothy R. Shaw

Anthony F. Pollio Jr.

Approved by: Dr. Douglas Borer
Thesis Advisor

Dr. Leo Blanken
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Implementing a proactive approach to deny, disrupt, and defeat terrorist networks that threaten U.S. national interests is a critical capability required by the U.S. government. The challenge arising from these threats stems from the semi- and non-permissive environments where U.S. freedom of action is reduced or non-existent. The purpose of this thesis is to propose a system that effectively integrates intelligence and operations in order to conduct a proactive method to global counter-terrorism (CT) operations in these arenas. This system is based on the Network Targeting Cycle- Find, Fix, Finish, Exploit, and Analyze (F3EA) utilized by USSOF most recently in Iraq and Afghanistan, but also in the recent past during the conflict in Vietnam and narco-terrorism operations in South America. The scope of this thesis is to examine how the U.S. military can develop a global CT approach using the F3EA process based on an interagency, allied, and host-nation collaborative environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AQ	Al Qaeda
AQAP	Al Qaeda in the Arabian Peninsular
AQI or AQIZ	Al Qaeda in Iraq
AQIM	Al Qaeda in the Islamic Maghreb
AQSL	Al Qaeda Senior Leaders
ARVN	Army of the Republic of Vietnam
ASD/SOLIC	Assistant Secretary of Defense for Special Operations, Low-Intensity Conflict
AUC	*Autodefensas Unidas de Colombia*
BOS	Battlefield Operating Systems
CIA	Central Intelligence Agency
CICV	Combined Intelligence Center Vietnam
COIN	Counterinsurgency
COM	Chief of Mission
CORDS	Civil Operations and Revolutionary Development Support
CT	Counterterrorism
D3A	Decide, Detect, Deliver, and Assess
DEA	Drug Enforcement Agency
DIA	Defense Intelligence Agency
DIOCC	District Intelligence and Operations Coordination Center
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
DS	Bureau of Diplomatic Security
DSCA	Defense Security Cooperation Agency
ELN	*Ejército de Liberación Nacional*
F3EA	Find, Fix, Finish, Exploit and Analyze
FARC	*Fuerzas Armadas Revolucionarias de Colombia*
FBI	Federal Bureau of Investigation

FMV	Full Motion Video
GCC	Geographic Combatant Commander
GOC	Government of Colombia
GWOT	Global War on Terrorism
HIIDE	Handheld Interagency Identification Detection System
HUMINT	Human Intelligence
HVI	High Value Individual
IC	Intelligence community
ICEX	Intelligence Coordination and Exploitation
IDF	Indirect Fire
IED	Improvised Explosive Device
IMINT	Imagery Intelligence
INR	Bureau of Intelligence and Research
ISF	Iraqi Security Forces
ISN	Bureau for International Security and Nonproliferation
ISR	Intelligence, Surveillance, and Reconnaissance
JIATF	Joint Interagency Task Force
JIEDDO	Joint IED Defeat Organization
JTF	Joint Task Force
LEGAT	Legal Attaché
MACV	Military Assistance Command
NCR	National Capitol Region
NCTC	National Counterterrorism Center
NDS	National Defense Strategy
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
NSAM	National Security Action Memorandum
NSC	National Security Council
NSS	National Security Strategy
NVA	North Vietnamese Army
OAS	Organization of American States

OCONUS	Outside Continental United States
OFAC	Office of Foreign Assets Control
OIA	Office of Intelligence Analysis
OIC	Officer in Charge
OSS	Office of Strategic Services
PIOCC	Province Intelligence and Operations Coordination Center
PoL	Pattern of Life
PRU	Provincial Reconnaissance Units
PSC	Province Security Committee
PW	Prisoner of War
RVN	Republic of Vietnam
RVNAF	Republic of Vietnam Armed Forces
S/CT	Office of the Coordinator for Counterterrorism
SIGINT	Signals Intelligence
SOCSOUTH	Special Operations Command South
SOF	Special Operations Forces
SOFA	Status of Forces Agreement
SOUTHCOM	Southern Command
SSE	Sensitive Sight Exploitation
UCP	Unified Command Plan
USEMB	U.S. Embassy
USSOCOM	United States Special Operations Command
VBIED	Vehicle Borne Improvised Explosive Device
VCI	Vietcong Infrastructure
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to acknowledge and thank the following individuals for their guidance, feedback, and advice during the writing of this thesis:

Dr. Douglas Borer
Dr. Leo Blanken

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. DIYALA PROVINCE IRAQ, INSURGENT SAFEHOUSE: 01:03 AM, 14 JUNE 2009

The door exploded. Smoke, dust, and sand cloaked a team of sixteen heavily armed men as they methodically filtered into the void and rapidly dominated every room of the mud-plastered building. In time measured by seconds rather than minutes, the team had detained and flex-cuffed all military-aged males on site and began transferring data obtained on the target. It was received instantly by the task force operations officer who was monitoring the mission's progress from a remote location via satellite. Papers and physical evidence not transferable via SATCOM were separated, photographed, bagged, and diligently annotated as to where the items were found. To accompany the items taken from the objective area, the team leader made a rough sketch of the compound, to include the layout of the building's rooms. Particular attention and care was given to the electronic media found on site, since, as was learned through tough experience, analysts could retrieve and piece together remnants of data left on hard drives and other memory devices. These sources often provided critical details on the detainee's network of associates and activities. Specially trained members of the strike team segregated and questioned each of the detainees to determine if they could garner information that may lead to an immediate follow-on target. Those individuals refusing to cooperate or deemed of possible intelligence value were identified and quickly escorted to the waiting helicopter. These individuals would receive additional screening upon return to the team's base. Once the mission commander had deemed that all intelligence of value was gleaned from the site, he issued the order to begin exfiltration. As his men and detainees moved past him to the exfiltration aircraft, he made one last sweep of the area to ensure the site exploitation team had secured everything that might have potential intelligence value.

Upon return to base, while the detention team escorted those apprehended to the screening facility, the exploitation team rushed the items seized on the objective to the

task force operations' center staff. The sense of urgency to sift through documents, disks, computer hard drives, and cellular phones was palpable. It was a well-rehearsed battle drill to pass these items to the resident exploitation experts (computer forensic, translators, and signals specialists) who would both swiftly and meticulously look for the evidence of malfeasance, as well as new information that might be actionable. While this was occurring, the remaining team members would recheck their own equipment, return to their prep area, and replace any items expended during the raid. They would then do the same to the gear of the absent team members, who would likely return soon with a follow-on mission gleaned from the captured information and material. Once the information was processed and the links established, they would re-board the helicopters, sometimes within hours of the first one, to strike the next piece of the insurgent puzzle.

B. BACKGROUND

This scenario took place on an almost daily basis, often multiple times each evening, across cities in Iraq between 2004 and 2009. U.S. Special Operations Forces had become experts at disrupting, denying, and defeating terrorist networks through a synchronized targeting cycle they perfected and called F3EA: Find, Fix, Finish, Exploit, and Analyze. It is a cycle that works.

Unfortunately, most people, both inside and outside the military, are often distracted by the explosions, the heroic warriors, the excitement and the dangers that create the popular aura of a midnight raid. They forget that the "finish" phase in the process, the action that leads to the capture or killing of a High Value Individual (HVI), is only the middle stage in a much more complex cycle. Most often, the real importance of the mission is the additional intelligence that is collected that leads one step closer to the elimination of a terror network, one terrorist, one cell, one node at a time. In the F3EA cycle, a considerable portion of the critical effort is conducted by the exploitation and analysis (or EA) teams: located "behind the wire" on forward operating bases. Working as a team, it these "EA specialists," the military intelligence officers, computer forensics technicians, and translators who develop the operational picture for the high value target.

It is through time-sensitive exploitation and analysis that they find the links, fissures, and nodes that must be severed to the collapse of the enemy network. Without them, the high-profile finish force is blind and dumb.

How did F3EA come into being? While the term F3EA has gained significant use by select counter-terrorism units, in Iraq and Afghanistan, the principles for F3EA emerged over time, and are based on historic U.S. experiences confronting threats from decentralized adversary networks. How might a broader understanding of F3EA be useful to enhancing U.S. national security? Terrorism is not a threat only faced by the United States. Can the F3EA concept be exported to allies? Under what conditions? This thesis will highlight the need for such exportation. It will propose an organizational design for a worldwide network of Operations and Intelligence Fusion Nodes that can apply F3EA to effectively conduct counterterrorism (CT) operations against transnational terrorist networks. Chapter II will examine the foundation and overview of the F3EA. The following three chapters then provide historical examples that illustrate how the process was developed in different political environments: during the Phoenix Program in Vietnam; the interdiction of narco-terrorist networks in South and Central American; and operations against the Al Qaeda terrorist network in Iraq (AQI). After examining these historic elements in the evolution of F3EA, Chapter IV will present a hypothetical scenario that illustrates the critical role a globally linked network of Fusion Nodes can play in combating the global terrorist threat. Lastly, an Appendix will provide the organizational design aspect for these Fusion Nodes.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE FOUNDATIONS OF F3EA

This chapter will provide the foundation for the F3EA process. It will begin by outlining the requirements for effective targeting of organizations that are decentralized and demonstrate how targeting these networks is different from targeting organizations that are hierarchical. It will then define some of the different environments where F3EA can occur, provide an overview of existing military targeting doctrine, and provide a detailed examination of the F3EA process. Finally, the chapter will focus on the insurgent model, highlight the importance of targeting insurgent infrastructure and explain why targeting of insurgent networks and terrorist networks are similar.

A. COUNTER-STATE VS. COUNTER-NETWORK BASED TARGETING

Historically, the U.S. military has focused on targeting enemy militaries that are large, hierarchical organizations. In previous conflicts such as WWI, WWII, Korea, and the Cold War, the threat to the U.S. was from other states, not non-state actors. However, in contrast, Al Qaeda and its regional affiliates, which are the primary focus for GWOT operations, are actually organized as a comparatively small, decentralized, scale-free network. This section will discuss the theory behind network based targeting and the balance between the size of the Find/Fix and Finish forces for the different enemy structures.

Using F3EA to conduct network based targeting in CT operations is a deliberate process that identifies key nodes that act as hubs in a network for removal. As previously discussed, it is not a piece-meal strategy that merely identifies members of the enemy organization and eliminates any target of opportunity. A fundamental property of scale-free networks is that some nodes have a large number of connections to other nodes, while the majority of nodes only have a small number of connections; these highly connected nodes are called hubs.[1] Sageman refers to AQ and its affiliates as the global Salafi jihad and describes their organizational structure as a scale-free network where "[a]

[1] Albert-Laszlo Barabasi and Eric Bonabeau, "Scale-Free Networks," *Scientific American*, May 2003, 52.

few highly connected hubs dominate the architecture."[2] Scale-free networks are extremely resilient to random removal of nodes, because any random attack will typically only remove a small number of the hubs that are critical to the survival of the network.[3] However, they are extremely vulnerable to focused attacks against the hubs, because the removal of 5 to 15 percent of the hubs can fragment the network.[4] According to Sageman, attacking the hubs and fragmenting the network can significantly reduce AQ and its affiliates' ability to conduct large-scale sophisticated terrorist attacks.[5] Identifying, Finding, and Fixing the hubs in the AQ network in order to conduct Finish operations against them is difficult and requires the correct mix of capabilities.

One of the differences between targeting a large, state, military structure and a relatively small, decentralized, scale-free network structure is the composition of the force used. Typically, a state enemy structure involves large military units that have significant amounts of military equipment. They are distinguishable from the civilian population and are significantly easier to Find and Fix. However, based on their size and firepower, conducting Finish operations against this type of enemy can be challenging. As a result, the size of the force required to Find and Fix this type of enemy is relative small compared to the size of the force required to Finish it. As an example, the intelligence section of an infantry battalion, which is approximately 500 personnel, typically has three to five intelligence specialists in it. On the opposite side of the spectrum, an enemy, such as AQ and its affiliates, has a small, decentralized scale-free network structure. Since this type of enemy consists of networks of individuals and small cells that are geographically dispersed and can easily blend into the civilian population, it can be significantly more difficult to Find and Fix targets, while Finish operations against this type of enemy can be comparatively easier than Finish operations targeting larger military organizations. In this situation, the size of the Find and Fix force is larger and the size of the Finish force smaller. See Figure 1 for a graphical representation. In

---

[2] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 137.

[3] Barabasi and Bonabeau, "Scale-Free Networks," 56.

[4] Barabasi and Bonabeau, "Scale-Free Networks," 56.

[5] Sageman, *Understanding Terror Networks*, 140.

Figure 1, the x-axis denotes the enemy organizational structure; on the left of the spectrum you have an enemy with a network based structure, while on the right you have an enemy with a state based structure. The y-axis denotes the size of the friendly force required to conduct F3EA operations against the enemy. The dotted line denotes the size of the Find/Fix force, while the solid line denotes the size of the Finish force. As is evident from the graph, as you move from a state based structure on the right to a network based structure on the left, the size of the Find/Fix force increases and while the size of the Finish force decreases. This is significant, because any organization that is designed to conduct CT operations will require an extremely robust Find/Finish element.

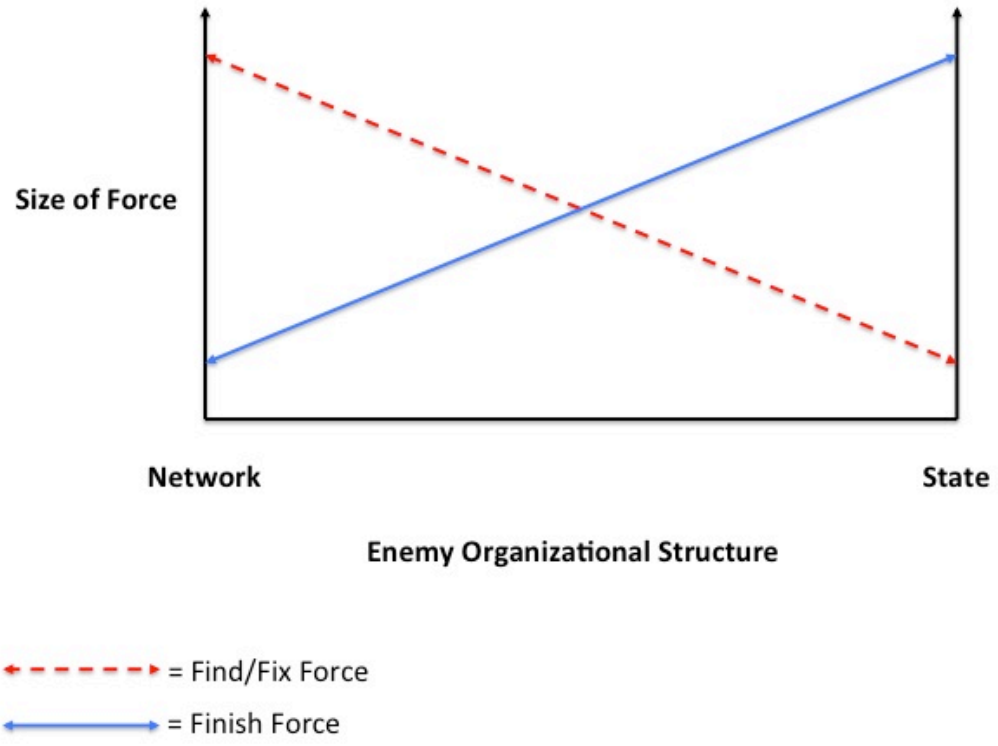

Figure 1. Find/Fix and Finish Force Size vs. Enemy Organization Structure

B. CURRENT TARGETING DOCTRINE

The conventional military defines the term targeting as part of the military decision making process used to focus battlefield operating systems (BOSs) to achieve the commander's intent. In order to accomplish this, the targeting methodology used is known as Decide, Detect, Deliver and Assess (D3A). See Figure 2.

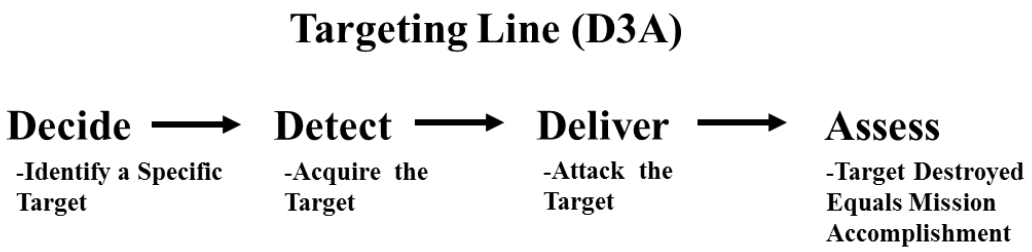

Figure 2. Decide, Detect, Deliver, and Assess (D3A) Targeting Process[6]

While it is not necessary to examine each phase of the D3A, it is important to understand that it is designed to target enemy organizations that use a hierarchical structure, not networks. Although it does have a few similarities as the F3EA, it is not the same. The reason it is not is because the D3A process is designed to destroy non-related targets such as an enemy vehicle staging areas or a tank column. The destruction of one tank column does not provide information that leads to the next column. While this targeting process is very effective during conventional war, the very nature of it does not lend itself to decentralized networks. The targeting process that is effective very effective against these types of networks is the F3EA.

C. FIND, FIX, FINISH, EXPLOIT AND ANALYZE PROCESS (F3EA)

The breaching of the door to the terrorist's house was just one phase of a targeting cycle designed to deny, disrupt, and defeat a terrorist network. The five phases of the targeting cycle are: Find, Fix, Finish, Exploitation, and Analysis (F3EA) (Figure 3).

---

[6] U.S. Army FM 3-09.12, *Tactics, Techniques, and Procedures for Field Artillery Target Acquisition*, June 2002.

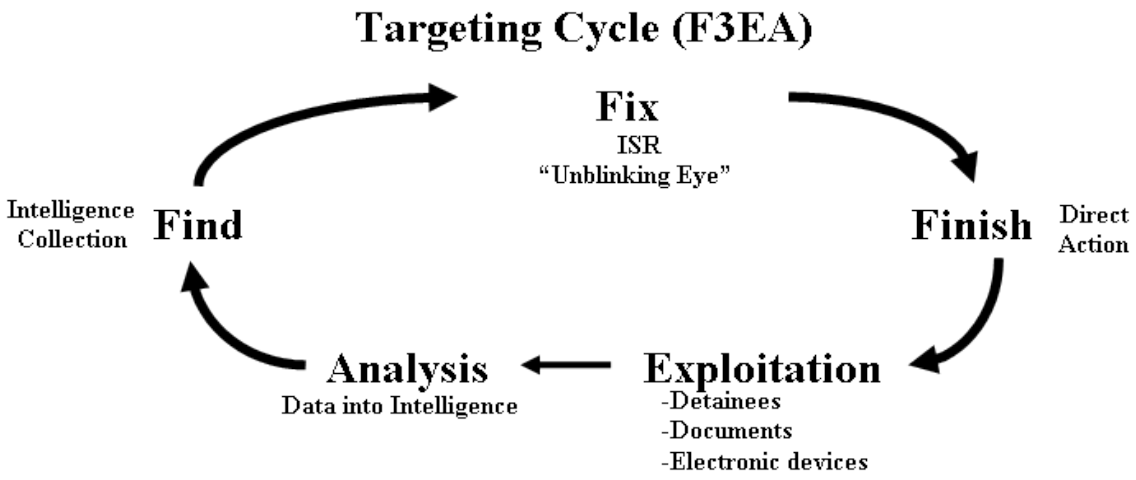

Figure 3. Find, Fix, Finish, Exploit, and Analyze Targeting Process

> The concept of the targeting cycle was to combine analysts who found the target (Find); assets such as drone to pinpoint the targets exact location (Fix); an assault force that captured or killed the target (Finish); specialists who exploited the intelligence the raid yielded (Exploitation); and the intelligence analysts who turned this raw information into usable knowledge (Analysis). The goal is to speed up the cycle for a counterterrorism operations in order to gather valuable insights in hours, not days.[7]

A thorough understanding of the targeting cycle and speed enables U.S. CT forces to attack the networks faster than the enemy can regenerate them. This is critical because it reverses the historical information advantage terrorist networks and insurgencies have over CT and COIN forces. Typically, a terrorist network or insurgency uses the population to remain underground and hidden because it has a force disadvantage. It uses its intelligence and information network to remain one step ahead of the larger security and CT forces and attack at a time and place of its choosing.[8] However, following a finish operation, terrorist network and insurgency loses the information advantage for a brief period of time because it needs to figure out who was captured or killed, what

[7] Stanley A. McChrystal, "It Takes a Network." *Foreign Policy*, March-April 2011. http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.

[8] Gordon H. McCormick, "A Systems Model of Insurgency," (Naval Postgraduate School, Department of Defense Analysis, 2006).

information was compromised, and how the security or CT forces were even able to obtain the required information to conduct the finish operation in the first place. At this point, the security or CT forces now have the information advantage. If they are able to quickly and effectively continue to utilize the F3EA targeting process, they can to degrade the network or insurgency until it is ultimately unable to reconstitute itself, and therefore defeated. In order to understand how this is possible, it is necessary to examine each phase of the targeting process.

The first phase of the targeting cycle is the find. The intent of this phase is to identify the individuals associated within the targeted network. This information can come from a variety of sources through analysis of collected intelligence. This information provides a general starting point in which to leverage resources to locate targeted individuals within the network. U.S. CT forces are able to use a vast array of technical means to facilitate this phase.

The next phase of the targeting cycle is the fixing. The key to this phase is actually locating the targeted individual. This enables information to be gathered about the individual's pattern of life (PoL) and any other potential associates of the network. U.S. CT forces utilize a combination of human intelligence and surveillance aircraft to accomplish this. This involves maintaining constant surveillance, often referred to in U.S. CT terms as the "unblinking eye" on the targeted individual. It is important to understand that a level of tactical patience is required to develop the targeted individual's PoL and associates prior to executing the third phase of the targeting cycle. Once the appropriate trigger is met, the next phase begins.

The third phase of the targeting cycle is the finishing phase. In the early hours of 2 May 2011, U.S. helicopters carrying Navy SEALs launched from a staging base in Afghanistan after meeting trigger to conduct an operation to kill or capture Osama Bin Laden in Abbottabad, Pakistan. This trigger is typically based on an established set of criteria such as human, imagery, and/or signals intelligence that produces a high degree of certainty that the targeted individual is in a specific location. Ideally, the finishing phase is ideally conducted during hours of limited visibility for two reasons. First, the targeted individual(s) are usually at their bed-down location, and therefore they are

stationary for longer periods of time. Second, it is easier during low-light hours to isolate targeted individual's location and prevent anyone from escaping before the cordon is established because most others are also asleep. The goal of the finishing phase is twofold. The first is to gather more information on the network, and the second is to kill or capture the targeted individual(s). In order to accomplish this, the question which needs to be answered before executing any finishing operation is, "How does this get us further along in regards to deny, disrupting, or defeating the entire network?" Failure to do this causes CT operations to become simply a piece-meal strategy, rather than a network approach.[9] This question also enables the finishing force to know what questions to ask and what to look for during the next phase of the targeting cycle.

The fourth phase of the targeting cycle is the exploitation. The goal of this phase is to gather as much information on the network as possible on the objective. A detailed search of the objective and good tactical questioning of detainees often provides time sensitive information, which if acted upon immediately, results in further degradation of the targeted network. To be effective, it critical to understand that the mission is not over just because the target individual was killed or captured, but rather was the start of conducting a detailed exploitation of the site to gain information about the network. Even though the Navy SEALs had killed Osama Bin Laden, they still conducted a detailed search of his compound for any items that might provide further insight into the Al Qaeda network. Often the information gathered during exploitation is time-sensitive and requires immediate follow-on objectives. A thorough exploitation provides a wealth of information that needs to be examined during the final phase of the targeting cycle.

The final phase of the targeting cycle is the analysis phase. The goal of this phase is to analyze the information gathered during exploitation and develop actionable intelligence. This intelligence consists of things such as how targeted network operates, the roles and functions of its members and where they are located. U.S. CT forces rely on a pool of intelligence analysts to sort through this data and develop potential targets.

[9] Author's Note: "Whack-a-Mole" strategy is a termed referred to when an individual pops up. This is usually after an incident occurs. It is reactive in nature and not a systematic approach to targeting and defeating a network.

One of the items recovered by the SEALs during the exploitation of Osama's compound was a series of computer files. Analysis of these files revealed that a Libyan national named Atiyah Abd al-Rahman was deeply involved in running the terror network and was in regular communication with Bin Laden.[10] On 22 August 2011, Rahman, now serving as Al Qaeda's deputy chief, was reported to have been killed by a U.S. missile strike in northwest Pakistan. It is unknown if the analysis of these files actually facilitated Rahman's death, but there is little doubt that the files elevated his priority in the U.S. targeting cycle.

D. SIMILARITIES OF INSURGENT AND TERRORIST NETWORKS

While the F3EA process is critical for conducting good unilateral CT operations, it also provides a method in which CT forces can integrate intelligence and operations for precision targeting as part of a counterinsurgency (COIN) strategy. For the purpose of this thesis, it is necessary to define several key terms in order to understand the relationship between CT and COIN. The term "terrorism" means premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents; and the term "terrorist group" means any group practicing, or which has significant subgroups which practice, international terrorism.[11] The term "insurgency" means the organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority.[12] As different as these terms are on paper, during actual operations trying to distinguish whether someone is simply a terrorist, insurgent or both is much more difficult. A good example of this is the IED cells that targeted American military forces during Operation Iraqi Freedom. By definition, these cells were not terrorists, but rather insurgents. However, due to their operating structure, cells like this were more closely aligned to

[10] Voice of America News, "US Officials Confident Al-Qaida's No. 2 Killed in Pakistan," 29 August 2011, http://www.voanews.com/english/news/US-Officials-Confident-Al-Qaidas-No-2-Killed-in-Pakistan-128592638.html.

[11] U.S. Department of State, *Country Reports on Terrorism 2010*, 18 August 2011, accessed 1 November 2011, http://www.state.gov/s/ct/rls/crt/2010/170265.htm.

[12] Headquarters Department of the Army, *FM 3-24Counterinsurgency*, 15 December 2006, Glossary 4, accessed 1 November 2011, http://www.fas.org/irp/doddir/army/fm3-24.pdf.

terrorists groups, rather than traditional military organizations. It is because of this operating structure, CT units are often ideally suited to support COIN efforts. The reason is their use of an integrated intelligence and operations network targeting process is specifically designed to disrupt, deny, and defeat these kinds of cells. By doing this, CT units can provide time for a government's military, paramilitary, political, economic, psychological, and civic actions that are necessary to defeat an insurgency to become effective.[13] This relationship can be seen Figure 4.

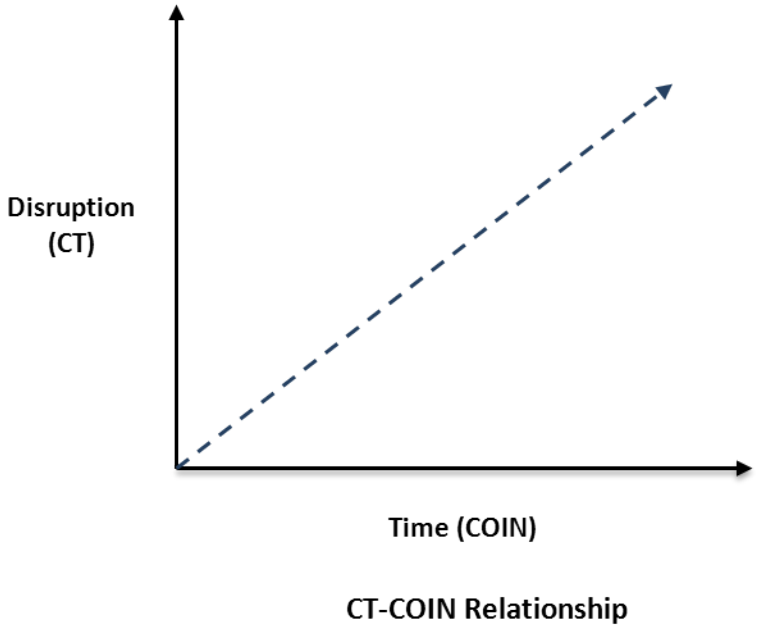

Figure 4. The CT-COIN Relationship

However, traditional type military units that are not well versed in the F3EA process and not properly resourced to do precision targeting can often have the opposite effect. In the case of Iraq, conventional forces often used large-scale sweep operations based on limited intelligence to target IED or indirect fire (IDF) networks. Not only did these operations often upset the local populace, but they also resulted in the unwarranted detention of many innocent Iraqi civilians. In addition to sweep operations, their

[13] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

attempts to use their limited ISR in an effort to target networks such as IED or IDF cells often produced little tangible results.[14] This concept can be easily summarized by understanding that good CT efforts buy time in COIN, where as bad one reduce it.

As part of this CT effort to buy time, attacking insurgent infrastructure through the means of targeting senior leadership, denying critical resources, and forcing insurgents to divert resources to defensive operations are all valuable components of a COIN campaign.[15] This effort enables the building the legitimacy of the government and establishing government control of the population, which is number one priority in COIN.[16]

In order to better understand how targeting the insurgency's infrastructure supports COIN, it is necessary to define what constitutes the insurgent infrastructure, as well as provide a brief overview of the insurgent model. An insurgent organization can be considered a system where inputs are passed through a conversion mechanism that consists of the insurgent organization's infrastructure, and the inputs are converted into outputs that are the insurgents' actions; ideally, the results of these actions should generate new inputs for the system.[17] The inputs for the insurgent system can be internal to the country and external to the country; in most insurgencies, the vast majority of inputs are generated internally, and they are impacted by insurgent outputs (actions), but it is also possible for insurgent outputs to impact the level of external support.[18] The inputs to the system are in the form of people, information, money, equipment, and logistical support, and they are typically obtained through persuasion and coercion.[19] The insurgent infrastructure that converts inputs to outputs consists of all the people that

---

[14] Anonymous Special Operations Soldier. The information referenced is the result of several conversations with an anonymous special operations soldier who had professional interaction with one of the authors during his deployments to Iraq from 2008 – 2010. For the remainder of this thesis the short reference will be Anonymous Special Operations Soldier.

[15] Nathan Leites and Charles Wolf Jr., *Rebellion and Authority: An Analytic Essay on Insurgent Conflict* (Chicago: Markham Publishing Company, 1970), 79–83.

[16] Eric P. Wendt, "Strategic Counterinsurgency Modeling," *Special Warfare*, September 2005: 5-6.

[17] Leites and Wolfe, *Rebellion and Authority*, 32–34.

[18] Leites and Wolfe, *Rebellion and Authority*, 32.

[19] Leites and Wolfe, *Rebellion and Authority*, 32–33.

organize personnel; provide financial and logistical support; provide intelligence information; and manage recruitment, training, and operations for the insurgency.[20] The outputs of the system consist of acts of violence, intimidation, military attacks, and public demonstrations.[21]

Since the models in the preceding section that were used to highlight the need to target infrastructure refer to insurgent organizations, it is important to highlight why it is valid to apply them toward global CT operations. This thesis uses Al Qaeda and its various branches as the primary terrorist threat to the United States. According to David Kilcullen, an insurgency is "a popular movement that seeks to overthrow the status quo through subversion, political activity, insurrection, armed conflict and terrorism,"[22] and terrorism is defined as "politically motivated violence against non-combatants with the intention to coerce through fear."[23] The stated goal of al Qaeda's global jihad is to overthrow the existing order and governments in the Islamic world and replace them with an Islamic Caliphate.[24] Once established, the Caliphate will then spread Islam throughout the rest of the world. Al Qaeda plans to accomplish this goal in two phases.[25] In the first phase, the main objective is to target the United States and its Western allies to force them to withdraw from the Islamic world, which will undermine Western support for existing governments in the region. This will allow al Qaeda to overthrow the existing governments in the region and enable them to establish an Islamic Caliphate. In the second phase, once the Caliphate is established, it will be used to conduct an Islamic Jihad against the West and to spread Islam to the rest of the world. As demonstrated by the terrorist attacks against the United States on 11 September 2001, terrorism has been one of the main tools used by al Qaeda to accomplish their larger political goal of coercing the West to withdraw from the Islamic world. Based on al Qaeda's goal to

---

[20] Leites and Wolfe, *Rebellion and Authority*, 34.

[21] Leites and Wolfe, *Rebellion and Authority*, 34.

[22] David J. Kilcullen, "Countering Global Counterinsurgency," *Journal of Strategic Studies* 28, no. 4 (August 2005): 603.

[23] Kilcullen, "Countering Global Counterinsurgency," 603.

[24] Kilcullen, "Countering Global Counterinsurgency," 604.

[25] Kilcullen, "Countering Global Counterinsurgency," 598.

overthrow the existing status quo and their use of terrorism to accomplish this goal, it is valid to classify their global jihadist movement as an insurgency.[26] Therefore, applying lessons from previous COIN campaigns should prove useful when developing strategies in the GWOT.

E. FRICTION POINTS AND RISK

The method to integrated operations and intelligence through the F3EA targeting cycle for global CT and supporting COIN seems like an easy process to follow. Apply it properly with enough speed and resources and all the terrorists' networks should be defeated. This begs the question, why in reality is this not the case? The answer is friction. Clausewitz defines friction as the "only concept that more or less corresponds to the factors that distinguish real war from war on paper."[27] When it comes to trying to apply the FE3A process in the real world, it faces friction in two categories. The first is objective or capabilities friction. This friction consists of things such as having enough resources such as ISR, technical intelligence equipment, timely and accurate intelligence, translators, intelligence analysts, sensitive site exploitation equipment, finishing forces, aircraft, and screening/detention facilities. The second category is subjective friction. This consists of things such as political approval, organizational culture, battle-space deconfliction, sensitive intelligence and operational sharing and dissemination, approval authorities, competing agendas by different units and agencies, and host-nation cooperation. In addition, these two categories are affected by different operational environments. In countries like Somalia, which is considered a failed state, the United States does not have to seek the same approval requirements to fly ISR compared to a politically less permissive country such as Pakistan. The different environments and friction points make actually utilizing the F3EA targeting process much more difficult in the real world.

---

[26] Kilcullen, "Countering Global Counterinsurgency," 604.

[27] Carl Von Clauswitz, *On War*, trans. Michael Eliot Howard and Peter Paret (Princeton: Princeton University Press, 1989), 119.

As difficult as this is, there is a way to help overcome these real-world challenges. We will argue in Chapter VI the method to do this is by establishing a series of globally connected fusion nodes that thoroughly understand the operational environment and grease potential friction points in order to effectively enable the F3EA targeting process to deny, disrupt and defeat transnational terrorist networks. The next three chapters will use historical examples to illustrate how the F3EA targeting process was utilized in different operational environments and the different friction points it encountered.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LESSONS FROM VIETNAM

A. INTRODUCTION

During the Vietnam War, a program that was designed to target Viet Cong Infrastructure (VCI) was the Phoenix Program.[28] This chapter analyzes aspects of the Phoenix Program, and it identifies key lessons that can be applied toward improving the effectiveness of current operations targeting the global terrorist network infrastructure of al Qaeda and its regional affiliates. It begins by looking at the background of the Phoenix Program, which includes the political context that existed when the Phoenix Program was initiated, an overview of the VCI, and the history of the program. This is followed by an analysis of how the Phoenix Program conducted the different phases of the Find, Fix, Finish, Exploit and Analyze (F3EA) targeting cycle. From this analysis, the paper identifies the friction points encountered by the Phoenix Program, both objective and subjective, and how they affected operations. Objective friction points that affected operations included the political environment and resources, while subjective friction points included unity of effort and legitimacy.

B. POLITICAL CONTEXT

On 22 November 1963, after the assassination of President Kennedy, Lyndon B. Johnson assumed the presidency of the United States. At the time, the U.S. had approximately 16,263 military personnel in South Vietnam.[29] In 1964, President Johnson increased the U.S. military presence in the south to approximately 40,000.[30] By the end of 1965, he had adopted a military strategy that would deploy an additional 100,000 military personnel to South Vietnam and included sustained bombing of North Vietnamese targets.[31] This strategy was not intended to defeat North Vietnam; rather, it

---

[28] William Rosenau and Austin Long, *The Phoenix Program and Contemporary Counterinsurgency*, Research Paper, RAND National Defense Research Institute (Arlington: RAND Corporation, 2009), iii.

[29] Henry Kissinger, *Diplomacy* (New York: Simon & Shuster, 1994), 653.

[30] George C. Herring, *America's Longest War: The United States and Vietnam*, 1950-1975 (New York: Wiley, 1979), 146.

[31] Herring, *America's Longest War*, 150–153.

was designed to inflict high costs on North Vietnam for supporting the communist insurgency in the South and force the North Vietnamese to negotiate a peace settlement acceptable to the United States.[32]

Soon after becoming president, Johnson ordered a review of American policy in Vietnam. This review concluded that the United States should continue its existing policies in Vietnam, but it should strive to implement its policies more efficiently, and it emphasized the importance of an independent, non-communist government in South Vietnam.[33] As a result of this review, President Johnson approved the objectives outlined in National Security Action Memorandum (NSAM) 288. The main objectives in NSAM 288 were to establish stable political leadership in South Vietnam, to provide programs that fostered economic development for the rural population, and to assist in the training of a guerilla force to augment the conventional South Vietnamese Army (ARVN).[34] This policy stressed the importance of self-reliance on the part of the South Vietnamese government, and resulted in an immediate $50 million dollar increase in the amount of economic aid; it also increased the number of U.S. military advisors from 16,300 to 23,300.[35]

During this same period, significant political and military problems within the South Vietnamese government had an impact on the strategy that President Johnson pursued. Less than a month prior to the assassination of President Kennedy, President Diem of South Vietnam was assassinated. Prior to Diem's assassination, the political situation had been steadily deteriorating, and the United States viewed the South Vietnamese government as ineffective. While the United States did not play an active role in Diem's assassination, it is believed they did encourage Diem's removal with the hope that it would improve governance in the South. However, after Diem's assassination, the political situation became even more chaotic.

---

[32] Herring, *America's Longest War*, 156.

[33] Herring, *America's Longest War*, 130.

[34] Guenter Lewy, *America in Vietnam* (Oxford: Oxford University Press, 1980), 30.

[35] Herring, *America's Longest War*, 130.

In 1964 alone, there were seven different governments in South Vietnam, and none of them were viewed as competent or popular among the South Vietnamese population; the political situation had gone from bad to critical. As a result of the political chaos, the military situation was also worsening and the Vietcong controlled large portions of the population in key areas outside of Saigon. Additionally, it was discovered that the optimistic reports that the Diem regime had been producing about the strategic hamlet program were false. These factors, along with the low morale and numerous defeats of the South Vietnamese Army, led the United States to the conclusion that South Vietnam would collapse unless the United States increased its role in the war.[36]

C. THE HISTORY OF THE PHOENIX PROGRAM

As of 1965, the U.S. Embassy in Saigon controlled the civilian stabilization efforts in Vietnam, while Military Assistance Command Vietnam (MACV) controlled the military advisor efforts that were focused primarily on training the Republic of Vietnam Armed Forces (RVNAF).[37] As the efforts to support the Republic of Vietnam's (RVN) pacification program increased, "the embassy began to reach its organizational limits"[38] to run and coordinate the various U.S. civilian agency programs. In May 1967, in an effort to concentrate U.S. support to RVN pacification programs, the office of Civil Operations and Revolutionary Development Support (CORDS) was created under the control of MACV. During this period, included among the various RVN pacification programs, was a renewed focus on targeting the VCI. The effort to target the VCI was intended to disrupt and degrade the VC, which would improve security and enable other COIN efforts to be more effective.

Even before the beginning of the Phoenix Program there was a need for improved intelligence and operations fusion. As a result, in June 1967, the Director of CORDS,

---

[36] Lewy, *America in Vietnam*, 25–28.

[37] Richard W. Stewart, "Chapter 8. CORDS and the Vietnam Experience: An Interagency Organization for Counterinsurgency and Pacification," in *Project on National Security Reform Case Studies Volume I*, 451-481 (Washington DC: Center for the Study of the Presidency, 2008), 454.

[38] Stewart, "Chapter 8. CORDS and the Vietnam Experience," 454.

Ambassador Robert Komer, received approval to establish the Intelligence Coordination and Exploitation (ICEX) program, which later became Phoenix.[39] Once established, the Phoenix Program consisted of two elements.

The first element was designed to fuse intelligence and operations, and to promote intelligence sharing between the various U.S. and South Vietnamese agencies involved in the program. The overall intent was to improve the effectiveness of operations targeting the VCI. The name for the U.S. contribution to this portion of the program was Phoenix, while the South Vietnamese contribution was called Phung Hoang, which is the Vietnamese name for a mythical bird that resembles a Phoenix. In order to improve coordination, a series of Province Intelligence and Operations Coordination Centers (PIOCCs) and District Intelligence and Operations Coordination Centers (DIOCCs) were established. The South Vietnamese provided the majority of the manning for these coordination centers, and South Vietnamese personnel came from across a wide spectrum of military, civilian, and law enforcement agencies.[40] On the U.S. side, the CIA provided the majority of advisors at the provincial level, while MACV CORDS provided military advisors at the district level; "[b]y 1970, more than 700 [U.S.] advisors were serving in Phoenix."[41] Additionally, in their VCI targeting campaign, the program leveraged the efforts of other combined U.S./South Vietnamese intelligence organizations, such as the Combined Military Interrogation Center, the Combined Document Exploitation Center, the Combined Materiel Exploitation Center, and the Combined Intelligence Center Vietnam (CICV). In particular, the CICV contained a Political Order of Battle Section that maintained thousands of dossiers on suspected VCI personnel.[42]

The second element of the program was the action-arm that targeted the VCI. While numerous law enforcement and military agencies within the RVN supported the program, the main action-arm element of the program consisted of South Vietnamese Provincial Reconnaissance Units (PRUs) that were sponsored by the Central Intelligence

[39] Rosenau and Long, *The Phoenix Program*, 7.

[40] Rosenau and Long, *The Phoenix Program*, 7–8.

[41] Rosenau and Long, *The Phoenix Program*, 8.

[42] Rosenau and Long, *The Phoenix Program*, 8–9.

Agency (CIA). The CIA had the primary role of training, paying, and advising the PRUs; however, the CIA received support from U.S. Army Special Forces to perform these functions.[43] In essence, the PRUs were a highly trained, well-equipped and better-paid South Vietnamese police force that leveraged detailed intelligence to target the VCI.[44] The majority of PRU members had previous experience in elite South Vietnamese military units, and U.S. advisors helped plan and participated in operations.[45] Many PRU members had also lost family members due to VC violence and were highly motivated in their efforts. Additionally, the PRUs typically operated in their home province, so their understanding of the local environment was exceptional, which enabled them to establish extensive networks of informants and personal contacts.[46] The primary mission of the PRUs was to apprehend VC cadre and exploit them for intelligence purposes.[47] In the words of one American PRU advisor, "prisoner snatches were key. You can't get information out of a dead man."[48] The PRUs also used their influence to encourage VCI personnel to defect.

D. F3EA AND THE PHOENIX PROGRAM

As previously stated, currently, the preferred method of targeting insurgent and terrorist network infrastructure is F3EA. This section seeks to determine how the functions of F3EA were conducted to target the VCI during the Vietnam War, and to identify key lessons that can be applied to the GWOT. The authors acknowledge that the targeting methodology used in the Vietnam War was not specifically referred to as the F3EA cycle. However, under the Phoenix Program, the targeting effort did perform each phase of the F3EA cycle. The following sections will provide an overview of the F3EA targeting process and then examine how the Phoenix Program performed them.

---

[43] Rosenau and Long, *The Phoenix Program*, vii.

[44] Rosenau and Long, *The Phoenix Program*, 11.

[45] Rosenau and Long, *The Phoenix Program*, 12.

[46] Rosenau and Long, *The Phoenix Program*, 11.

[47] Rosenau and Long, *The Phoenix Program*, 10.

[48] Rosenau and Long, *The Phoenix Program*, 11.

1. Find and Fix

In the find phase, multiple sources of intelligence, such as signals intelligence (SIGINT), human intelligence (HUMINT), and imagery intelligence (IMINT), are fused to identify critical nodes in the insurgent network for targeting. Much of the intelligence used in this phase is typically generated during the exploit and analyze phases of previous operations. In the find phase, the intent is to find a target among the larger civilian population and identify a general operating area for the target; "the most difficult task in [combating] insurgencies is finding the enemy."[49]

In the fix phase, again, multiple sources of intelligence are used, but now the intent is to generate a detailed picture on the targets pattern of life. The ultimate goal in this phase is to identify the targets exact location at a specific moment in time. During both the find and fix phase detailed information is also being generated on how the target fits into the overall network, specifically, the targets role in the network, and who else the target interacts with in the network. At this point, a key decision must be made; should the target be removed from the network, or should the target continue to be exploited for additional information about the network.[50] Often times, it is more beneficial to continue to collect intelligence on the target rather than to eliminate the target from the network. While not specifically mentioned in the literature, during the find and fix phases, if appropriate, efforts can also be applied to encourage the target to defect from the insurgent organization. Defection can be either overt, where the target openly leaves the insurgent organization and cooperates with friendly forces, or it can be covert, where the target is recruited as a HUMINT source within the insurgent network.

In order to conduct find and fix operations, the Phoenix Program attempted to enhance collaboration between the U.S. and Vietnamese forces and it placed an emphasis on using Vietnamese personnel for intelligence collection. The entire intent of the Phoenix Program was to improve the effectiveness of VCI targeting by increasing collaboration between the U.S. and South Vietnamese, and by increasing interagency

[49] Flynn et al., "Employing ISR: SOF Best Practices," 56–61.

[50] Flynn et al., "Employing ISR: SOF Best Practices," 56–61.

collaboration within the South Vietnamese government. This emphasis on collaboration led to the establishment of the PIOCCs and DIOCCs to help develop the detailed collection required to find and fix members of the VCI. MACV Directive 381-41 specifically states:

> At each level, the designated U.S. ICEX coordinating elements will be charged with coordinating and focusing the intelligence and operational attack on infrastructure, and with stimulating, energizing, guiding and collaborating with the corresponding Vietnamese organizations effort.[51]

MACV recognized that in order to be able to find and fix members of the VCI, they would need to create intelligence and operations fusion nodes at all levels. Additionally, by assigning PRU teams to their home province, the PRUs were able to establish extensive intelligence collection networks that greatly enhanced their ability to find and fix targets.

The Phung Hoang Advisor's Handbook provides excellent insight into how the find and fix phases were accomplished. According to the handbook:

> Once a suspect VCI is identified (name and VCI position are known) … the next step is to develop a VCI Target Folder on the individual; a good target folder will enable the cadre to be specifically targeted (you will know his habits, contacts, schedules, and modus operandi).[52]

As can be seen from the handbook, the first step in the targeting process was to identify a potential member of the VCI through existing intelligence. Once the potential target was identified, a target folder was created and the intelligence effort was focused to conduct pattern-of-life analysis on the target, identify the larger network, and determine how the target fit into that network. The PIOCCs and DIOCCs placed considerable emphasis on identifying and targeting the network as a whole, not just the individual VCI member.

---

[51] U.S. Military Assistance Command Vietnam, *MACV Directive 381-41: Intelligence Coordination and Exploitation for Attack on VC Infrastructure*, (San Francisco, July 9, 1967).

[52] U.S. Military Assistance Commad Vietnam, *Phung Hoang Advisors Handbook* (San Francisco, November, 20 1970), 9.

This point is emphasized in the handbook, "consistently up-dated organization charts will particularly aid in the development of operations to neutralize entire VCI staff elements or organizational echelons."[53]

2. Finish

Once it is determined that a target should be removed from the network, then, the process moves into the finish phase. More emphasis is usually placed on capturing a target, because it allows the collection of additional intelligence about the insurgent network to be gathered during interrogation operations.[54] Additionally, Sensitive Site Exploitation (SSE) is also a critical part of finish operations. SSE consists of gathering all electronic equipment, such as cell phones, computers, laptops, PDAs, and other devices, as well as any documents and pocket litter that may be found during a finish operation. Items gathered during SSE can provide additional information on the network and prove useful during interrogation operations.

Finish operations were one of the most controversial aspects of the Phoenix Program. Part of the difficulty was related to the status of suspected VCI cadre. North Vietnamese (NVA) and VC military cadre that were members of the VCI received Prisoner of War (PW) status under the Geneva Conventions, while civilian members of the VCI were considered civil defendants.[55] Critics of the Phoenix Program claimed that it was "a merciless assassination campaign"[56] that represented the excessive violence used by U.S. forces; however, assassination was not part of the official Phoenix policy.[57] This is clearly highlighted in MACV Directive 525-36:

> Operations against the VCI include: the collection of intelligence identifying these members, inducing them to abandon their allegiance to the VC and rally to the government, capturing or arresting them in order to bring them before province security committees for lawful sentencing, and

---

[53] MACV, *Phung Hoang Advisors Handbook*, 9.

[54] Flynn et al., "Employing ISR: SOF Best Practices," 56–61.

[55] MACV, *Phung Hoang Advisors Handbook*, 15.

[56] Rosenau and Long, *The Phoenix Program*, 1.

[57] Rosenau and Long, *The Phoenix Program*, 1.

> as a final resort the use of military, or police force against them-if no other way-of preventing them from carrying on their unlawful activities is possible. Our training emphasizes the desirability of obtaining these target individuals alive and of using intelligent and lawful methods of interrogation to obtain the truth of what they know about other aspects of the VCI.[58]

In the finish phase, the Phoenix Program placed an emphasis on encouraging defections and attempting to capture targets verses killing them. This was beneficial because debriefing a defector or interrogating a prisoner provided critical intelligence on the enemy infrastructure network. Again, in the finish phase the use of Vietnamese forces as the primary action-arm proved to be extremely beneficial. As a result of their detailed knowledge of the operating environment, they were able to conduct highly effective finish operations, very rapidly, once a target was found and fixed.

3. Exploitation and Analysis

Next the process moves into the exploit and analyze phase. According to the former senior intelligence officer for the Joint Special Operations Task Force in Iraq, Major General Michael Flynn, "[e]xploit – analyze is the main effort of F3EA because it provides insight into the enemy network and offers new lines of operations."[59] The use of analysts from across the numerous intelligence agencies that are part of the intelligence community (IC) working in a collaborative environment is critical, because these analysts can leverage their unique perspectives and the resources of their parent organizations. It is also key to ensure that any items that were recovered during the SSE in the finish phase are thoroughly exploited and the intelligence obtained is rapidly disseminated.

Members of the Phoenix Program understood the importance of exploiting actionable intelligence. MACV Directive 381-41 highlights this point, "[p]rogress and

---

[58] House of Representatives Ninety-Second Congress First Session, "U.S. Assistance Programs in Vietnam," in *Hearings Before a Subcommittee of the Committee on Government Operations* (Washington: U.S. Government Printing Office, 1971), 329–330.

[59] Flynn et al., "Employing ISR: SOF Best Practices," 56–61.

success clearly will depend on a variety of interrelated factors, including … [m]ore selective targeting, and timely exploitation of operational intelligence."[60]

In the exploit and analyze phases, the Phoenix Program also provides a key lesson. Collaboration was emphasized in the exploit and analyze phases by leveraging the Combined Military Interrogation Center, the Combined Document Exploitation Center, the Combined Materiel Exploitation Center, and the Combined Intelligence Center Vietnam (CICV). The intelligence derived from this collaborative approach enabled the development of thousands of dossiers on suspected VCI cadre, which then generated new targets for the find and fix phases.

E. FRICTION POINTS

As described above, while the Phoenix Program did not refer to the targeting process as F3EA, the program did perform the same functions as the various phases of the F3EA process to target the VCI. Therefore, an examination of the friction points that were encountered by the Phoenix program can provide valuable lessons on how to design targeting efforts against the global terrorist network infrastructure of AQ and its affiliates. Friction points, as defined in Chapter 1, can be both objective and subjective. This section will examine major friction points is the design of the Phoenix Program that had an impact on operations. Objective friction points that affected operations included the political environment and resources, while subjective friction points included unity of effort and legitimacy.

1. Objective Friction Points

The first objective friction point that impacted the program was the political environment in South Vietnam. Two factors that help to determine a particular states ability to deal with a specific challenge are its capabilities and its will. These factors define the political environment. Ideally, it is best for the U.S. to have a partner that is both capable and willing. However, in the case of Vietnam, as previously mentioned, the RVN's poor performance and limited abilities to deal with the conflict are what prompted

[60] Military Assistance Command Vietnam, *MACV Directive*, 381–41.

President Johnson to drastically increase the presence and role of U.S. forces to prevent a total collapse of South Vietnam. The large increase of U.S. forces actually provided a security umbrella that allowed the RVN to renew its efforts "to establish a wide range of programs for governmental administration, economic development, regional security, refugee control, anti-Viet Cong infrastructure, national police, and other pacification or counterinsurgency activities."[61] While during the Vietnam War the U.S. only had to operate in a single political environment, due to the global nature of the AQ network, worldwide CT operations will have to be tailored to adjust to the political environments of numerous host nations with varying levels of capability and will.

Resources are another objective friction point that impacted the Phoenix Program. Personnel, specifically the quality of the advisors, were the main resource that created friction for the Phoenix Program. The more experienced CIA advisors functioned at the provincial level. However, due to the limited resource of CIA personnel, the advisors at the district level were military advisors that sometimes lacked experience and the skills required to make them effective.[62] An excerpt from the Phung Hoang Advisor's Handbook makes it apparent that leaders of the program recognized this problem: "The disadvantages of youth and low rank can be overcome by initial eagerness to learn what your counterparts can teach you and by taking action only when you are sure of your grounds."[63] In order to compensate, the Phoenix Program established an in-country advisors orientation course. The course was designed to "acquaint both PHUNG HOANG Advisors and other personnel with those GVN agencies that support[ed] the PHUNG HOANG Program and with the problems encountered within the program."[64] The orientation course also included a two-day practical exercise to familiarize the trainees with DIOCC operations.[65] The lesson for global CT operations is clear. Personnel need to be experienced and well trained to be effective.

---

[61] Stewart, "Chapter 8. CORDS and the Vietnam Experience," 453.

[62] Ken Tovo, *From the Ashes of the Phoenix: Lessons for Contemporary Counterinsurgency Operations*, (Carlisle Barracks: U.S. Army War College, 2005), 13.

[63] MACV, *Phung Hoang Advisors Handbook*, 11.

[64] MACV, *Phung Hoang Advisors Handbook*, 19.

[65] MACV, *Phung Hoang Advisors Handbook*, 19.

2. Subjective Friction Points

The first subjective friction point is unity of effort. CORDS, the larger organization that encompassed the Phoenix Program, "placed nearly all civilian and military interagency assets involved in the pacification struggle under one civilian manager – and then subordinated that individual to the military hierarchy as a Deputy Commander of Military Assistance Command Vietnam."[66] This allowed the CORD's leadership to conduct centralized planning, coordinate resources more effectively and to synchronize the efforts of the various interagency partners under their control. The Phoenix Program attempted to generate this same level of unity of effort by establishing the PIOCCs and DIOCCs. However, while CORDS forced cooperation at the upper levels, cooperation at the lower levels was not as effective, especially in the area of intelligence sharing. As a result of interagency rivalries, the various intelligence organizations at the PIOCC and DIOCC level often refused to share intelligence. Unity of effort will be an essential element for future CT operations.

Legitimacy was the friction point that probably had the greatest impact on the Phoenix Program. Two aspects that undermined legitimacy were the extrajudicial aspects of the program and the system of metrics used to track the progress of the program.

The extrajudicial ability to sentence suspected VCI cadre members drew significant criticism from some members of the U.S. Congress, which undermined the legitimacy of the Phoenix Program. Once a suspect was captured, he was brought before a Province Security Committee (PSC). The PSC was able to order the "administrative detention of those persons reasonably believed to endanger the national security, but against whom sufficient evidence for a trial [was] lacking."[67] The committees had the authority to sentence suspected VCI cadre to administrative detention, known as "an tri" detention. It was not necessary to prove that an individual broke the national security laws of the RVN, it only had to be demonstrated that a "reasonable belief exists that the

[66] Stewart, "Chapter 8. CORDS and the Vietnam Experience," 603.

[67] Ninety-Second Congress, "U.S. Assistance Programs in Vietnam," 331.

suspect threatens the national security."[68] Congressional criticism of the program focused on the potential for abuses inherent in the "an tri" system. Members of congress were concerned that the U.S. was helping the RVN establish mechanisms for political suppression of the South Vietnamese population in which the amount of evidence required to detain a person was dangerously low. An additional area of concern highlighted in the congressional testimony was why U.S. forces had to be specifically prohibited from conducting assassinations under MACV Directive 525-36. Members of Congress believed that the prohibition to participate in assassinations was proof that the RVN was conducting assassinations.[69]

Detailed metrics were collected on the number of VCI neutralized under the program. A person was considered neutralized if they were killed, if they defected to the government, or if they received a prison sentence greater than one year.[70] As part of collecting metrics, neutralization quotas were placed on the various units that supported the Phoenix Program. In an effort to meet quotas, it is believed that innocent civilians were sometimes arrested.[71] It is also possible that the desire to meet neutralization quotas caused the PSCs to administer longer detentions, because a detention had to exceed one year for a suspected VCI cadre to be considered neutralized.

F. CONCLUSION

This chapter has outlined lessons from the Phoenix program that can be applied to targeting operations in the GWOT. Any program that is designed to conduct F3EA operations will inevitably encounter friction points. By examining the friction points from the Phoenix Program, the U.S. can design a structure that attempts to eliminate or reduce these friction points. Specifically, the Phoenix Program demonstrates that key friction points that must be considered are the political environment, the quality and ability of human resources, unity of effort and the legitimacy of any efforts. Considering

---

[68] Ninety-Second Congress, "U.S. Assistance Programs in Vietnam," 331.

[69] Ninety-Second Congress, "U.S. Assistance Programs in Vietnam," 331–332.

[70] Ninety-Second Congress, "U.S. Assistance Programs in Vietnam," 328.

[71] Tovo, *From the Ashes of the Phoenix*, 12.

the GWOT began on 11 September 2001, any lessons from history that may improve overall effectiveness are worth further exploration and consideration.

IV. FROM ESCOBAR TO JIATF-SOUTH

A. INTRODUCTION

This chapter analyzes aspects of the manhunt for the drug cartel kingpin, Pablo Escobar, and the United States subsequent efforts to counter the narco-terrorist and illicit drug trafficking problem. Unlike the campaign in Vietnam, elements of the U.S. national security apparatus operated in a sovereign nation that it was not at odds with, and operating in conjunction with its security forces, to counter its internal threat. Within this environment, the U.S. elements operated both overtly and covertly under predominantly restrictive authorities in order to aid the Government of Colombia's (GOC) search and prosecution of Escobar's Medellín Cartel. Like the operations in Vietnam, the U.S. utilized a targeting process that also incorporated the efforts of the host nation, in this case the various security agencies. It also identifies key lessons that can be applied toward improving the effectiveness of current operations targeting the global terrorist network infrastructure of al Qaeda and its regional affiliate. The chapter begins by looking at the background of the U.S. relations in Central and South America following WWII, provides an overview of Escobar's rise to power, and the ensuing fragmentation of the cartels after his demise. This is followed by an evaluation of how the U.S. government conducted the different phases of the Find, Fix, Finish, Exploit and Analyze (F3EA) targeting cycle relating to the case. From this analysis, the chapter identifies the friction points encountered during the man-hunting mission, both objective and subjective, and how the U.S. adopted an interagency approach to counter the later challenges that arose. Objective friction points that affected operations included the environment and resources, while subjective friction points included unity of effort, legitimacy, and leadership.

B. BACKGROUND

In the aftermath of World War II, twenty-two countries in North, Central, and South America sought to enhance their partnership and create a system of collective security by signing the Inter-American Treaty of Reciprocal Assistance in 1947. Less

than one year later, all but one of these same countries joined to form the Organization of American States (OAS) in response to the perceived threat of the spread of communism.[72] The United States and its OAS partners benefited from these mutually beneficial relationships with an enhanced sense of security and through regional and economic cooperation. The effects of these coalition efforts played a role in the modernization and professionalization of OAS member states security forces as witnessed by U.S. Southern Command observers in the late 1980's.[73] It also created a collaborative environment, which enabled U.S. policy makers and defense officials to build lasting partnerships in aiding those countries in combating their own internal regional problems.[74]

One such benefit of OAS relationships came to bear in Colombia, when U.S. Department of Defense Special Operations Forces (SOF) assisted host nation forces in targeting Pablo Escobar, the cocaine kingpin of the Cartel de Medellín. This was one of the first successful cases in the post-Cold War era that U.S. SOF would test a capability often practiced, but rarely put into action, man-hunting. Unlike the dismal failure to capture General Mohammed Farah Aideed in Somalia in the fall of 1993, military liaison, working covertly and in conjunction with interagency partners, merged U.S. intelligence efforts with those of the Colombian *Bloque de Busqueda* (Search Bloc) in order to enhance their counter-cartel missions.[75] The persistence and professionalism of the U.S. soldier-diplomats led to a successful finale to the Colombian government's ultimate endeavor, the demise of the "world's greatest outlaw." Although it would take over a decade before U.S. SOF would perfect and coin the commonly termed phrase, operators in Colombia effectively applied the tenets of the Find, Fix, Finish, Exploit, and Analyze

---

[72] *Our History: Organization of American States.* 2011. http://www.oas.org/en/about/our_history.asp (accessed October 2, 2011).

[73] Kenneth, Finlayson, "Colombia: A Special Relationship," *Veritas: Journal of Army Special Operations History* 2, no. 4 (2006): 5–7.

[74] Chris Kraul, "Colombia assuming instructor role for other militaries." *www.LATimes.com.* March 6, 2011. http://articles.latimes.com/2011/mar/06/world/la-fg-colombia-mexico-pilots-20110306 (accessed March 14, 2011). Colombian forces are training Mexico and 13 other Latin American and Caribbean countries on counter-narcotic missions.

[75] Mark Bowden, *Killing Pablo: The Hunt for the World's Greatest Outlaw* (New York, NY: Atlantic Monthly Press, 2001), 206–208.

(F3EA) cycle to target Pablo Escobar while successfully establishing interagency and international (joint and combined) fusion of intelligence.[76]

As in many cases involving the removal of a key figure in a controversial organization, the negative side effects of Escobar's targeted killing included the decentralization and spreading of the Colombian drug industry into hundreds of smaller "mini-cartels" that spread from the confines of the nation to become a transnational problem.[77] To further exacerbate the problem, many of the burgeoning cartels developed alliances with destabilizing actors, such as the *Fuerzas Armadas Revolucionarias de Colombia* (FARC), in mutually supporting relationships that would provide protection for the cartels and a source of income for the FARC. This exponentially increased the difficulty for the Colombian security forces, which quickly spread to other South and Central American countries. Fortunately, the multi-national ties fostered by the OAS, the interagency and military partnerships established with the Colombians, and the evolution of the Joint Interagency Task Force-South (JIATF-South), provided a baseline structure for effectively targeting the expanding narco-terrorist network.

C. THE TARGETING CYCLE

The search for tangible effects on the "War on Drugs" frustrated U.S. policy makers as early as the late nineteenth century.[78] As in most cases, targeting a problem that is rooted with many variables requires a synergistic approach. The bi- and multi-lateral approaches made possible through OAS cooperation created a medium for nations to collaborate on approaches to fluid, transnational problems such as the evolving drug trade. However, traditional methods of throwing money at the problem via foreign aid packages and security assistance training were not adequately stemming the problem. As this challenge elevated to a national security concern in the mid-1980s, decision makers

---

[76] Michael T. Flynn, Rich Juergens and Thomas L. Cantrell, "Employing ISR: SOF Best Practices," *Joint Force Quarterly*, no. 50 (3d Quarter 2008): 57. The F3EA cycle is an aggressive targeting model that fuses all-source intelligence to achieve operational effects on the battlefield.

[77] David T. Buckwalter, and Struckman, Dana T. "Colombia: Mission Impossible?" In *Case Studies in Policy Making, 11th Edition*, by Alvi-Aziz, Hayat and Knott, Stephen F., eds. Newport, RI: Naval War College, 2008, 81.

[78] NPR, "Timeline: America's War on Drugs," 02 April 2007, accessed 05 October 2011, http://www.npr.org/templates/story/story.php?storyId=9252490.

began seeking additional methods to thwart the lucrative drug trade. These leaders needed something more tangible to target than the billion dollar Colombian cash crop; the persona of Pablo Escobar provided this object.

The act that propelled Escobar into the public spotlight, and brought him to national attention, was through his involvement in the Avianca Flight 203 bombing on 27 November 1989. This single action thrust him into the cross hairs of the U.S. National Security Council as a result of the death of two luckless U.S. citizens onboard.[79] It also provided the impetus for bi-lateral covert action and enhanced cooperation between the Colombian and U.S. governments in a mission to capture or kill, at the time, the most famous narco-terror leader in the Americas. Leading the effort fell into the lap of the U.S. Ambassador to Colombia, Morris D. Busby, who instituted a whole-of-government approach to targeting Escobar and his cartel. Under his direction, the USEMB Joint Task Force (JTF) and concurrently, the Colombia Task Force, were created to assist in the apprehension of Escobar and other members of the Medellín Cartel.[80] Components of the JTF included elements of the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and SOF Operators all merged in an adhocratic fusion cell to aid Colombian security elements.[81] Thus began "the hunt for the world's greatest outlaw."

1. Find, Fix, and Finish

Significant to the man-hunting operation to apprehend Escobar was the fact that a small element of U.S. SOF Operators was actively and covertly targeting a foreign person in the sovereign territory of Colombia. These conditions would limit the tactical actions available; however, Escobar's threat to the stability of Colombia and the collateral effects

---

[79] Robert D. McFadden, *Drug Trafficker Convicted Of Blowing Up Jetliner*, December 20, 1994, accessed 6 October 2011, http://www.nytimes.com/1994/12/20/nyregion/drug-trafficker-convicted-of-blowing-up-jetliner.html?src=pm.

[80] Office of Congressional Affairs, Central Intelligence Agency. "Briefings of NSC and SSCI on "Los Pepes" Affair: Secret, Memorandum for Record, OCA 2512-93." *Digital National Security Archive*, 06 December 1993, accessed 10 October 2011, http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&queryType=quick&ResultsID=13259A972FC&QueryName=cat&ItemNumber=72&ItemID=CCD00801.

[81] Bowden, *Killing Pablo*, 141.

of his narco-activities on the U.S. influenced the executive branch to authorize the military a more active role in the hunt, which would follow the traditional find, fix, finish target cycle.[82]

Through signals intelligence (SIGINT), SOF and CIA Operators were able to quickly pinpoint the locations of senior Medellín Cartel members, which was then passed to officials in the Search Bloc who would, if possible, corroborate the information with their human intelligence (HUMINT), and then deploy their security forces to establish a perimeter around the target area.[83] In theory, isolating the targeted individual in this way would enable those same forces to cordon off escape routes and allow the host nation capture/kill force to conduct their mission. In actuality, almost eighteen months passed before this force terminated Escobar.

The vast majority of the challenges attributed to this prolonged hunt are a result of Escobar's penetration of the government, police, and military forces. This provided him an intelligence advantage over his adversaries, which allowed him to elude capture on several occasions despite the veracity of the Search Bloc's intelligence. Other contributing factors included the competency of the Colombian's fix and finish force, as well as its own intelligence failures. To compete against these shortcomings, the U.S. enhanced its FBI and DEA liaison relationships with their Colombian counterparts, often resulting in sharing previously restricted intelligence, and deployed additional SOF Operators to advise and train the Search Bloc's finish force.[84] The efforts came to fruition in early December, 1993, when SIGINT provided the tip that led to Escobar's finish.

---

[82] Bowden, *Killing Pablo*,147.

[83] Ibid., 194.

[84] USEMB Cable – Colombia, "GFZE-92-8001, [Excised] Operation Envigado CCX: ZE-89-0007, [Excised] Pablo Escobar-Gaviria TKO-558, TKO Coordinator GFAI-93-9020, Threats/Assaults, Confidential, Cable, 006250." *Digital National Security Archive.* April 23, 1993, accessed 05 October 2011, http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&ResultsID=13259D15D46&queryType=quick&QueryName=cat&ItemNumber=59.

2. Exploitation and Analysis

Although operations leading up to Escobar's death provided a dearth of intelligence via interrogations, detainee reports, and material acquired through sensitive site exploitation, the coalition relationships and intelligence sharing restrictions often inhibited the process of targeting the cartel network. Each of the security and law enforcement elements assigned to targeting Escobar realized the importance of evidence collection, which often led to follow-on targeting; however, not all of these organizations were created equally. Many were unofficial paramilitary groups who merely sought revenge on Escobar and who the U.S. government could not legally support.[85] Additional shortfalls came from the lack of urgency to exploit the often time-sensitive data. This deficit could be attributed to the competency of the "Finish" force, but also to the linear targeting technique that failed to account for the networked structure of the Medellín organization, which was a result of incongruences within the bi-lateral intelligence fusion.

Despite the challenges associated with the disparate element's competencies and flaws, the establishment of the Colombian and USEMB Joint Task Force, as well as the Government of Colombia's Search Bloc, was instrumental in the exploitation and analysis of the Escobar mission. Each element, through cooperation and synergistic efforts, set the conditions for destabilizing the Medellín network. These nodes incorporated the each of the various agencies responsible for certain aspects of the manhunt and fused them into a single entity, which created an environment for better intelligence sharing and deconfliction of effort. This was essential for the exploitation and analysis that led on to follow-on targeting to deconstruct the cartel framework.

---

[85] CIA, Directorate of Intelligence, *Colombia: Alliances of Military Convenience*, March 1993, accessed 05 October 2011, http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItemImages.do?Multi=yes&queryType=quick&&ResultsID=1324170188A&QueryName=cat&ItemNumber=51&ItemID=CCD00752&imageNumber=2#imageTop.

D. FRICTION POINTS

The entire manhunt operation to apprehend Escobar was rife with friction, both objective and subjective in nature. Within the objective realm, the environmental factors included the actual operation area, which fell within the sovereign borders and airspace of Colombia, as well as the political realm both within the U.S., between the executive, legislative, and judicial, branches, as well as the diplomatic realm between the U.S. and Colombian governments. The lack of open hostilities and no declaration of war limited the size and scope of the military package deemed necessary to support the Colombian government. It also limited the activities in which SOF Operators could conduct under Title 10 authorities. However, once the National Security Council determined the actions of Escobar's Medellín Cartel a substantial threat, the authorities to deploy covertly, under Title 50, allowed those Operators to conduct intelligence collection activities, as well as to serve in an "advise and assist" capacity. It was incumbent on the Chief of Mission that all operations remain transparent since the roles members of his country team were filling were controversial in nature to senior leaders in the Colombian government as well as with policy makers and the judiciary in the U.S. Ultimately, the employment of military personnel within a sovereign country was a contentious subject for both nations even if the mission was primarily to provide and assist in the fusion of intelligence.

The realm of resources encompassed an additional objective friction point. As foreign monetary aid proved insufficient in assisting the Colombian government in the late 1980's, the U.S. Executive Branch authorized expending additional resources in battling the cartels and the drug trade. With that, greater funding was diverted to the DEA, and expanded their, and the FBI's, role and manpower outside the continental United States in the form of liaison staff and legal attachés (LEGAT) operating from embassies and consulates. It would also employ the vastly funded and resourced U.S. military, which had an abundance of technical, mechanical, and personnel at its disposal. These resources were abundant during the Escobar mission, but suffered on later occasions, specifically when they were redirected to assist GWOT operations in 2002.[86]

[86] Munsing et al., "Joint Interagency Task Force," 30.

Eventually, the U.S. government's willingness to direct adequate assets toward the mission was a necessary condition in achieving the initial success against the Medellín Cartel while follow on success destabilizing the FARC and other narco-terrorists.

Several subjective friction points came into play during the Escobar campaign, the first being the unity of effort. Because of the level of attention the problem received at the national policy level, and the creation of the Colombian and Joint Task Force, interagency actors became less reticent about working together. The traditional boundaries set by institutional norms were overcome by the need to accomplish the mission. Within the country team, a whole-of-government approach was employed to bring the full brunt of the elements of national power on the personal of Escobar and later transnational drug trafficking. This is not to say that interagency friction did not occur. Since all agencies compete for funding and resources, a certain level of rivalry plagued the country team.[87] Along with that, the commonplace debates of which intelligence is releasable and to who regularly afflicted interagency meetings. Outside of interagency circles, U.S. elements often felt at odds with their host nation counterparts, who did not appear to take the same dedicated approach to the problem or invest the same amount of effort. Such hindrances must be overcome in order to achieve effects.

Legitimacy of the mission was also at stake during the manhunt for Escobar. As previously mentioned, the targeting of General Aideed in Somalia came to national attention during the same timeframe as the Colombia mission, and both occurred within the first year of President Clinton's administration. Although there are few similarities between the two cases, the casual observer will see no distinction between the two. However, the mission in Colombia was deemed of national security interest, which provided the legitimacy for U.S. SOF to operate within the country in an intelligence collection capacity and in training the host nation force. Neither mission would have been possible had it not been strictly approved by the President of Colombia, who allowed it at the expense of appearing weak to his contenders, providing them material to

[87] Bowden, 171–172. Declassified Department of State Cables do not provide the behind the scenes metrics that Bowden captured from personal interviews with individuals working out of the USEMB at the time. Based on his research, competition between the various agencies did exist.

attack his political administration. On a broader scale, and a consequential result of the fragmentation of the cartels, the effort to counter the expansive drug trafficking problem and various insurgencies (FARC, ELN, AUC) is a regional problem, which gives legitimacy to JIATF-South's mission and its coalition efforts against narco-terrorism. Without public and diplomatic support by the host nation, the operations will never be seen as legitimate.

The final, yet no less contentious source of friction is that of leadership, which plays an essential role in effective counter-network operations. An individual must have the attributes necessary to focus a disparate group of interagency and coalition players toward a common goal. This must also be accomplished at the strategic, operational, and tactical levels. In the Colombia case, President Clinton accomplished the strategic approach by balancing relationships and national interests with the Colombian President, César Gaviria, as well as the U.S. Legislative Branch. Operationally, Ambassador Busby managed the interagency players on his Country Team as well as the interaction with Colombian leaders, specifically Gaviria. On the tactical level, the various interagency players themselves had to effectively lead their peers within the embassy depending on their various specialties and their counterparts in the Colombian National Police and the Search Bloc. Presently, elements of JIATF-South fill similar leadership roles, not only within the command, but also with various regional actors and their counterparts, proving the efficacy of overcoming leadership friction.

E. CONCLUSION

Overall, the mission to capture/kill Pablo Escobar contained all of the components of the F3EA cycle, incorporated an interagency approach, and increased the bilateral cooperation that proved to be essential for achieving positive target-based effects. However, it was only a small chapter in the history of United States' "war on drugs." Four U.S. Presidential Administrations oversaw the genesis of what would become the Joint Interagency Task Force (JIATF) South, which matured during this highly romanticized operation. The nodal approach encompassing the Escobar affair would be expanded to encompass a much broader region and mission as the cartels fragmented and

merged with transnational insurgencies such as the FARC, *Ejército de Liberación Nacional* (ELN), and *Autodefensas Unidas de Colombia* (AUC).[88] JIATF-South would be tasked with conducting interagency and international Detection & Monitoring operations, facilitating the interdiction of illicit trafficking and other narco-terrorist threats in support of national and partner nation security.[89] The task force and its predecessors adopted a targeting cycle, or End-to-End Mission Management, more robust than that what is taught in traditional military courses and is more in line with the F3EA process. It, like the F3EA, is cyclic and is composed of seven steps or stages: 1. Cueing, 2. Detection, 3. Monitoring, 4. Interdiction, 5. Arrest, 6. Prosecution, which leads to 7. More Intelligence.[90] Through the utilization of this process, "JIATF-South became *the* model for interagency collaboration as well as a widely cited example of effective intelligence fusion."[91]

The collaboration of U.S. and coalition efforts in conducting man-hunting missions and narco-terrorist activities in SOUTHCOM's area of responsibility resulted in the destabilization the drug cartels as well as the FARC's influence in the region. Each operational success, ranging from drug interdictions to aiding in the apprehension of cartel leaders, validated the targeting cycle employed, highlighting the importance of fusing intelligence with operations and interagency cooperation. None of which would have been possible if not for the decades old relationships built within the OAS.

This successful collaboration transcended traditional narco-terrorism missions in 2009 by the successful conclusion of Operation WILLING SPIRIT in U.S. military circles and Operation *Jaque* within Colombia, when fifteen hostages, including three U.S.

---

[88] Anne Patterson, "Notes from the Field: A View from Medellín Confidential, Cable, 011431," *Digital National Security Archive*, December 21, 2001, accessed 05 October 2011, http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&queryType=quick&ResultsID=13259FF8D6A&QueryName=cat&ItemNumber=83&ItemID=CCD01851.

[89] *Joint Interagency Task Force South*, accessed 05 October 2011, http://www.jiatfs.southcom.mil/index.aspx.

[90] Evan Munsing, and Christoper J. Lamb, "Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success," *Institute for National Strategic Studies: Strategic Perspectives, No. 5*, June 2011, 21.

[91] Ibid. 30.

military contractors, were rescued from FARC captivity.[92] Operational effectiveness helped break the barriers between various agencies and partner nations, which was illuminated when Colombian forces, in conjunction with a small contingent of U.S. support personnel, rescued the hostages from their captors, bringing an end to their six years in captivity. The establishment of mission focus nodes consisting of a Joint Task Force from SOCSOUTH, interagency actors within the USEMB, and Colombian SOF built a collaborative environment to tackle the problem. By fusing intelligence, plans, and operational capability, the fusion nodes brought about the successful end to a multi-year operation.

The U.S. can replicate the success of the interagency efforts in Colombia by applying the same methods toward the global targeting of terrorist networks through the establishment of counter-terrorism (CT) fusion nodes within U.S. embassies and consulates. It is done in Colombia during the Escobar campaign and now, on a regular basis, within JIATF-South, which is coined "*the* model" for interagency activities. It is not an easy task; however, setting the conditions by ensuring the proper authorities are in place while establishing a collaborative effort between the interagency and host nation forces will lead to the disruption of non-state actors and terrorist networks.

[92] Tim, Padgett, "Colombia's Stunning Hostage Rescue," *Time*, 02 July 2008, accessed 10 October 2011, http://www.time.com/time/world/article/0,8599,1819862,00.html.

THIS PAGE INTENTIONALLY LEFT BLANK

V. AL-QAEDA IN IRAQ

> Our operations have, in fact, produced substantial progress against Al Qaeda and its affiliates in Iraq. In the past 8 months, we have considerably reduced the areas in which Al Qaeda enjoyed sanctuary. We have also neutralized 5 media cells, detained the senior Iraqi leader of Al Qaeda-Iraq, and killed or captured nearly 100 other key leaders and some 2,500 rank-and-file fighters. Al Qaeda is certainly not defeated; however, it is off balance and we are pursuing its leaders and operators aggressively. Of note, as the recent National Intelligence Estimate on Iraq explained, these gains against Al Qaeda are a result of the synergy of actions by: conventional forces to deny the terrorists sanctuary; intelligence, surveillance, and reconnaissance assets to find the enemy; and special operations elements to conduct targeted raids. A combination of these assets is necessary to prevent the creation of a terrorist safe haven in Iraq.
>
> GENERAL David H. Petraeus
> Report to Congress on the Situation in Iraq
> 10–11 September 2007[93]

This chapter will focus on the historical example of the integration of operations and intelligence through F3EA targeting cycle as part of the CT efforts against al-Qaeda in Iraq (AQI). This effort was directly in support of overall COIN strategy in Iraq. Whereas the previous historical examples discussed on how the targeting cycle overcame minor degrees of friction, this chapter will emphasize how friction became a major challenge to U.S. CT forces following the implementation of the Status of Forces Agreement (SOFA).

A. BACKGROUND

On 7 June 2006, two 500-pound laser-guided bombs dropped from American F-16 fighter-bombers exploded on a safehouse located five miles outside the Iraqi town of Baqubah. After weeks of constant surveillance following the target's spiritual advisor, Task Force 145's effort had finally paid off. Abu Musab al-Zarqawi, the leader of AQI, was now dead. Shortly after the strike, American Special Operation Forces secured the

[93] David H. Petraeus, "Report to Congress on the Situation in Iraq," 10-11 September 2007, accessed 06 October 2011, http://www.defense.gov/pubs/pdfs/Petraeus-Testimony20070910.pdf.

area and collected a treasure trove of intelligence on the terrorist organization as part of the follow-up sensitive site exploitation. This new information was quickly passed to the Task 145 intelligence analysts in order to identify additional AQI associates of al-Zarqawi. This group of Special Operations Forces, known as Task Force 145, was specially trained and specifically organized to track and then capture or kill High Value Targets in Iraq. Once again, they had just demonstrated how effective they could be when operations and intelligence were integrated as part of a deliberate network targeting cycle.[94]

> The airstrike that killed Zarqawi was only a fraction of the effort to find and accurately target him. The true operational art behind that strike was a multidisciplined intelligence, surveillance, and reconnaissance (ISR) endeavor coupled with agile SOF that patiently laid bare the Zarqawi network and resulted in a find-fix-finish operation. It took more than 600 hours of ISR to track and observe the network that yielded the target. . . . The SOF–ISR combination was effective because it unified operations and airborne collections with all other intelligence disciplines under a single commander.[95]

Their effectiveness only continued to improve. By May 2007, it was reported that American Special Operations Forces were averaging between 6 and 12 missions a night against AQI, insurgent fighters and militia targets.[96] Although these missions were not as high profile as Zarqawi, they demonstrated American's CT forces had become experts at utilizing the F3EA targeting cycle to disrupt, deny and defeat terrorist networks across Iraq. Then in late June 2009, this specialized Task Force and their finely-tuned F3EA targeting cycle came to almost grinding halt.

---

[94] Chris Cuomo and Eamon McNiff, "The Men in the Shadows—Hunting al-Zarqawi," ABC News Good Morning America, 9 June 2006, accessed 29 September 2011, http://abcnews.go.com/GMA/Terrorism/story?id=2056386&page=1.

[95] Michael Flynn, Rich Jergens, and Thomas Cantrell, "Employing ISR: SOF Best Practices," Joint Force Quarterly 50 (3d Quarter, 2008), 56.

[96] Thom Shanker, "Special Operations: High Profile, but in Shadow," The New York Times, 29 May 2007, accessed 29 September 2011, http://www.nytimes.com/2007/05/29/world/middleeast/29forces.html?ref=abumusabalzarqawi.

B. FRICTION

On 30 June 2009, the U.S.-Iraq Status of Forces Agreement (SOFA) had officially taken affect. As part of the agreement, U.S. combat troops were no longer permitted to operate within Iraqi cities and now required Iraqi-approved warrants for individuals suspected of terrorist activities.[97] In addition, there was increased pressure to start including Iraqi forces during finish operations instead of solely Americans troops. Prior to the SOFA, the CT operational environment was one that required little U.S.-Iraqi coordination or approval. U.S. CT forces simply had to decide that they had collected a sufficient amount of intelligence and that there was a high probability of capturing or killing the target before unilaterally loading up in the helicopters or assault vehicles to launch on a finish operation.[98] Now, the new operational environment created not just a massive increase in the amount of U.S.-Iraqi coordination required during and after a raid, but it also required Iraqi approval before starting it.

U.S. CT forces realized the only way to continue maintaining pressure on AQI was by trying to facilitate the F3EA targeting cycle by, with and through the Iraqi security forces (ISF). Heeding the words of Clausewitz, they knew that as easy as this sounded on paper, there was going to be a certain degree of friction when it was attempted in real war. Unfortunately, no one was quite prepared for just how much objective and subjective friction there would really be, as well as the amount of effort it was going to take to try and overcome it.[99] While there were countless friction points at the tactical, operational and strategic level in the post SOFA Iraq, this chapter will only address a few of the major ones in order to highlight the importance and role a fusion node can play in facilitating the F3EA targeting process in similar type of operational environment.

---

[97] *US-Iraq Status of Forces Agreement*, 17 November 2008, p. 3-15. http://graphics8.nytimes.com/packages/pdf/world/20081119_SOFA_FINAL_AGREED_TEXT.pdf.

[98] Thom Shanker, "Special Operations: High Profile, but in Shadow," The New York Times, 29 May 2007, accessed 29 September 2011, http://www.nytimes.com/2007/05/29/world/middleeast/29forces.html?ref=abumusabalzarqawi.

[99] Anonymous Special Operations Soldier.

C. FUSION NODES

In an effort facilitate the targeting cycle and reduce friction, the U.S. CT Task Force decided to stand-up several Fusion Nodes across Iraq. These nodes were based on the previously used principle of Fusion Cells, which had been established to work in conjunction with U.S. general purpose forces in Iraq to synchronize CT efforts. The idea was that with a little tweaking, Fusion Nodes would be able to accomplish the same thing with the ISF. On paper, the concept looked easy; however, in reality they immediately encountered unforeseen subjective friction.

The first and most important one involved the F3EA targeting process itself. As a general rule, an understanding of targeting as a cycle did not exist within the ISF, and the parts of it that did, where too slow to facilitate a pro-active approach.[100] Attempts to educate the ISF seemed to make very little headway because it was hard to change their hierarchical targeting mindset. An example of this is apparent when in August 2009, the Iraqi Ninawa Province Operations Center senior intelligence officer provided the Mosul Fusion Node with a spreadsheet containing 400 targets in numbered order. When asked about the relationship of each target to one another, the Iraqi intelligence officer simply answered, "They are all bad."[101] This response clearly indicated a piece-meal targeting mentality rather than any sort of integrated network targeting strategy.

In addition to the difficulty of instilling a network targeting mentality, the second significant subjective friction point involved the actually location of the Fusion Nodes. The Fusion Nodes were to be embedded within the Iraqi Provincial Operational Centers based on the belief that this was a critical hub for information and command and control. This belief was based on the American military model where information freely and quickly flowed up and down chain-of-command at centralized command and control centers. At this location, the Node would be able to share intelligence, synchronize assets, and coordinate operations using a robust communications architecture. While this idea fit well with current American military thinking, and a considerable amount of

[100] Anonymous Special Operations Soldier.

[101] Anonymous Special Operations Soldier.

money and resources were spent trying to turn the operational centers into mirror images of American tactical and joint operations centers equipped with computers and flat screen TVs, there was little return on this investment because of cultural factors. The attempts to facilitate network targeting by embedding at the provincial operational level netted little to no results. According to one U.S. CT officer:

> The information I provided, or feedback I asked for to kick-start the targeting cycle seemed to get lost in a "black hole." My assessment for this is that the inherent mindset of the ISF did not encourage rapid vertical and horizontal information sharing, which is the critical component for successful network targeting. I surmise some of the reasons for this were:
>
> - Operational level commanders did not want to share information with their subordinates because information is power
> - Operational level commanders did not trust my information
> - Subordinate commanders did not trust the information because they did not know where it came from
> - The ISF communication process at the operational level was too slow to effectively facilitate the information flow
> - Operational level commanders simply choose to ignore my information because they knew I had no way to confirm if it was indeed passed down to the tactical level[102]

As a general rule, the Iraqi military mindset was not conducive to freely sharing information up and down the chain of command like it is in the U.S. military. An important reason for is that during the Saddam Hussein Regime, not only was information a tool that could be used to protect a police or military officer in the case of blackmail, but it also could easily cost him his life in the form of repercussions if an operation was conducted and the information was wrong. One way to overcome this "black hole" effect was implemented in the Diyala Province in April 2010. Once the Fusion Node no longer embedded itself at the Diyala Operations Center and instead established a direct relationship and gained trust with the tactical level commanders that were involved with the actual CT operations (in this case the Federal Police and the Major Crimes Unit) the targeting process significantly improved. This new relationship enhanced the speed of the ISF targeting cycle by quickly facilitating the sharing of intelligence, leveraging any available resources and gaining immediate feedback. It even

[102] Anonymous Special Operations Soldier.

included the ISF willingly handing over sensitive site exploitation material that was recovered during unilateral ISF missions.[103] Although this arrangement in Diyala improved CT targeting in the post SOFA Iraq, it did not eliminate friction all together. In order to better understand the remaining friction points, it is better to examine them through the actual F3EA targeting cycle.

D. FIND

The ISF lacked the technical means, such as signal intelligence, that was readily available to U.S. CT forces to find targets. This resulted in the ISF solely relying on their human intelligence (HUMINT) network to find their targets. While HUMINT is one method to find a target, it is often slow because of the dense population centers in Iraq. In addition, the robust road system enabled a target to rapidly travel around the country. Due to the need for the targeting cycle to be hours instead of days, often HUMINT alone was not fast enough to capitalize on the government's brief information advantage over the insurgency following a successful CT operation. In order to overcome this obvious objective friction point, U.S. CT forces leveraged the Fusion Nodes to take intelligence gathered by U.S. collection assets and then make it Iraqi-Releasable. Then the Fusion Nodes would assist the ISF in focusing their HUMINT to a particular area where the target was known to be operating. This action decreased the amount of time it took to move to the next phase of the targeting cycle.

E. FIX

A second area where objective friction was present was during in the fixing phase of the targeting cycle. As mentioned in chapter one, the critical component of this phase is actually locating the target in order to gain information about the individual's pattern of life (PoL), as well as any other potential associates of the network. U.S. CT forces utilized a combination of HUMINT and surveillance aircraft to accomplish this. Unfortunately, the ISF lacked surveillance aircraft, and therefore, relied solely on HUMINT. In an effort to reduce the objective friction caused by lack of Iraqi ISR,

[103] Anonymous Special Operations Soldier.

Fusion Nodes attempted to integrate U.S. Full Motion Video (FMV) assets to assist the ISF in tracking a targeted individual. Unfortunately, even with coaching and mentoring by the Fusion Node, this resulted in only limited success because of subjective friction. The reason was the ISF leadership often lacked the tactical patience required to develop the targeted individual's PoL and associates prior to executing the third phase of the targeting cycle.[104]

F. FINISH

U.S. CT forces in Iraq demonstrated an extremely high level of tactical patience waiting for the appropriate trigger to be met before executing a finish operation. This trigger was typically based on an established set of criteria such as HUMINT or FMV that produce a high degree of confidence that the targeted individual was present in a specific location and there was a high probability of capturing or killing him. In order to accomplish this, U.S. CT forces relied on constant surveillance of the targeted individual. As previously mentioned, the ISF lacked the ISR support to help do this so they solely relied on HUMINT to tell them when and where a target was located. Unfortunately, often as soon as the ISF would get a report from one of their sources that a target was located somewhere they would roll out the gate to try and capture him. They did little to confirm that their source remained in a position to keep constant surveillance on the target to ensure he did not flee the area prior to assault force getting there. More times than not, this resulted in the failure to capture the targeted individual.[105] The Fusion Nodes attempted to overcome this objective friction by utilizing U.S. FMV assets to assist the ISF in meeting trigger, but again this was met with only limited success for same reason as during the Fix phase, a lack of ISF tactical patience. As was previously discussed in chapter one, the effect of these unsuccessful ISF CT finish operations meant that the time available to conduct COIN was continuously being reduced.

[104] Anonymous Special Operations Soldier.

[105] Anonymous Special Operations Soldier.

G. EXPLOITATION

By 2009, U.S. CT forces in Iraq had become experts at conducting detailed searches for sensitive material and good tactical questioning of detainees while still on the target objective. However, the post SOFA operational environment meant that the majority, and in many cases all site exploitation was to be conducted by the ISF. Unfortunately, this brought about a degree of subjective friction. The reason was the ISF were not experienced or willing to conduct detailed searches and tactical questioning while still on the site. ISF CT operations typically seemed to be a race to see how fast they could grab the targeted individual, throw him in a truck and drive back to the base without ever conducting any exploitation.[106] Fusion Nodes attempted reduced this friction by constantly emphasizing to the ISF leadership that the mission is not over just because the target individual was killed or captured. In order for the mission to be a success, a detailed exploitation of the site to gain information about the network had to be conducted.[107]

Often, exploitation provided time sensitive intelligence that was quickly acted up and resulted in further degradation of the targeted network. U.S. CT forces could quickly get approval for these follow-on targets because of instantaneous communication with higher headquarters. This was not the case with the ISF. Typically, the ISF were hesitant to conduct time sensitive follow-on missions because of a lack of prior approval from their chain-of-command and the lack of a legal search warrant. The Diyala Fusion Node attempted to overcome this subjective friction by establishing a means to gain immediate permission from ISF the chain-of-command, as well as the ability to get legal approval from an Iraqi judge. The method to this was by telling the approving commander and the judge to leave their cell phones (the primary means of communication by ISF) turned on

[106] Anonymous Special Operations Soldier.

[107] Anonymous Special Operations Soldier.

throughout the entire operation. Unfortunately, this was not always effective because of poor cell phone coverage or the commander or judge simply failed to answer the phone.[108]

Finally, the last form of friction encountered during exploitation was objective friction. The ISF also lacked the technical means available to U.S. CT forces that were required to conducted in-depth exploitation of key electronic items recovered on an objective. This meant the ISF were unable to gather critical information about the network contained within these devices. In an effort to overcome this friction, U.S. CT forces attempted to utilize the Fusion Nodes as means to collect electronic items from the ISF. Once collected, these items were sent to U.S. technical exploitation facilities within Iraq as quickly as possible. Once the item was exploited, the Fusion Node would put the information in the form of an Iraqi Releasable intelligence report and disseminated it back to the ISF. Since the ISF were receiving intelligence from these items, they became much more willing to continue passing along them to the Fusion Nodes.[109] In addition, this exchange provided a means for American CT intelligence analysts to gain access to technical devices that were previously unavailable for exploitation.

H. ANALYSIS

U.S. CT forces in Iraq relied on a massive pool of intelligence analysts to sift through the collected intelligence data. This enabled them to quickly identify additional members or associates of the targeted network. Unfortunately, U.S. CT forces encountered objective friction when they attempted to implement this phase of the targeting cycle to the ISF. The reason for this was ISF CT units lacked a dedicated pool of analysts; therefore, their ability to piece together information regarding the network was either non-existent or extremely slow. An effort to overcome this friction was made in places like Diyala Province in April 2010. The Fusion Node there emphasized the need for the ISF commanders and intelligence officers to develop products such as a link analysis chart to assist in identifying and understanding connections within the network.

[108] Anonymous Special Operations Soldier.

[109] Anonymous Special Operations Soldier.

The intent of this type of analysis was that it would assist the ISF in speeding up the amount of time it took to start the targeting cycle over again.[110]

I. CONCLUSION

U.S. CT experience in Iraq demonstrated that the F3EA targeting cycle was a very effective method to deny, disrupt and defeat terrorist networks. As American CT forces transitioned from unilateral operations to SOFA environment, the need to assist the ISF in maintaining pressure against terrorist networks became increasingly apparent. In an effort to overcome the friction associated with ISF network target, U.S. CT Task Force established a series of Fusion Nodes across Iraq. While there were many lessons to be learned once the Fusion Nodes were actually put into practice, they did increase the speed and efficiency of ISF network targeting. They also provided the means for American CT legitimacy and a level of American visibility on the terrorist networks operating within the post SOFA Iraq. Despite the multifaceted problems these nodes in Iraq experienced, we are confident that they provide a starting point of designing a global CT network that is capable of effectively integrating intelligence and operations as part of a precision targeting process.

[110] Anonymous Special Operations Soldier.

VI. APPLICATION

> Terrorism will remain at the forefront of our national security threats over the coming year. Al-Qaida continues to aspire to spectacular attacks. Over the past two years, core al-Qaida has continued to be committed to high-profile attacks against the West, including plans against the United States and Europe. In light of the loss of experienced personnel, we judge it will seek to augment sophisticated plots by increasing its operational tempo with smaller, simpler ones to demonstrate its continued relevance to the global jihad.
>
> James R. Clapper
> Director of National Intelligence
> 10 February 2010[111]

The purpose of this chapter is to demonstrate the critical role a series of interconnected Fusion Nodes can play in integrating intelligence and operations in order to deny, disrupt and defeat transnational terrorism. It will do this by using recent real-world events as a foundation to build a hypothetical scenario that highlights the role and capabilities of these Fusion Nodes.

A. INTRODUCTION

In the early hours of Sunday morning, the sound of a large explosion echoed across the Algerian city of Tizi-Ouzou. The explosion that wounded 33 people, including 11 police officers, was caused by a car bomb outside of a police station.[112] Although, no group immediately claimed responsibility for the blast, it was widely suspected that the city, located only 62 miles east of the capital Algiers, had just been the victim of another attack by the Algeria-based Sunni Muslim jihadist group Al Qaeda in the Lands of the Islamic Maghreb (AQIM).

---

[111] James R. Clapper, Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence, 10 February 2010, accessed 27 August 2011. http://www.dni.gov/testimonies/20110210_testimony_clapper.pdf.

[112] CNN Wire Staff, "Car Bomb Wounds 33 in Algeria," CNN World, 14 August 2011, accessed 10 October 2011, http://articles.cnn.com/2011-08-14/world/algeria.bomb_1_car-bomb-wounds-tizi-ouzou-algerian-city?_s=PM:WORLD.

AQIM, an internationally recognized terrorist organization, has two goals. The first is to overthrow the Algeria government in order to establish an Islamic caliphate state. The second is to attack western interests to support Al Qaida's goal of expelling Western influence from Muslim countries. This second goal was made glaringly clear when the leader of AQIM declared, "Everyone must know that we will not hesitate in targeting it [America] whenever we can and wherever it is on this planet."[113] This real-world event, which occurred on 14 August 2011, as well as the goals of AQIM provide an excellent foundation to build a "what if" scenario based on what might happen if similar attack occurred and after series of Fusion Nodes were established across the globe.

B. HOBOKEN, NEW JERSEY

It was almost 9 PM when the dark blue Toyota 4Runner finally backed into the driveway of the house. Three men got out of the vehicle, walked up to the door, and after a quick knock, were hurried inside. For the men of the F.B.I. Counter-Terrorism unit covertly watching outside, trigger had just been met and the finish phase of the operation was about to commence. Within minutes, F.B.I. agents assisted by local police raided the house and detained four men. During the search of the premises, they discovered eight full propane tanks, several initiating devices, and multiple electronic devices. These items were quickly secured and sent back to the lab for analysis. Another terrorist attack against New York City had been disrupted and an al-Qaeda IED cell had just been defeated. However, this success did not happen by chance, but rather by a series of earlier interconnected events that were made possible by a Fusion Node more than two years ago.

C. JFK AIRPORT, NEW YORK CITY: ONE MONTH EARLIER

After several hours of questioning, the 27 year old Malian national had just confessed to F.B.I. officials that he was supposed to meet with an American who lived in

[113] Souad Mekhennet et al, "A Threat Renewed: Ragtag Insurgency Gains a Lifeline From Al Qaeda," *The New York Times*, 1 July 2008, accessed 9 May 2011, http://www.nytimes.com/2008/07/01/world/africa/01algeria.html?pagewanted=1&_r=1&sq=ragtag&st=cse&scp=1#.

Hoboken, New Jersey. In the hopes of a reduced sentence, the Malian confessed that he had been communicating with an individual via email after meeting him on an Islamic chatroom more than a year ago. The Malian stated the American claimed he was part of an al-Qaeda cell that was planning an attack at the site of the new World Trade Center, but needed help making detonators for the bomb. The Malian had volunteered to fly to New York to help. When he applied for a tourist visa in Mali, his information was entered into a U.S. biometric database. The report came back stating the man had been detained in Mali two years ago for weapons smuggling and was also associate with a known AQIM VBIED facilitator. U.S. officials, working with the Joint Interagency Task Force (JIATF) located in the National Capital Region, decided to approve the visa. This was all based on the idea that it would bring him under U.S. jurisdiction for questioning about his involvement in an incident in Mali two years earlier.

D. MALI: 2 YEARS EARLIER

During a routine meeting with a Malian security forces commander, the Officer in Charge (OIC) of the Mali Fusion Node received information about four military aged males that were recently detained after trying to smuggle weapons and a bag of circuit boards through a military border checkpoint. The OIC asked the security forces commander if he could get biometrics on the individuals to check if they might have been involved in any known nefarious activity in the past. The Fusion Node OIC was taken to the holding facility and one at time, each detainee was brought out. Using a Handheld Interagency Identity Detection System (HIIDE), the OIC quickly took pictures of each detainee's irises, facial features and fingerprints. Then, he walked outside, attached the HIIDE to a Bgan satellite antenna and bursts the information to a military biometric database. This database, known as the Automated Biometric Information System, is accessible to American military forces across the globe through a set of portable consoles such as the HIIDE. [114] Within three minutes, an initial report came back stating that one of the detainee's biometric data had been previously entered into the database. The OIC

[114] Spencer Ackerman, "U.S. Scans Afghan Inmates for Biometric Database," Wired, 25 August 2010, accessed 10 October 2011, http://www.wired.com/dangerroom/2010/08/military-prison-builds-big-afghan-biometric-database/.

informed the Malian security force commander of the initial results and stated he would provide more detailed information after he was sent the full report. The OIC returned to his office located in the U.S. Embassy, and within four hours received the full report. It stated that the detainee's fingerprints had been identified on a circuit board that was recovered during an AQIM VBIED attack in neighboring Algeria. The OIC, who was a qualified Foreign Disclosure Officer, declassified the report and called the security force commander to setup a hasty meeting. He then called the Fusion Node in Algeria to let them know what he had found. The bomber maker, an Algeria national and an admitted member of AQIM, was quickly extradited back to Algeria for prosecution. Unfortunately, his three associates, all Malians, disassociated themselves from the AQIM member, claimed their innocence and were eventually released. On the positive, all of their biometric data was now part of the American database. None of this would have occurred had it not been for the Fusion Node in Algeria.

E. ALGERIA: 5 MONTHS EARLIER

As the vehicle pulled up to the military barracks checkpoint in the Algerian coastal town of Cherchell, the driver, dressed in a Lieutenant Colonel Algerian military uniform to help avoid suspicion, mutter "Allahu Akbar" to the guard and pressed the button. The vehicle exploded with a thunderous roar. The attack, which killed 18 people, could have been worse. Fortunately, a portion of the car did not detonate, and its pieces were scattered around the area. Upon hearing of the attack, the OIC of the Algeria Fusion Node accompanied Algerian security forces to the blast site to facilitate exploitation. A through search uncovered part of an electrical circuit board that as part of the initiating device. Having been instructed on the importance of site exploitation by the Fusion Node, Algerian security forces carefully collected, tagged and documented the circuit board. The security forces commander then provided the circuit board to the Fusion Node OIC to facilitate further technical exploitation. The Fusion Node took the circuit board, packaged it up and sent it off to the American Joint IED Defeat Organization (JIEDDO) exploitation lab. After further analysis, the lab identified a set of fingerprints from an unknown individual on the circuit board and submitted into the biometric database.

F. CONCLUSION

Although this scenario is hypothetical, it highlights several key points of why Fusion Nodes are critical. First, had there not been a Fusion Node in Algeria to collect the initial circuit board, it is unlikely the AQIM VBIED facilitator would have never been identified after being detained in Mali. Second, this information led to the Mali Fusion Node identifying the associates of the AQIM VBIED facilitator as potential AQIM members. This information enabled the identification of a potential AQIM member attempting to enter the U.S. two years later. This identification enabled F.B.I agents to find, fix, and finish an American born al-Qaeda cell and prevent an attack. Lastly, it demonstrates how Fusion Nodes can provide the U.S. government a joint-interagency means to integrate operations and intelligence with its allies and host-nations partners on a global scale to proactively disrupt, deny and defeat transnational terrorist networks.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX: THE DESIGN OF THE FUSION NODE

> Decentralized organizations can be so resilient that it's hard to affect their internal structure. Thus, if you can't beat them, join them. The best opponent for a starfish organization is often another starfish.
>
> The Starfish and the Spider[115]

The purpose of this appendix is to analyze the critical components and criteria necessary to develop and organizational design effective Fusion Nodes that are capable of integrating intelligence and operations as part of a network targeting process.

A. STAKEHOLDERS

Before going out and creating a series of Fusion Nodes across the globe, it is critical to identify all of the stakeholders, as well as the roles and responsibilities they might have in one. In order to do this, it is first necessary to define the term stakeholder. For the purpose of this thesis, a stakeholder is any entity inside or outside of the organization who: has a vested interest in counterterrorism operations, will be affected by the counterterrorism strategy implemented by the Fusion Node, or is in a position to effect the adoption or execution of the Fusion Node's counterterrorism strategy.[116] To put it more simply, a stakeholder is any entity inside or outside of the Fusion Node "upon whose action the organization depends or who in turn depends on the organization for the realization of some of its goals [and] objectives."[117]

Based on the stakeholder definition presented above, it becomes evident that the number of government stakeholders when conducting counterterrorism operations is numerous. However, in the case of the operations and intelligence Fusion Node, the number of government stakeholders be reduced from the larger counterterrorism community, since the primary function of the Fusion Node described in this paper is to

---

[115] Ori Brafman and Rod Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006), 121.

[116] R. Mason & I. Mitroff, *Challenging Strategic Planning Assumptions* (New York: John Wiley, 1981), 43.

[117] A.J. Rowe, R.O. Mason, K.E. Dickel, *Strategic Management & Business Policy: A Methodological Approach* (Reading, MA: Addison-Wesley, 1985), 2.

conduct counterterrorism operations outside of the continental United States (OCONUS) and outside of the battlefields of Afghanistan and Iraq.

At the very top of the list of government stakeholders is the President of the United States and the National Security Council (NSC). The President works with the NSC to receive the assessments and analyses from the various U.S. government agencies, which are then used to create, implement and monitor the national security strategies and policies of the United States, including counterterrorism. While the NSC has a basic structure that is mandated by law, the actual structure of the NSC is defined by each presidential administration according to the President's priorities and guidance. Under President Obama, the NSC consists of the President, Vice President, Secretary of State, Secretary of Defense, Secretary of Energy, Secretary of Treasury, Attorney General, Secretary of Homeland Security, the Representative of the United States of America to the United Nations, Chief of Staff to the President, National Security Advisor, Director of National Intelligence, and Chairman of the Joint Chiefs of Staff.[118]

Within the NSC there are the Principals Committee, the Deputies Committee, and the Interagency Policy Committees. The Principles Committee consists of the cabinet members who are part of the NSC, and it is responsible for addressing critical national security issues and overseeing policy implementation. The Deputies Committee consists of the sub-cabinet members (deputy secretaries), and it is responsible for process coordination between the NSC, the Principles Committee and the various Interagency Policy Committees. The Interagency Policy Committees are responsible for policy development and execution for various regional and functional areas. The three Policy Committees that impact counterterrorism are the committee for Counterterrorism and National Preparedness (also known as the Counterterrorism Support Group); the committee for Defense Strategy, Force Structure, and Planning; and the committee for Intelligence and Counterintelligence.[119] See Figure 1 for a graphic representation of the role of the NSC and the committees.

---

[118] Joint Special Operations University, *Special Operations Forces Interagency Counterterrorism Reference Manual*, (Hurlburt Field: The JSOU Press, 2009), 1-3 – 1-5.

[119] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-6 – 1-7.

Figure 5. Role of NSC and Committees. [120]

Below the President and the NSC there are the U.S. government agencies that are government stakeholders in OCONUS counterterrorism operations. They include the Department of State (DoS), the Department of Defense (DoD), the Department of the Treasury (Treasury), the Department of Justice (DoJ), and the Office of the Director for National Intelligence (DNI).[121]

The DoS is a major stakeholder and has the lead responsibility for counterterrorism efforts OCONUS. As a result, it has numerous elements that perform counterterrorism roles, which include: the Bureau of Diplomatic Security (DS); the Bureau of Intelligence and Research (INR); the Bureau of International Narcotics and Law Enforcement; the Bureau for International Security and Nonproliferation (ISN); the

[120] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-4.

[121] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-10.

Counterterrorism Finance Unit; the Office of the Coordinator for Counterterrorism (S/CT); the Office of Terrorism Finance and Economic Sanctions Policy; and the Public Designation Unit.[122]

Within DoS the main element for counterterrorism is S/CT. The central role of S/CT is explained on the DoS website:

> The mission of the Office of the Coordinator for Counterterrorism (S/CT) is to develop and lead a worldwide effort to combat terrorism using all the instruments of statecraft: diplomacy, economic power, intelligence, law enforcement, and military. S/CT provides foreign policy oversight and guidance to all U.S. Government international counterterrorism activities.[123]

The DS also plays a major role in counterterrorism within the DoS. It has responsibility for the Antiterrorism Assistance Program and the Rewards for Justice Program. The Antiterrorism Assistance Program helps establish cooperative relationships between U.S. law enforcement agencies and organizations with similar roles within partner nations conducting counterterrorism operations. The Rewards for Justice Program offers rewards to individuals who provide information that solves or prevents terrorist acts. It also provides rewards for information that leads to the capture or conviction of terrorists.[124]

As mentioned above, there are several other DoS bureaus that also have various counterterrorism roles. The INR is a member of the U.S. Intelligence Community (IC) and has the responsibility of providing intelligence on global terrorist threats for the DoS. The Bureau of International Narcotics and Law Enforcement develops policies and programs to address international drug trafficking and crime that may have an impact on terrorist organizations. The ISN is responsible for developing efforts to prevent the spread of weapons of mass destruction among terrorist groups and non-state actors. The Counterterrorism Finance Unit works with the Public Designation Unit to identify

---

[122] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-8 – 1-12.

[123] Office of the Coordinator for Counterterrorism, *Our Mission*, http://www.state.gov/s/ct/about/c16570.htm (accessed March 1, 2011).

[124] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-8 – 1-12.

terrorist financial support structures and eliminate them. The Public Designation Unit is responsible for recommending to the Secretary of State the organizations and individuals that should be formally identified as terrorists, and also monitors to ensure that sanctions are being enforced for those individuals and organizations on the list. Lastly, the Office of Terrorism Finance and Economic Sanctions Policy works to establish international support for initiatives that target terrorist financing.[125]

The next major stakeholder is the DoD. Similar to the DoS, within the DoD there are also numerous elements that are involved in counterterrorism efforts, such as: the Assistant Secretary of Defense for Special Operations, Low-Intensity Conflict and Interdependent Capabilities (ASD/SOLIC & IC); the United States Special Operations Command (USSOCOM); the Geographic Combatant Commanders (GCC); the Defense Intelligence Agency (DIA); the Defense Security Cooperation Agency (DSCA); the Military Department Intelligence Services; the National Geospatial-Intelligence Agency (NGA); the National Security Agency (NSA); and the National Reconnaissance Office (NRO).[126]

The main DoD entities that are involved with conducting counterterrorism operations are ASD/SOLIC & IC, USSOCOM, and the six GCCs. The ASD/SOLIC & IC is responsible to the SECDEF for all matters relating to special operations and low-intensity conflict, which includes counterterrorism.[127] According to the 2008 Unified Command Plan (UCP), USSOCOM "is responsible for synchronizing planning for global operations against terrorist networks, and will do so in coordination with other combatant commands, the Services, and, as directed, appropriate U.S. government agencies."[128] The six GCCs are NORTHCOM, PACOM, EUCOM, SOUTHCOM, CENTCOM, and AFRICOM. Within the 2008 UCP it also states, "[u]nless otherwise directed, the

[125] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-9 – 1-11.

[126] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-13 – 1-14.

[127] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-13.

[128] Barack Obama, *2008 Unified Command Plan*, (Washington DC: Office of the President of the United States, 2008), 24.

geographic combatant commanders are responsible for missions in their AORs."[129] This includes counterterrorism operations, unless directed otherwise.

There are also the various DoD intelligence organizations, which are part of the IC, and the DSCA that have roles in counterterrorism operations. The DIA provides a wide-range of intelligence support to DoD, which includes the Joint Intelligence Task Force for Combating Terrorism that consolidates terrorism related intelligence for DoD. The Military Department Intelligence Services are the intelligence organizations that are organic to the Army, Navy, Air Force, and Marine Corps. They focus on the intelligence requirements of their specific service. The NGA provides geospatial intelligence, which includes imagery, to assist decision makers and commanders planning and conducting operations. The NRO is responsible for space based intelligence collection, and works closely with other interagency partners within the IC. The NSA is the agency responsible for national signals intelligence and information assurance. The NSA plays a large role in supporting counterterrorism operations. The DSCA directs and manages security cooperation programs and is a hub for interagency coordination.[130]

The Treasury identifies and targets financial networks that sustain terrorism and has several elements that are involved in counterterrorism operations. The Office of Foreign Assets Control (OFAC) is responsible for managing and enforcing sanctions. The Office of Terrorism and Financial Intelligence is responsible for synchronizing terrorism related intelligence and enforcement within the Treasury. In addition, the Office of Intelligence Analysis (OIA) is part of the TFI and provides intelligence related to terrorist financial support networks and other threats.[131]

The DNI is the head of the U.S. Intelligence Community (IC) and is the primary intelligence advisor to the President and the NSC. The National Counterterrorism Center (NCTC) is part of the DNI. The NCTC is responsible for intelligence support designed to counter transnational terrorist threats, and it includes analysts from over 16 organizations.

---

[129] Obama, *2008 Unified Command Plan*, 4.

[130] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-13 – 1-14.

[131] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-17 – 1-18.

The CIA is a member of the IC and reports directly to the DNI. The CIA has a primary focus on national level human intelligence collection operations. See figure 2 for a chart on the IC.

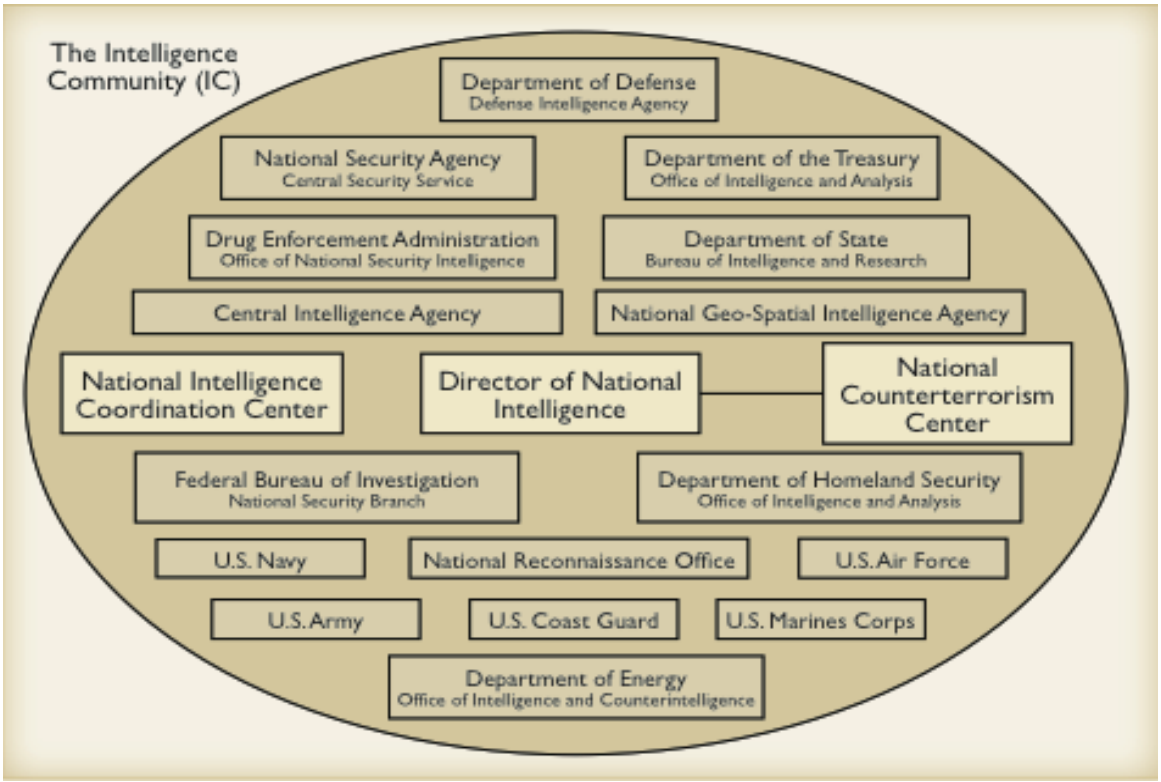

Figure 6. The Intelligence Community (IC) [132]

The DoJ also has a counterterrorism role and includes the Drug Enforcement Agency (DEA) and the Federal Bureau of Investigation (FBI). The DEA is part of the IC and focuses on threats from drug traffickers and global terrorist networks. The FBI is the lead U.S. government agency for domestic counterterrorism, but also works internationally to combat terrorism.[133]

The U.S. Country Team for a particular country is also a stakeholder. According to the SOF Counterterrorism Reference Manual:

[132] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-18 – 1-19.

[133] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 1-14 – 1-15.

> Led by the U.S. Ambassador or Chief of Mission (COM), the Country Team serves as the multifaceted "face" of the USG interagency process. The Country Team is made up of USG representatives who are placed on the ground to ensure the successful functioning of the programs administered by their parent departments, agencies and organizations. The COM has the discretionary authority to organize her Country Team in whatever fashion she sees fit.
>
> Members of the Country Team include: the Chief of Mission, Deputy Chief of Mission, Consul General, Economic Counselor, Management Counselor, Political Counselor, Political-Military Officer, Narcotics Control Officer, Public Affairs Officer, Regional Security Officer, Community Liaison Officer, USAID Representative, Defense Attaché, Commercial Counselor, Security Assistance Officer, Legal Attaché, Resident Legal Advisor, Political and Economic Section Chief, Treasury Attaché, Immigration and Customs Enforcement Attaché, Agricultural Attaché, Drug Enforcement Attaché, Aviation Attaché, Peace Corps Director, Office of Regional Affairs, and NCOIC USMC Security Detachment.[134]

In addition to the U.S. government, traditional U.S. allies and host nation partners are also stakeholders. However, due to the each of these countries having their own self-interest, as well as uniqueness of each location, their stakeholder interests will not be covered in this thesis. It is critical to keep this in mind when examining the environment the Fusion Node will operate in.

B. STRATEGY AND PURPOSE

President Obama's 2010 National Security Strategy (NSS), provides his Geo-Political and economic vision for the U.S. The policy guidelines set forth by the NSS allow the Secretary of Defense to align essential political-military strategic objectives and design the National Defense Strategy (NDS).[135] The president use of "align essential political-military" is the foundation that ensures interagency manpower, financial and collection resources allocated to a Fusion Node. Secretary Gates remarked that the new NDS is a balance between sustaining our force superiority and the need for cutting-edge capabilities to prevail against a persistent and emerging asymmetric or irregular

[134] JSOU, *SOF Interagency Counterterrorism Reference Manual*, 2-1, 2-3.

[135] DOD, National Defense Strategy 2008, 2–4.

adversary.[136] The NSS and NDS reflect the need for a strategic approach that can evolve and adapt in response to a changing security environment. The current battlefield encompasses air, sea, land and space challenges: violent extremist movements, transnational organized crime, rouge states, the proliferation of weapons of mass destruction (WMD), rising regional powers, emerging and failed states, resource conflicts, cyber-warfare, etc… The desired end state and goals are derived from the unit's next higher Agency headquarter, as well as Task Force Commanders Intent and Mission statement. The operational plan is aligned with theater campaign plans and synchronized with DoD National Defense Strategy. Understanding U.S. DoS and DoD strategy and purpose is important when evaluating the best environments to establish Fusion Nodes to maximize their performance capabilities.

C. STRUCTURE

In recent years, al Qaeda and its affiliated terrorist movements have developed a "less centralized command and control, (with) no clear center of gravity, and likely rising and falling centers of gravity, (dependent) on where the U.S. and the International focus is for that period."[137] They have adopted a social network spanning 70 countries, incorporating modern communications to expand their influence even further, and diversified their modus operandi to include less sensational attacks albeit not less deadly.[138] These small networks and associated nodes have contributed to the globalization of terrorist activity across both time and space resulting in a complex and unstable environment for the international community.

In order to effectively combat this threat, the U.S. must adopt an approach similar to that which is being utilized by the specific terrorist network in each region. This holds true to Ivan Arreguín-Toft's hypothesis that "same-approach interactions—whether direct-direct or indirect-indirect—favor strong actors because they imply shared values,

---

[136] Robert M. Gates. *National Defense Strategy.* Outlines DOD Strategy ISO the National Security Strategy 2010, Washington DC: Department of Defense, 2008, 1-2.

[137] John Rollins, "Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy," *Congressional Research Service*, January 25, 2011, (accessed February 17, 2011), i.

[138] Ibid., i.

aims, and victory conditions" as those of their opponents, in this case, non-state, terrorist actors.[139] Strong actors, such as the United States, "will win the same-approach interactions in proportion to their advantage in relative power."[140] This implies the U.S. will obtain better results dependent on its relative strength if it adopts a networked approach to combating the terrorist threat. The only limiting factor in this equation is time. Every commander realizes the "Washington Clock" continues to tick and popular public opinion is the only variable that can extend the ever-dwindling timeline.

To be successful, we must adopt what GEN(R) Stan McChrystal learned during his service as a task force commander:

> Al Qaeda in Iraq's lieutenants did not wait for memos from their superiors, much less orders from bin Laden. Decisions were not centralized, but were made quickly and communicated laterally across the organization.[141]

We must adopt a similar, decentralized approach, and allow regional task forces to operate with autonomy. Therefore, in order to successfully compete against the menace posed by a decentralized, global terrorist network, the organization must adopt a similar structure and social system. Due to the complexity of the environment and the unstable conditions in which terrorists operate, the most appropriate design for this organization is, what Mintzberg terms, a divisional form, due to the diverse problem-set resident in each regional affiliate.[142] Systemic to this organization is a group of "independent entities coupled together by a loose administrative structure."[143] A design of this nature provides an overlay in which a global, counter-terrorism (CT) network is placed on top of the existing non-state, terrorist actor.

---

[139] Ivan Arreguin-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (Summer 2001): 121.

[140] Ibid., 121–122.

[141] Stanley A. McChrystal, "It Takes a Network," *ForeignPolicy.com*, February 22, 2011, http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network (accessed February 22, 2011).

[142] Henry Mintzberg, "The Structuring of Organizations," in *The Strategic Process: Concepts, Contexts, and Cases*, 276-303 (Englewood Cliffs, NJ: Prentice-Hall, 1988), 301.

[143] Ibid., 301.

In order to adopt this form, a certain degree of bureaucracy is necessary; much like it is exhibited by the leadership of Ayman al-Zawahiri. Therefore, the global, counter-terrorism organization must have a centralized command and control orchestrating and ensuring transparency between each of its divisions. This strategic apex should reside within the interagency hub located within the National Capital Region (NCR) of the U.S. in order to allow easy access to key decision-makers within the government. Many other CT focused start-ups recognize the importance of maintaining close communications and easy access to policy makers; it is essential to capture lessons already learned by these organizations.[144] Because of their counter-terrorism functions, they retain a stakeholder status within the proposed organization and could benefit from mutual cooperation. In addition to easy access to government stakeholders, the benefit of using the nation's hub also capitalizes on the abundant resource pool resident within the district. Over the past ten years there has been a steady migration of experts, both academic and technological, to the region, which could provide valuable inputs to the organization. These come in the form of analysts who spent years deploying in support of Operation ENDURING FREEDOM and Operation IRAQI FREEDOM as well as the targeting experts who refined the technical capabilities that provide fidelity on the locations and activities of terrorist leaders and facilitators.

The subcomponents within this divisional organization will align with the respective threat in the region. While the strategic apex remains close to the political elite, the operational components will remain close to the fight. For example, both Iraq and Afghanistan would receive dedicated divisions due to the size and complexity of the terrorist threat in these existing warzones. Using Mintzberg's terminology, the support staff within the operating core must specialize in Middle-Eastern and Arab affairs with an expansive knowledge of tactical trends utilized by terrorists in this area. Both organizations would focus their efforts toward al Qaeda in Iraq (AQIZ) and al Qaeda's Senior Leaders (AQSL) while monitoring the splinter groups such as the Kurdistan

[144] Kimberly Dozier, "U.S. Building a Network To Hit Militants," *MSNBC.MSN.com*, January 05, 2011, http://www.msnbc.msn.com/id/40930584/ns/us_news-security/ (accessed February 13, 2011). This article discusses the stand-up of a counter-terrorism center in the nation's capital to speed the sharing of information in order to decrease the time between targeting and military action.

Workers Party, the Palestine Liberation Front, and Hezbollah in Iraq. Likewise, subdivisions focusing on the emerging threats in Yemen—AQ in the Arabian Peninsula (AQAP), Somalia—al Shabaab, North Africa—AQ in the Islamic Maghreb (AQIM), as well as the threats emanating from Europe, the Pacific and South American would have a dedicated organization focused on their area of responsibility.

The structure of these subcomponents cannot fit a pre-existing mold. Due to the complexity of the environment and the unstable conditions posed by an adaptable adversary, the regional organizations must be what Mintzberg defines as an adhocracy. Each must "innovate in very complex ways" in order to counter the disparate threat since terrorists' modus operandi in their respective regions generally differ.[145] The current conflicts in Iraq, Afghanistan, and to a certain extent, Pakistan, pose a very different problem for operational elements than those groups operating in the Horn of Africa, Indonesia, and Columbia. On the violent end of the spectrum rests the threat of daily attacks or improvised explosive device ambushes. On the opposite end resides the unknown prospect of a catastrophic attack being planned or the random kidnap for ransom operation to fund future terrorist operations.

In order to effectively pursue these various threats, highly specialized regional experts must fill the adhocratic task force. They must be allowed to operate independently and be given the authority to liaison directly with their respective agency and host nation counterparts. Bureaucracy and protocols cannot hinder the lines of communication between the adhocratic sub-elements and their counterparts in other regions. They must be empowered to make decisions or, at a minimum, access decision makers at a moment's notice. Non-state, terrorist actors are not restricted by boundaries, nor should the task forces. In order to move as quickly as the enemy, the highly trained experts must rely on a high degree of mutual adjustment with specialists in other regions as well as unhindered vertical adjustment with the divisional leadership.[146] Figure 3 provides a rough diagram of how the divisional organization is structured with adhocratic sub-elements. The adhocratic organizations within the divisional structure should reside

[145] Mintzberg, "Structuring Organizations," 301.

[146] Mintzberg, "Structuring Organizations," 302.

in their respective focus areas: Iraq (IZ), Afghanistan-Pakistan (AFG/PAK), North Africa (Trans Sahel), Arabian Peninsula (AP), Europe (EU), Pacific (PAC), and South America (SA).

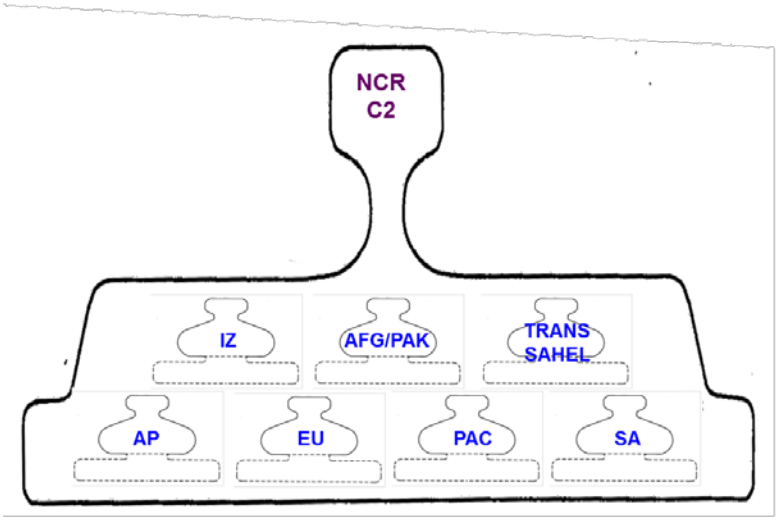

Figure 7. Divisional Organization with Adhocratic Sub-elements

It is imperative, although not an easy task, to place each organization in a location that will allow it to be most effective; much in the way the strategic apex of the division should be located in NCR. The task force focusing on the Iraqi terrorism problem set could be place in Baghdad with relative ease. Similarly, the task force overseeing counter-terrorism operations in Afghanistan and Pakistan could locate in Kabul or Islamabad. The difficulty will arise in creating these organizations in areas outside of a combat zone because of limited U.S. Embassy housing and office space, the lack of a status of forces agreement (SOFA), or simply lack of support from the host nation due to their anti-U.S. policies. For example, the ideal location to place a task force focusing on the AQAP problem set is Yemen. If constraints prevent the task force from operating within the borders of the country, it could possibly find space in nearby Djibouti or Qatar. Both have a small U.S. military base with airfields. From these locations, the task force could also focus its resources on the al Shabaab group in Somalia.

A more daunting challenge is identifying the best location to establish an adhocratic task force in North Africa to counter AQTS. The region extends over four

time zones and does not contain any governments with pro-U.S. agendas or tendencies. In this case it would be beneficial to co-locate with our French counterparts (if they are willing), since they declared war on AQIM in 2010 as a result of the assassination of French citizens by Nigerian and Mali terrorists.[147] Similar problems arise when trying to identify the ideal location for European, Pacific, and South American task forces. In these cases it would be best to co-locate with the Theater Commands and establish smaller sub-elements in countries that have a terrorism problem, and ideally, request U.S. assistance; however, this is not a necessary condition. Figure 2 offers an example of an adhocratic organization with an AQIM focus with experts spread throughout the region.

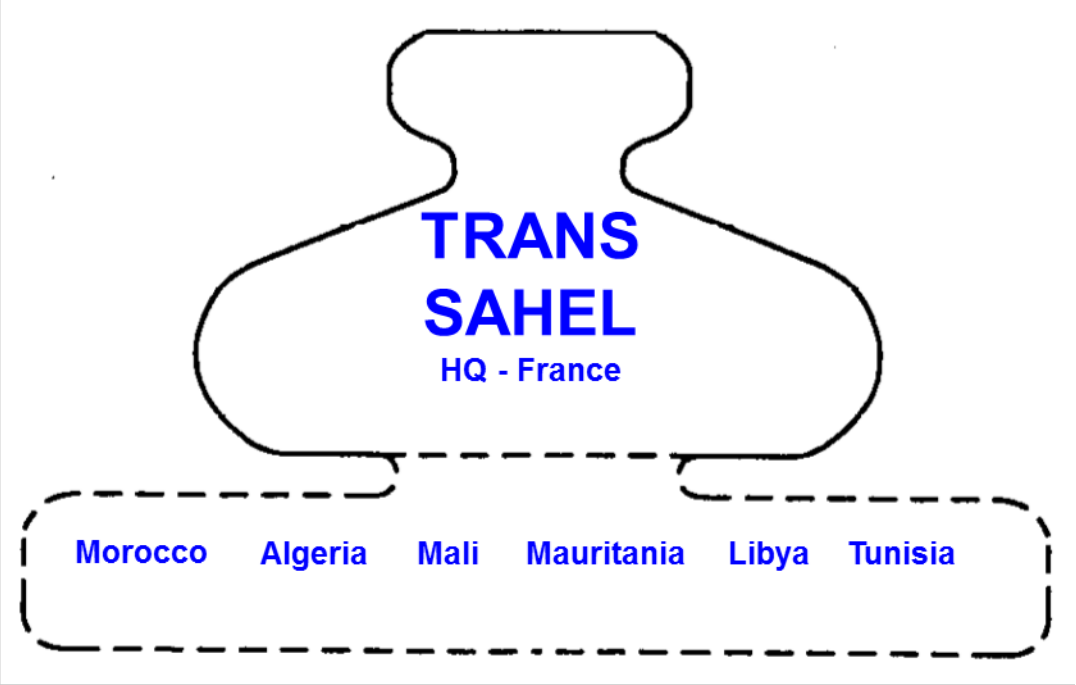

Figure 8. Example of Adhocratic Organization with Focus on AQIM

As previously mentioned, a problem establishing presence, whether requested or not, often lies in the ability to find a secure working space and billeting. The U.S.

[147] Paris - The Associated Press, "France Declares War Against al Qaeda," *HurriyetDailyNews.com*, July 28, 2010, http://www.hurriyetdailynews.com/n.php?n=france-declares-war-against-al-qaeda-2010-07-28 (accessed February 28, 2011). The French Prime Minister issued a declaration of war against al Qaeda after the murder of a French national by AQIM, which marked a shift in strategy for the French who generally had a behind-the-scenes approach to battling terrorism.

Department of State Bureau of Diplomatic Security (BDS) faces similar challenges while having an overlapping counter-terrorism mission through the execution of the Rewards for Justice Program.[148] Although it operates out of 188 countries, there remain several key locations in which it could be effective. The lack of embassy space and host nation cooperation are the limiting factors in conducting many CT operations simply because of the difficulty accessing the region. The task forces must capitalize on the existing structures and partners in these difficult to reach countries and use existing organizations, such as the BDS, to assist their efforts. They must also rely on partner nation assistance to access countries that are even more restrictive, such as Syria and Lebanon, to pass demarche requests or intelligence packets on terrorist residing within their borders.

The CT task forces must transcend problems such as these through open lines of communication and vertical adjustment between regional task forces. As evident in Iraq circa 2006, one third of the terrorist foreign fighters streaming into the country originated in North Africa, transiting through Syria, before crossing into Iraq.[149] They recognize no borders or boundaries. Similarly, the analytical experts within the task force must be allowed to bypass the barriers resident in theater and combatant commands. The traditional dialogue required to cut across arbitrarily designated borders and areas of operation and or responsibility simply serves as a hindrance to effectiveness and results in slower reaction times for matters that are often time-sensitive.

In addition to the horizontal integration between the regional task forces there must be an even higher degree of lateral coordination within the intra-agencies of the task force. To maximize effectiveness, experts from the interagency as well as the Department of Defense will fill the positions within the task force in order to capitalize on each organization's respective authorities. The U.S. Department of State Bureau of Diplomatic Security is just one example of the many agencies and experts that are

---

[148] Michael Bayer, "Operation Global Pursuit: In Pursuit of the World's Most Dangerous Fugitives and Terrorists," *The Police Chief* 72, no. 8 (August 2005): 32–37.

[149] Joseph Felter and Brian Fishman, "Al-Qaeda's Foreign Fighters in Iraq: A First Look at the Sinjar Records," *Combating Terrorism Center at West Point, United States Military Academy, West Point, NY*, December 19, 2007, http://www.ctc.usma.edu/harmony/pdf/CTCForeignFighter.19.Dec07.pdf (accessed February 28, 2011).

government stakeholders roles and responsibilities and contributors to the task force goals. The Department of State, Central Intelligence Agency, Department of Treasure, and Federal Bureau of Investigation also contribute to the pool of experts that will liaison with, if not hold seats in, the task force. Every player must be allotted the autonomy to coordinate directly with representatives in another agency and across the task force regions and, when established, will most closely resemble Duncan's matrix form. This set-up will allow for the "flexible sharing of human resources," will help "achieve coordination necessary to meet dual demands" such as those regions competing for resources, and is best suited to complex decision making and frequent changes in unstable environments, which is the type of setting provided by the global terrorist network.[150] The organizational design will also follow Thompson's theory in regards to reciprocal interdependence due to the horizontal feedback with respect to the task forces' mission of global pursuit.[151]

Each organization's size and structure will morph dependent on two independent variables, the nature of the threat and the level of access to the region. The nodes within a task force should consist of an experienced operational officer, an analytical expert of the region, and if possible, a communications specialist. It is conceivable that there may be room for only one mature, responsible team member in a particular country of interest. In this situation, the ability to ask for external support through the region hub of experts will alleviate the need for a bigger presence under these less than permissive locations. In many cases it may be impossible to place one of the task force experts in a country, such as in Libya or Syria, due to diplomatic strains. In these cases, the regional experts should be placed in surrounding countries that share our CT goals. The nature of a specific region's threat will also affect resource allocation. As the threat in an area is reduced, the resources allocated to that region will be moved to areas in need; however, it is important not to completely withdraw all resources and repeat the mistakes made by the French in Algeria circa 1962.

---

[150] Robert Duncan, "What Is the Right Organization Structure? Decision Tree Analysis Provides the Answer," *Organizational Dynamics*, Winter 1979: 429.

[151] Richard L. Daft, *Organization Theory and Design*, 9th Edition (Mason, OH: Thompson: South-Western, 2007).

In summary, a divisional organization is necessary to counter the existing terrorist network. The sub-elements of the divisional structure should be regional adhocracies forged with operational and analytical experts who can navigate the interagency to identify solutions to counter the terrorist threat within their area of responsibility. They must be able to capitalize on the existing authority's resident in other agencies and offer multiple options to policy-makers who must make a decision or pass those options to the host nation government. These specialists must also be able to communicate directly with task forces in other regions since the terrorist network recognize no boundaries. Foreign fighters routinely transit from Europe, North Africa, and the Arabian Peninsula to the Middle-Eastern warzones and often return to their country of origin to proliferate their destructive tendencies. Our network must operate with the same freedom of maneuver.

D. HUMAN RESOURCES

Identifying the right people to fill the operational and analytical positions is essential to the organization's success. In order to maximize effectiveness, recruiting must focus on the individual's expertise and abilities. These attributes must already be ingrained in the individual; therefore, rather than focusing on a training program to create experts to fill a position, efforts should be directed toward screening applicants who already possess these skills. The threat is here and now and the experts have grown and matured over the past ten years. This pool of existing experts will continue to expand as long as the U.S. continues to send troops to Iraq, Afghanistan, and other troubled spots throughout the world.

As was learned by "Wild" Bill Donovan while he stood up his force of OSS operatives, the proper psychological vetting of individuals and the establishment of a "sense of the importance of their mission" will ensure that those selected perform to the expected standards.[152] Because of this, the members of the OSS were able to operate independently and accomplished complex, dangerous tasks behind enemy lines without

[152] John Whiteclay Chambers II, "Office of Strategic Services Training During World War II ," *Studies in Intelligence* 54, no. 2 (June 2010): 16.

any supervision. Those same criteria are applicable to the members of a CT task force. They must be given the autonomy and sense of purpose to operate alone while being empowered to make decisions. This provides the intrinsic motivation to execute their mission to the highest of standards.

The selection process provides an additional incentive for those who are chosen; it establishes a cohesion and sense of elitism for each individual allowed into the organization. In order to retain this mindset, it is important to constantly assess the performance of the individual. Those who fail to perform must be removed. This should only occur when team members fail to uphold the standards and maturity necessary to operate in an independent setting. Members of the organization must be trusted to act accordingly to the stations they hold and are capable of adapt to their surroundings, specifically being able to adopt a personality that enables them to operate in an interagency and international environment. If they cannot acclimate, they should not be punished, only returned to their former employer with accolades for their contributions.

The events of 9/11 nationalized a vast number of individuals to fight the evils of terrorism. Everyone who volunteers for the organization will already possess the shared values and norms of those motivated individuals who signed up to fight. Their goal is to seek out and punish those responsible for the event as well as those who wish to replicate similar such events. Each successful operation that results in the prevention of another terrorist attack or that leads to the capture or kill of a known terrorist provides additional incentives for the organization's members. Success breeds additional success and builds cohesiveness, not only within the organization, but also within the international and interagency community who wish to be a part of that success.

E. CONCLUSION

Fusion Nodes will provide the U.S. government a joint-interagency means to integrate operations and intelligence with its allies and host-nations partners on a global scale to proactively degrade, deny and defeat terrorist networks. In order to accomplish this, it is critical to examine the organizational design requirements needed by Fusion Nodes. These requirements are:

- Identify any entity inside or outside of the Fusion Node who: has a vested interest in counterterrorism operations, will be affected by the counterterrorism strategy implemented by the Fusion Node, or is in a position to effect the adoption or execution of the Fusion Node's counterterrorism strategy
- Address the forces and objects that shape the Fusion Node and ensure its members are in agreement to achieve the unified purpose
- Identifying the right people to fill the operational and analytical positions is essential to the organization's success
- A group of "independent entities coupled together by a loose administrative structure

If these are requirement are met, Fusion Nodes will be a key component of the U.S. government efforts to target the global terrorist threat posed by Al Qaida, its affiliates, and other networked terrorist organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ackerman, Spencer. "U.S. Scans Afghan Inmates for Biometric Database." *Wired*. 25 August 2010. Accessed 10 October 2011. http://www.wired.com/dangerroom/2010/08/military-prison-builds-big-afghan-biometric-database/.

Arreguin-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26, no. 1 (Summer 2001). 93–128.

Barabasi, Albert-Laszlo, and Eric Bonabeau. "Scale-Free Networks," *Scientific American*, (May 2003): 52–56.

Bayer, Michael. "Operation Global Pursuit: In Pursuit of the World's Most Dangerous Fugitives and Terrorists." *The Police Chief* 72, no. 8 (August 2005). 32–37.

Bowden, Mark. *Killing Pablo: The Hunt for the World's Greatest Outlaw*. New York: Atlantic Monthly Press, 2001.

Brafman, Ori Brafman, and Rod Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin, 2006.

Buckwalter, David T., and Dana T. Struckman. "Colombia: Mission Impossible?" In Case Studies in Policy Making, 11th Edition, by Alvi-Aziz, Hayat and Knott, Stephen F., eds. Newport, RI: Naval War College, 2008. 81.

Chambers II, John Whiteclay. "Office of Strategic Services Training During World War II." *Studies in Intelligence* 54, no. 2 (June 2010). 1–28.

CIA, Directorate of Intelligence. Colombia: Alliances of Military Convenience. March 1993. Accessed 05 October 2011. http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItemImages.do?Multi=yes&queryType=quick&&ResultsID=1324170188A&QueryName=cat&ItemNumber=51&ItemID=CCD00752&imageNumber=2#imageTop.

Clapper, James R., Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence, 10 February 2010. Accessed 27 August 2011. http://www.dni.gov/testimonies/20110210_testimony_clapper.pdf.

Clausewitz, Carl von. *On War*. Translated by Michael Eliot Howard and Peter Paret. Princeton: Princeton University Press, 1989.

CNN Wire Staff. “Car Bomb Wounds 33 in Algeria.” CNN World. 14 August 2011. Accessed 10 October 2011, http://articles.cnn.com/2011-08-14/world/algeria.bomb_1_car-bomb-wounds-tizi-ouzou-algerian-city?_s=PM:WORLD.

Colburn, Forrest D. *The Vogue of Revolution in Poor Countries.* Princeton: Princeton University Press, 1994.

Cuomo, Chris, and Eamon McNiff. “The Men in the Shadows -- Hunting al-Zarqawi,” ABC News Good Morning America, 9 June 2006. Accessed 29 September 2011, http://abcnews.go.com/GMA/Terrorism/story?id=2056386&page=1.

Daft, Richard L. *Organization Theory and Design*, 9th Edition (Mason, OH: Thompson: South-Western, 2007.

Dozier, Kimberly. “U.S. Building a Network To Hit Militants,” *MSNBC.MSN.com*, January 05, 2011. Accessed 13 February 2011. http://www.msnbc.msn.com/id/40930584/ns/us_news-security/ .

Duncan, Robert. “What Is the Right Organization Structure? Decision Tree Analysis Provides the Answer.” *Organizational Dynamics*. Winter 1979: 429.

Eggen, Dan, Karen DeYoung, and Spencer S. Hsu. “Plane Suspect was Listed in Terror Database After Father Alerted U.S. Officials.” *The Washington Post*, 27 December 2009. Accessed 23 October 2010. http://www.washingtonpost.com/wpdyn/content/article/2009/12/25/AR2009122501355.html.

Felter, Joseph, and Brian Fishman. “Al-Qaeda’s Foreign Fighters in Iraq: A First Look at the Sinjar Records.” *Combating Terrorism Center at West Point, United States Military Academy, West Point, NY*. 19 December 2007. Accessed 28 February 2011. http://www.ctc.usma.edu/harmony/pdf/CTCForeignFighter.19.Dec07.pdf.

Finlayson, Kenneth. “Colombia: A Special Relationship.” *Veritas: Journal of Army Special Operations History* 2, no. 4 (2006): 5–7.

Flynn, Michael, Rich Jergens, and Thomas Cantrell. “Employing ISR: SOF Best Practices,” *Joint Force Quarterly* 50 (3d Quarter, 2008), 56-61.

Gates, Robert M. *National Defense Strategy.* Outlines DOD Strategy ISO the National Security Strategy 2010. Washington DC: Department of Defense, 2008.

Headquarters Department of the Army. *FM 3-24Counterinsurgency*. 15 December 2006. Accessed 1 November 2011, http://www.fas.org/irp/doddir/army/fm3-24.pdf.

Herring, George C. America’s Longest War: The United States and Vietnam, 1950–1975. New York: Wiley, 1979.

House of Representatives Ninety-Second Congress First Session. "U.S. Assistance Programs in Vietnam." Hearings Before a Subcommittee of the Committee on Government Operations. Washington: U.S. Government Printing Office, 1971.

Johnson, Andrew, and Emily Dugan. "Wealthy, Quiet, Unassuming: the Christmas Day Bomb Suspect." *The Independent*, 27 December 2009. Accessed 27 August 2011. http://www.independent.co.uk/news/world/americas/wealthy-quiet-unassuming-the-christmas-day-bomb-suspect-1851090.html.

Joint Interagency Task Force South. Accessed 05 October 2011. http://www.jiatfs.southcom.mil/index.aspx.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010. Accessed 1 November 2011, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Joint Special Operations University. *Special Operations Forces Interagency Counterterrorism Reference Manual*. Hurlburt Field: The JSOU Press, 2009.

Kilcullen, David J. "Countering Global Counterinsurgency." *Journal of Strategic Studies* 28 no. 4 (August 2005): 598–603.

Leites, Nathan, and Charles Wolf Jr. *Rebellion and Authority: An Analytic Essay on Insurgent Conflict*. Chicago: Markham Publishing Company, 1970.

Lewy, Guenter. *America in Vietnam*. Oxford: Oxford University Press, 1980.

Kraul, Chris. "Colombia assuming instructor role for other militaries." www.LATimes.com. March 6, 2011. Accessed 14 March 2011. http://articles.latimes.com/2011/mar/06/world/la-fg-colombia-mexico-pilots-20110306.

Kissinger, Henry. *Diplomacy*. New York: Simon & Shuster, 1994.

Mason, R., and I. Mitroff. *Challenging Strategic Planning* Assumptions. New York: John Wiley, 1981.

McChrystal, Stanley A. "It Takes a Network." *ForeignPolicy.com*. February 22, 2011. Accessed 22 February 2011. http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network .

McCormick, Gordon H. "A Systems Model of Insurgency." Department of Defense Analysis, (Naval Postgraduate School, Monterey, CA, 2006).

McCormick, Gordon H. and Frank Giordano. "Things Come Together: Symbolic Violence and Guerrilla Mobilization." *Third World Quarterly* 28. 2007.

McFadden, Robert D. Drug Trafficker Convicted Of Blowing Up Jetliner. December 20, 1994. Accessed 6 October 2011. http://www.nytimes.com/1994/12/20/nyregion/drug-trafficker-convicted-of-blowing-up-jetliner.html?src=pm.

Mintzberg, Henry. "The Structuring of Organizations." in *The Strategic Process: Concepts, Contexts, and Cases*, 276-303 (Englewood Cliffs, NJ: Prentice-Hall, 1988).

Munsing, Evan, and Christopher J. Lamb. "Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success." *Institute for National Strategic Studies: Strategic Perspectives*, 5, (June 2011):. 21–30.

National Public Radio. "Timeline: America's War on Drugs." April 02, 2007. Accessed 05 October 2011. http://www.npr.org/templates/story/story.php?storyId=9252490.

Obama, Barack. *2008 Unified Command Plan*. Washington DC: Office of the President of the United States, 2008.

Office of the Coordinator for Counterterrorism. *Our Mission*. Accessed March 1, 2011. http://www.state.gov/s/ct/about/c16570.htm.

Office of Congressional Affairs, Central Intelligence Agency. "Briefings of NSC and SSCI on "Los Pepes" Affair: Secret, Memorandum for Record, OCA 2512-93." Digital National Security Archive. December 06, 1993. Accessed 10 October 2011. http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&queryType=quick&ResultsID=13259A972FC&QueryName=cat&ItemNumber=72&ItemID=CCD00801.

Our History: Organization of American States. 2011. Accessed 2 October 2011. http://www.oas.org/en/about/our_history.asp.

Padgett, Tim. "Colombia's Stunning Hostage Rescue." Time. July 02, 2008. Accessed 10 October 2011. http://www.time.com/time/world/article/0,8599,1819862,00.html.

Paris - The Associated Press, "France Declares War Against al Qaeda," *HurriyetDailyNews.com*, July 28, 2010. Accessed 28 February 2011. http://www.hurriyetdailynews.com/n.php?n=france-declares-war-against-al-qaeda-2010-07-28.

Patterson, Anne W. "Notes from the Field: A View from Medellín Confidential, Cable, 011431." Digital National Security Archive. December 21, 2001. Accessed 5 October 2011. http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&queryType=quick&ResultsID=13259FF8D6A&QueryName=cat&ItemNumber=83&ItemID=CCD01851.

Rollins, John. “Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy.” *Congressional Research Service*. January 25, 2011.

Rosenau, William, and Austin Long. The Phoenix Program and Contemporary Counterinsurgency. Research Paper, RAND National Defense Research Institute, Arlington: RAND Corporation, 2009.

Rowe, A.J., R.O. Mason, and K.E. Dickel. *Strategic Management & Business Policy: A Methodological Approach*. Reading, MA: Addison-Wesley, 1985.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Shanker, Thom. “Special Operations: High Profile, but in Shadow.” The New York Times. 29 May 2007. Accessed 29 September 2011. http://www.nytimes.com/2007/05/29/world/middleeast/29forces.html?ref=abumusabalzarqawi.

Stewart, Richard W. “Chapter 8. CORDS and the Vietnam Experience: An Interagency Organization for Counterinsurgency and Pacification.” In Project on National Security Reform Case Studies Volume I, by Richard Weitz (Editor), 451-481. Washington DC: Center for the Study of the Presidency, 2008.

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

Tovo, Ken. From the Ashes of the Phoenix: Lessons for Contemporary Counterinsurgency Operations. Carlisle Barracks: U.S. Army War College, 2005.

US-Iraq Status of Forces Agreement, 17 November 2008, p. 3-15. http://graphics8.nytimes.com/packages/pdf/world/20081119_SOFA_FINAL_AGREED_TEXT.pdf.

US Army FM 3-09.12, *Tactics, Techniques, and Procedures for Field Artillery Target Acquisition*, June 2002.

U.S. Department of State. *Country Reports on Terrorism 2010*. 18 August 2011. Accessed 1 November 2011, http://www.state.gov/s/ct/rls/crt/2010/170265.htm.

USEMB Cable - Colombia. “GFZE-92-8001, [Excised] Operation Envigado CCX: ZE-89-0007, [Excised] Pablo Escobar-Gaviria TKO-558, TKO Coordinator GFAI-93-9020, Threats/Assaults, Confidential, Cable, 006250.” Digital National Security Archive. April 23, 1993. Accessed 05 October 2011. http://nsarchive.chadwyck.com.libproxy.nps.edu/quick/displayMultiItem.do?Multi=yes&ResultsID=13259D15D46&queryType=quick&QueryName=cat&ItemNumber=59.

U.S. Military Assistance Command Vietnam. Directive 525-36-Military Operations, Phoenix (Phung Hoang) Operations. San Francisco, 18 May 1970.

———. Phung Hoang Advisors Handbook. San Francisco, 20 November 1970.

Voice of America News. “US Officials Confident Al-Qaida’s No. 2 Killed in Pakistan.” 29 August 2011. Accessed 29 August 2011. http://www.voanews.com/english/news/US-Officials-Confident-Al-Qaidas-No-2-Killed-in-Pakistan-128592638.html.

Wendt, Eric P. “Strategic Counterinsurgency Modeling.” *Special Warfare* (September 2005): 5–6.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. JSOU
   Hurlburt Field, Florida

4. SOCOM J-7
   MacDill AFB, Florida

5. HQ USSOCOM Library
   MacDill AFB, Florida

6. ASD/SOLIC
   Washington, DC