2011-06

Targeting Social Network Analysis in Counter IED Operations

Giles-Summers, Brandon.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TARGETING: SOCIAL NETWORK ANALYSIS IN COUNTER IED OPERATIONS

by

Jeffrey Morganthaler
Brandon Giles-Summers

June 2011

Thesis Advisor: Heather Gregg
Second Reader: Sean Everton

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** June 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Targeting: Social Network Analysis in Counter IED Operations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jeffrey Morganthaler and Brandon Giles-Summers			
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)

The purpose of this research is to provide insights to Commanders in the field for attack-the-network (AtN) operations in the fight against Improved Explosive Devices (IED). Established in 2006, the Improved Explosive Devices Defeat Organization (JIEDDO) has spent billions of dollars to execute its operational mandate: defeat the device, attack the network, and train the force. JIEDDO has excelled in training the force and defeating the device, but lagged behind in providing necessary information to facilitate attack-the-network operations. To facilitate AtN operations, JIEDDO created a Counter-IED Operation Integration Center (COIC), which provides analysis, but utilizes metrics that are not necessarily intuitive. Rather than metrics, what commanders need is a clear understanding of what *attack the network* means in order to create lines of operations that undermine networks that use IEDs. The goal of this thesis, therefore, is to define attack-the-network, introduce social network analysis, provide a focused discussion on how to apply social relational information to operations, determine a targeted person's relevance, provide operational commanders with a basic matrix to gain perspective on social interactions of network members, and offer case studies illuminating the difficulties inherent in network targeting.

14. SUBJECT TERMS Social Network Analysis, Counter Terrorism, Attack-The-Network, Counter-IED Operation, Leadership Targeting, Terrorist Network.			**15. NUMBER OF PAGES** 65
			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

TARGETING: SOCIAL NETWORK ANALYSIS IN COUNTER IED OPERATIONS

Jeffrey Morganthaler
Lieutenant Commander, United States Navy
B.A., University of Texas, 1991

Brandon Giles-Summers
Lieutenant, United States Navy
B.S., Liberty University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

NAVAL POSTGRADUATE SCHOOL
June 2011

Author: Jeffrey Morganthaler

Brandon Giles-Summers

Approved by: Heather Gregg
Thesis Advisor

Sean Everton
Second Reader

Gordon H. McCormick
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this research is to provide insights to Commanders in the field for attack-the-network (AtN) operations in the fight against Improved Explosive Devices (IED). Established in 2006, the Improved Explosive Devices Defeat Organization (JIEDDO) has spent billions of dollars to execute its operational mandate: defeat the device, attack the network, and train the force. JIEDDO has excelled in training the force and defeating the device, but lagged behind in providing necessary information to facilitate attack-the-network operations. To facilitate AtN operations, JIEDDO created a Counter-IED Operation Integration Center (COIC); this center provides analysis, but utilizes metrics that are not necessarily intuitive. Rather than metrics, what commanders need is a clear understanding of what *attack-the-network* means in order to create lines of operations that undermine networks that use IEDs. The goal of this thesis, therefore, is to define attack-the-network, introduce social network analysis, provide a focused discussion on how to apply social relational information to operations, determine a targeted person's relevance, provide operational commanders with a basic matrix to gain perspective on social interactions of network members, and offer case studies illuminating the difficulties inherent in network targeting.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALN	Armèe de Libèration Nationale
AtN	Attack-the-Network
BC	Betweenness Centrality
CC	Closeness Centrality
CCE	Comite de Coordination et d'Execution
COIC	Counter-IED Operations Integration Center
COIN	Counterinsurgency
CT	Counter Terrorism
DC	Direct Centrality
DI	Darul Islam
EFP	Explosively Formed Penetrator
FLN	National Liberation Front
IED	Improvised Explosive Device
IRGC	Iran Revolutionary Guard Corps
ISWAT	Iraq Special Weapons and Tactics
JAM	Jaysh al-Mahdi (militia)
JI	Jemaah Islamiyah
JIEDDO	Joint Improvised Explosive Device Defeat Organization
ODA	Operational Detachment Alpha
QF	Qods Force
SF	Special Forces (Green Berets)
SG	Special Groups (militia)
SNA	Social Network Analysis
ZAA	Zone Autonome d'Alger

THIS PAGE INTENTIONALLY LEFT BLANK

I. ATTACK-THE-NETWORK

A. PURPOSE

The purpose of this thesis is to provide insights to Commanders in the field for attack-the-network (AtN) operations. While a fusion cell, such as Counter-IED Operation Integration Center (COIC), provides analysis that supports attack-the-network operations, these organizations utilize metrics that are not necessarily intuitive. Absent a clear understanding of the metrics involved, operational commanders are constrained in their application of the provided organizational insights in formulating lines of operations that undermine these networks. The goal of this thesis, therefore, is to define attack-the-network, introduce social network analysis, discuss how to apply social relational information to operations, determine a targeted person's relevance, provide operational commanders with a basic matrix to gain perspective on social interactions of network members, and offer case studies illuminating the difficulties inherent in network targeting.

B. ATTACK-THE-NETWORK DEFINED

What is meant by attack-the-network (AtN) operations? Counter-network operations usually focus on leadership targeting of an organization, which follows the logic that by catching the right hornet, the whole colony dies. What is often overlooked in this approach, however, is that if just a worker bee is killed, the nest is aggravated and a much bigger problem is created. While this concept provides a convenient metaphor to discuss possible targeting methodology, it seldom resembles the facts, because human networks are not directly analogous to a hornet's nest. In other words, not every situation can be resolved by a single kill or capture of the "queen." To better illuminate this challenge in attack-the-network operations, leadership targeting will be discussed in Chapter II.

Attack-the-network operations, for the purposes of this thesis, are defined as actions, kinetic or non-kinetic, used to disrupt, destroy, or reduce an enemy's capacity to mount terror operations, specifically groups that use IEDs. In particular, the procedure

provided in this thesis will focus efforts on destroying a network's functionality by attacking certain social relationships that tie the network together. Attack-the-network operations, therefore, will focus on utilizing social network analysis to identify targets based on organizational principals.

C. SOCIAL NETWORK ANALYSIS AND THE IMPORTANCE OF WEAK TIES

SNA is a social science that examines the structure of the social ties between and among individuals, tribes, organizations, etc.[1] As a result of its analytical components, SNA attracts and is used by scholars across the academic spectrum, such as sociologists, anthropologists, economists, mathematicians, computer scientist, statisticians and marketing specialists.[2] One result of this dynamic is that books on the subject can be quite lengthy.[3] The intention of this thesis is not to create SNA specialists, but to provide the operational commander and his staff a focused look at the use of SNA as a tool that can provide context to individuals that are known to interact with one another. Once the individual's context is known, an operational commander and his staff can then decide which, if any, lines of operation they wish to utilize in attack-the-network operations.

A helpful distinction that social network analysts draw, and one that is relevant to the present study, is the difference between weak and strong ties. Strong ties are those to actors with whom one engages regularly, such as close friends or family members. Weak ties, by contrast, are ties to actors with whom one comes into contact with occasionally or rarely.[4] While it might seem that interactions with strong ties should provide the most beneficial opportunities to an individual, studies show quite the opposite. For example, in 1973, Mark Granovetter examined interpersonal relations between a single actor and

1 Linton C. Freeman, The Development of Social Network Analysis: A Study in the Sociology of Science (Empirical Press, 2004): 2.

2 Linton C. Freeman, The Development of Social Network Analysis: A Study in the Sociology of Science, 5.

3 See, for example, Stanley Wasserman and Katherine Faust. Social Network Analysis: Methods and Applications. (Cambridge, UK: Cambridge University Press, 1994) and David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World (Cambridge University Press, 2010).

4 Sean Everton Tracking, Destabilizing and Disrupting Dark Networks with Social Network Analysis, Naval Post Graduate School electronic workbook, version 1.05, 12.

an acquaintance, in order to understand what, if any, beneficial affects these reciprocal, friendly, yet casual linkages could produce.[5] In his study, Granovetter examined professionals in the Boston area and found that acquaintances, or weak ties, created more and better job opportunities than close friends, or strong ties, because close friends tend to know each other and thus information within the strong social group is readily shared.[6] Conversely, when a person runs into an acquaintance they have not seen in a long time, new information is shared that otherwise would not have been obtained. Furthermore, the acquaintance is familiar enough with the person, such as a school mate or a prior co-worker, that they can provide insight into the potential for happiness at the new position.[7] This connection outside of one's core group, or cluster, is referred to as a "bridge," because it provides the only connection between two points.[8] Removal of this relationship, therefore, cuts the connection between the groups.

A follow-up study by Onnela et al. examined the ties between mobile phone users.[9] The authors analyzed phone records over an eighteen-week period and used the length of call and the frequency of calls between a pair of individuals as key indicators for strength of ties. Consistent with their hypothesis the authors saw that the majority of strong ties, judged as such by the reciprocal nature and the long duration, were clustered together.[10] Once groups were identified, the study moved to an analysis of the effects of removing specific ties. The study revealed that removal of weak ties, starting from the weakest link and working up, caused the communication network to break apart, while the removal of strong ties had little effect on the overall integrity of the network.[11] The

5 M. S. Granovetter, "The Strength of Weak Ties," American journal of sociology 78, no. 6 (1973): 1361.

6 M. S. Granovetter, "The Strength of Weak Ties," 1370.

7 M. S. Granovetter, "The Strength of Weak Ties," 1371–1373.

8 M. S. Granovetter, "The Strength of Weak Ties," 1364.

9 J. P. Onnela et al. "Structure and Tie Strengths in Mobile Communication Networks," Proceedings of the National Academy of Sciences of the United States of America 104, no. 18 (May 1, 2007): 7332.

10 J. P. Onnela et al. "Structure and Tie Strengths in Mobile Communication Networks," 7333.

11 David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World (Cambridge University Press, 2010): 53.

authors, therefore, concluded that weak ties function as bridges in the network and maintain the network's integrity, while strong ties play a significant role in maintaining the integrity of the local cluster.[12]

Related to the idea of the importance of bridges is the small-world study of Stanley Milgram and Jeffrey Travers in which they selected at random a "target person" and a group of "starting persons" in order to map acquaintance chains.[13] The basic premise was to understand how long it would take to transfer a selected item between two randomly selected individuals. The researchers provided experimental guidelines to the starting person that included: an explanation of the study (mail a document to a named person at an unknown location), the target person's name, and directions that if they did not personally know the target person, they were to send the document to an acquaintance they did know personally and believed provided the best chance for "success,"—success in this case meaning that the document reached the target person.[14] The results of this and subsequent studies have helped illuminate the importance of bridges in the transfer of information, in this case a document.[15] They have also demonstrated that the average "number of intermediaries" between two randomly selected people in the United States was approximately six links or ties.[16] "Six degrees of separation," as it is known, provides a unique insight into the usefulness of bridges in the diffusion process.

12 J. P. Onnela et al. "Structure and Tie Strengths in Mobile Communication Networks," 7336.

13 Jeffrey Travers and Stanley Milgram, "An Experimental Study of the Small World Problem," Sociometry 32, no. 4 (December 1, 1969): 428.

14 Travers and Milgram, "An Experimental Study of the Small World Problem," 428–429.

15 See, for example, Duncan J. Watts, "Networks, Dynamics, and the Small-World Phenomenon." American Journal of Sociology (1999) 105:493–527; Duncan J. Watts, Small Worlds: The Dynamics of Networks Between Order and Randomness. (Princeton, NJ: Princeton University Press, 1999); Duncan J. Watts, Six Degrees: The Science of a Connected Age (New York: W. W. Norton & Company, 2003) and Peter S. Dodds, Peter, Roby Muhamad, and Duncan J. Watts, "An Experimental Study of Search in Global Social Networks." Science (2003) 301:827–829.

16 Travers and Milgram, "An Experimental Study of the Small World Problem," 431.

These studies suggest a myriad of reasons why understanding networks, particularly dark networks, requires patience and attention to detail.[17] They provide overarching considerations that an operational commander and his staff should address in targeting analysis. First, weak ties, because they are typically the bridges between clusters, enable a rapid diffusion of tactics and techniques across a network, link one network to another, and provide a conduit for resupply of critical resources throughout the network. Second, weak ties are casual relationships that hinder detection because they are limited in nature and reside outside of the main group. Third, weak ties present a challenge at the tactical level because, in general terms, if the military focuses on an enemy it assumes has a similar design as itself and fails to identify the context of individuals, then it will miss an opportunity to "remove the legs" of their opponent. SNA provides context to the overall structure of a network as well as it allows the staff to visually display relationships that can be attacked or exploited.[18] More importantly, through the understanding the power of weak ties, an operational commander and his staff can align targeting information and tactical operations with their operational goals.

D. CONCLUSION

Current military doctrine does not present in-depth analysis of attacking and defeating IED networks. Furthermore, the idea of weak ties suggests one reason why the "conventional wisdom," or basic intuition, of leadership targeting does not maximize the probability of network collapse. The following thesis will provide one means for tracking and understanding the effects one has on networks through the implementation of a focused SNA approach. As such, the thesis proceeds as follows. Chapter II will present ideas for the operational commander and his staff in regards to employing SNA. It identifies key constructs such as network design, provides social metrics to focus identification on key positions within the organization, and finishes with a matrix to visualize lines of operations in support of attack-the-network. A familiarity with the idea of weak ties, therefore, will maximize the usefulness of the included matrix.

---

17 The term dark networks is used to describe IED, terror, or any other network that must remain covert in order for the network to survive in its operational environment.

18 B. H. Liddell Hart, *Strategy: Second Revised Edition*, 2nd ed. Plume, (1991): 349.

Chapters III, IV, and V will provide case studies to show the benefit of understanding networks and the associated roles performed by individuals. Chapter III will examine Algeria and the effective, at least in the short run, yet completely unacceptable way for attacking an IED network. Chapter IV examines Indonesia's tracking and eventual destruction of the Noordin Top IED Network. Chapter V will examine operations to counter the effects of IEDs in Iraq and the successful tactics employed during Operation Yarborough.

Chapter VI offers concluding thoughts on the what effect of attacking IED networks has on the overall picture of success in defeating an insurgency. Findings will include a recommendation for a change in the military lexicon to encourage a broader spectral analysis in network targeting, reasons for using IEDs in an insurgency, and how insurgencies typically end.

II. SOCIAL NETWORK ANALYSIS: AN OPERATIONAL COMMANDER'S FRAMEWORK

A. INTRODUCTION

Information on "attack the network" operations in military doctrine is sparse, and provides a limited understanding of what a network is, and how best to undermine it. However, in academia, literature on analytical tools and their utility in targeting insurgent IED cells or networks, such as social network analysis (SNA), is growing rapidly.[19] Targeting an enemy network is as multi-faceted as IED construction and therefore requires an in depth understanding of what a network is and how to attack it. This chapter will, therefore, provide a brief description on network typology, and offer a computational and visual analytical tool to help illuminate some of the ways for attacking the networks responsible for the placement and detonation of IED's. In the course of the following discussion, this chapter will also forward ideas to enhance critical thinking and debate between the operational commander and his staff in executing "attack the network" operations.

B. WHAT IS A NETWORK?

In order to attack the network, one must first have a basic understanding of what a network is. We will discuss network typology in two ways: macro, by the organizational design; and micro, through social network analysis, which identifies the individual types of nodes within the organization, or network. Focusing first at the macro level, organizations can be broken down into two main categories, those that are hierarchical in design and those that are distributed. A hierarchical organization, or network, is highly centralized and similar in structure to a large corporation, such as the military or any heavily bureaucratic organization, with information flowing to one central point.[20] The

19 K. M. Carley, Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva, "Destabilizing Dynamic Covert Networks," (in proceedings of the 8th international Command and Control Research and Technology Symposium, Pittsburg, Pennsylvania, 2003). Nancy Roberts and Sean F. Everton, "Strategies for combating dark networks," Journal of Social Structure, Vol. 12, No. 2, (2011): 1–32.

20 R. L. Daft, Essentials of Organization Theory and Design, Mason, OH. (2003): 107–111.

weakness within a hierarchical design is that information flows to one "great leader," for interpretation and response, which slows reaction time and adaption to the changing environment.[21]

Distributed networks, or the organizations typically targeted in attack the network operations, are the operational elements of the current IED fight, and can be broken down into three types: an all channel network, in which each node is linked to every other node; a star or hub network, in which one node serves as the central actor, which all other nodes must use to coordinate; and a chain or line network, in which people, information, and supplies, travel along a single path and where direct end-to-end communication does not exist.[22] The distributed network's strength lies in its innate ability to diffuse information through the network, and absorb shocks, or pulses, to the system, such as the capture or death of key individuals from coalition forces.[23] The organizational design of a distributed network is, therefore, distinct in its ability to quickly adapt to a situation or changing environment.[24]

Yet, within these seemingly amorphous groups, there is resemblance of a hierarchical structure, based on prestige, in which opinion leaders guide the networks adaptations. Opinion leaders are those members of a network that are able to informally influence others attitudes or actions.[25] The fluidity within the group's dynamics often means that the removal of this opinion leader, or a refocus of the group opinions, does not affect IED operations. It is this non-hierarchical idea of leadership that enables IED

21 John Arquilla and David F. Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy (Rand Corporation, 2001): 4.

22 John Arquilla and David F. Ronfeldt, Swarming and the Future of Conflict (RAND Corporation, 2000): 58–59.

23 John Arquilla and David F. Ronfeldt, Swarming and the Future of Conflict, 52.

24 John Arquilla and David F. Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, 12. K. M. Carley, Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva, "Destabilizing Dynamic Covert Networks."

25 Everett M. Rogers, Diffusion of Innovations, 5th Edition (Original Free Press, 2003): 24–37.

networks to overcome pulsing attacks on the leadership, and is why these relationships are often difficult to understand for people who work in environments dominated by the hierarchical framework.[26]

On the micro side of network analysis are the different measurements SNA gives in order to provide context to the intelligence picture. Three measurements are particularly important to the commander: degree centrality (DC), betweenness centrality (BC), and closeness centrality (CC). A brief description is provided to show the unique position each associated term has within the network and ways to target each.

- **DC**: focus is on the most active and visible members of the network, typically recognized as a leader within the network.[27]
- **BC**: focus is on the actors that are the path, or conduit, for two nodes to communicate. The more information and communications "funneled" through a node the higher the betweenness scores.[28]
- **CC**: focus is on how close an actor is to all other actors in the network, and reflects someone who can quickly interact with all others in the network.[29]

The combination of identifying the type of network one faces, and the actors or nodes within that network allows potential targets to be mapped and understood through SNA. This provides the operational commander and his staff the unique ability to decide on whether to use either a non-kinetic information operation/deception tactic, a kinetic kill or capture tactic or a combination.

C. SOCIAL NETWORK ANALYSIS AND MILITARY APPLICATIONS

Social network analysis, in its modern form, is accomplished using computer software with specifically designed algorithms that allow analysis of the patterns and structural properties of human relationships that define the inner workings of a specific

26 K. M. Carley, Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva, "Destabilizing Dynamic Covert Networks."

27 Stanley Wasserman and Katherine Faust, Social Network Analysis: Methods and Applications, 1st Edition (Cambridge University Press, 1994), 178.

28 Stanley Wasserman and Katherine Faust, Social Network Analysis: Methods and Applications, 1st Edition, 188–189.

29 Stanley Wasserman and Katherine Faust, Social Network Analysis: Methods and Applications, 1st Edition, 188–189. 183.

group or network.[30] SNA's software visualization capability provides an important quantitative display of relational ties within a network. For example, Valdis Krebs, who mapped the 9/11 terrorist network, and Jose Rodriguez, who mapped the March 11th Madrid bombing network, display the military application of SNA, by identifying the relations of those involved in these terrorist events.[31] In doing so, their research furthered the discussion on the importance of weak ties and the challenge of limited data on dark or covert networks.[32] In particular, Krebs points out that the strategy used by the 9/11 hijackers to keep cell members distant from each other was specifically designed to minimize damage if one member was compromised.[33]

However, what make endeavors in SNA worthwhile is that, if an operational commander can overcome his informational disadvantage through the application of intelligence gleaned from reconnaissance, village surveys, individual interviews, police assets, or any number other intelligence gathering resources, he can begin to literally develop a picture of his opponent and the network that supports his nefarious IED activities.[34] This information, analyzed through SNA software, can provide valuable insights on an enemy's network design from which weakness can be identified and targeted for either attack or exploitation operations. The observed change in the network, from an operation, then can be compared against the anticipated results and thereby confirm or deny the effectiveness of a chosen strategy. From there, the operational commander can maintain the current course of action or reassess and attack via an alternate line of operation.

---

30 Barry Wellman, "Toolkit Essay," Review of *The Development of Social Network Analysis: A Study in the Sociology of Science*, by Linton Freeman, *Contemporary Sociology*, May 2008, Vol. 37, No. 3, Book Review: 222.

31 V. E. Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3 (2002): 43–52.; J. A. Rodríguez, "The March 11th Terrorist Network: In its Weakness Lies its Strength," Working Papers EPP-LEA (2005).

32 V. E. Krebs, "Mapping Networks of Terrorist Cells," 44.

33 V. E. Krebs, "Mapping Networks of Terrorist Cells," 46.

34 Gordan H. McCormick and Frank Giordano, "Things Come Together: Symbolic Violence and Guerrilla Mobilisation," *Third World Quarterly* 28, no. 2 (January 1, 2007): 308.

SNA is, therefore, a type of applied art where social science and mathematics collide and value is determined by the operational commander. As an art style, however, SNA only represents one genre within the larger collective body of social relationship studies and should, therefore, be utilized as a tool and not the only means to an end.[35]

D. RECOMMENDATIONS TO THE OPERATIONAL COMMANDER

The success of a particular strategy will depend on the type of network you are trying to attack. As such, attack the network operations that work for one network may not work for another because of size, social structure, and because nodes are living and adapting beings.[36] This is where the judgment of the operational commander will be a balancing act between action and a wait-and-see posture. Unfortunately, this method places the operational commander on the horns of a dilemma: act and you alert the network you know of its existence and allow its members to escape; do not act and risk more casualties because the network persists.

The Holy Grail in attack-the-network operations is targeted killings that end a network's activity. In reality, targeted killing alone may not undermine an organization, and this option must be balanced against other possible operational approaches. For example, in her study of 298 groups, Jenna Jordan shows that, in order to understand if targeted killing would be effective, one has to take into consideration organizational age, type, and size.[37] This is where the amorphous network design and fluid concept of leadership presents its greatest challenge to hierarchical based thinkers. Even with these considerations taken into account, there is still no predicting when decapitation will actually be an effective means to ending an organization.[38]

---

35 Nancy Roberts and Sean Everton, "Strategies for Combating Dark Network."

36 K. M. Carley, Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva, "Destabilizing Dynamic Covert Networks."

37 Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," *Security Studies* 18, no. 4 (2009): 719–755.

38 K. M. Carley, Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva, "Destabilizing Dynamic Covert Networks."

The main intention of this thesis is to examine the literature in the light of actual cases and highlight best practices for attacking networks that use IEDs. Table 1 is provided as an easy reference for the operational commander to inform decisions about attack the network operations.

Targeting Matrix		Interdiction vs. Channeling			
		Interdiction		Channeling	
		Sequential	Simultaneous	Sequential	Simultaneous
Small Network	DC				
	BC				
	CC				
Large Network	DC				
	BC				
	CC				

Table 1. Operational Commanders targeting matrix

Starting with the horizontal axis, the first decision point is whether one is facing a large or small network. The pros and cons of a small network verses a large network campaign involves an inverse in strategy because "size matters."[39] A large organization, such as Hezbollah, will suffer a lesser degree of disrupted operations when unique specialized operators are eliminated; however, a smaller group, such as the Special Groups in Iraq, will feel a greater impact to operations. The degree of the impact to the smaller group is based on many things including: being less able to adapt to its environment, reducing performance as a result of lost skill set, inhibiting the flow of information.[40] In other words, a small network would be more likely to succumb to shocks to its operational structure, yet it is hard to uncover the fact that it exists. On the other hand, large networks are easier to uncover, but much harder to design shock factors that will reduce or eliminate its existence.

[39] Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," *Security Studies* 18, no. 4 (2009): 719–755.

[40] K. M Carley, J. S Lee, and D. Krackhardt, "Destabilizing networks," *Connections* 24, no. 3 (2001): 31–34.

The next decision point is which node to attack or manipulate, based on centrality measures, with a more refined explanation of these metrics below.

- **DC**: this measures "where the action is," and provides a metric for network leadership that can be used in determining targets or targeting effects.[41]
- **BC**: are the people within the organization that bridge the gap between the local network and its outside means of support for people, guns and money.
- **CC**: represents someone who can quickly access a multiple nodes of the network.

Shifting to the vertical axis, the commander's method of approach is the first decision. Interdiction is a kinetic approach, typically a direct action mission, with the intent to kill or capture the intended target.[42] Channeling, on the other hand, is a non-kinetic attack on the node(s) or actor(s) that represents the route traveled by particular resources, assets, or pieces of information. Channeling can be done any number of ways, including: psychological operations aimed at influencing the emotions, reasoning, cohesion and behavior of a network; amnesty, negotiations, political opportunities or a similar strategy of enemy engagement; information operations aimed at reducing the means to communicate or targeting electronic devices; increasing the cost benefit analysis for the network members by increasing the punitive measures against their particular activity; network burn out; or backlash from the population over actions use by the network.[43]

In actuality, the above decisions are not either-or situations, but a combination of techniques best suited to attack a specific network.

---

41 Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, 1st Edition, 179.

42 Nancy Roberts and Sean F. Everton, 2009, "Strategies for Combating Dark Networks."

43 Nancy Roberts and Sean F. Everton, 2009, "Strategies for Combating Dark Networks", A. K. Cronin, "How al-Qaida Ends: The Decline and Demise of Terrorist Groups," *International Security* 31, no. 1 (2006): 41–47. Martha Crenshaw, "How Terrorism Declines," *Terrorism and Political Violence* 3, No. 1 (1991): 80–84.

E. CONCLUSION

While SNA is not a panacea against terror organizations, it does provide a good reference point for estimating the effectiveness of actions taken to attack dark networks. The dilemma that the operational commander must face is to either act or wait for more information. SNA provides a valuable tool for making this decision. It is therefore necessary to ensure attack the network is more than just a concept in a publication, but is tangible with causal logic and tools for analysis. How an Operational Commander thinks about networks, and a reassessment of the logic associated with relational ties, must occur as we adapt to the fluidity inherent in a networks basic structure.

III. ALGERIAN CASE STUDY

A. INTRODUCTION

There have been several debates as to what is the best way to defeat a terrorist network. Amongst these debates is the question, "how effective is leadership targeting"? Some theorists have suggested that eliminating the leader is effective only when engaging a small network. This argument suggests that larger networks have the ability and depth to promote within the network, making leadership targeting ineffective. Other scholars, such as John Arquilla, argue that "it takes a network to fight a network.".[44] Forming smaller specialized military units to combat a terrorist network is far more effective than fighting a network with a conventional force. This chapter will show how the French were able to combine the two theories of leadership targeting as well as using a network to fight a network to stop the National Liberation Front's (FLN) terrorist bombings during the Algerian Revolution from 1954–1962.

It is important to note that while the French lost the overall war in Algeria, they conducted several successful special operations aimed at countering the FLN. Out of the many French operations conducted during the Algerian War, their offensive strategy during the "Battle of Algiers," which aimed to disassemble the leadership of the Armée de Libération Nationale (ALN), was the best way to put an end to the terrorist attacks. The actions taken by the 10th Paratroop Division should be a learning tool for all future counterinsurgency operations aiming to tear down a network. The use of the Battle of Algiers as a model for counterinsurgency has been discouraged because of the 10th Paratrooper Division's use of torture. However, it is important to recognize that while the interrogation tactics used in the Battle of Algiers cannot (and should not) be followed, there are still valuable lessons learned from the French's operational objectives. The tactics they used by in this engagement are classic examples of how to conduct counterinsurgencies (COIN) today.[45]

---

44 John Arquilla, and David F. Ronfeldt. Networks and Netwars: The Future of Terror, Crime, and Militancy. Rand Corporation, 2001.

45 David Gulaula, Counter-insurgency Warfare, (New York: Frederick Praeger, 1964).

B. BACKGROUND

By 1954, France had controlled Algeria for over a century. France's governance of Algeria catered solely to European settlers. European cultural influence soon took over, destroying Algeria's social, cultural, linguistic, religious, and economic structures.[46] Under the French, Algerians lost 85 percent of their landholding and had no political influence. Algerian Muslims were denied the opportunity to hold political office by the French government; local Europeans held all the political positions even though Algerian Muslims made up the majority of the population. Algerians' desired to have the same rights as French citizens.[47] Instead they were treated as second class citizens. After several failed attempts to achieve unity through political elections, Algerian Muslims, totaling about nine million, began to have "no hope of attaining equality or freedom within the French Political system…."[48] Following this systematic oppression, the terrorist nucleus of the FLN formed and started a nationalist revolution to liberate Algeria.

In November 1954, the Algerian Revolution began with a wave of attacks across Algeria that aimed to remove the French government. French officials began counterinsurgency operations against FLN bases and, "what had begun as terrorist bombings and raids on isolated French farms by armed groups of the Algerian FLN, had turned into a bloody, no-quarter guerrilla war."[49] FLN members caused havoc amongst both French and Algerian citizens by placing bombs in public buildings, police stations, cafes, cinemas, and dance halls in Algiers and in other cities and towns.[50] Robert Lacoste, the minister of Algeria at the time, proved to be powerless in stopping the FLN from bombing the city of Algiers with his conventional forces. Conversely, FLN members were initially successful in their strategy of guerilla warfare, with FLN

46 Martha Crenshaw, Revolutionary Terrorism: The FLN in Algeria, 1954–1962 (Stanford: Hoover Institution Press, 1972): 2.

47 Martha Crenshaw, Revolutionary Terrorism, 6.

48 Martha Crenshaw, Revolutionary Terrorism, 6.

49 Howard Simpson, The Paratroopers of the French Foreign Legion: From Vietnam to Bosnia, (Washington: Brassey's, 1997): 16.

50 Howard Simpson, The Paratroopers of the French Foreign Legion: From Vietnam to Bosnia, 31.

operators mixed into the population, making them hard to find by the French army. In 1956, Lacoste called upon the help of the 10th Paratroop Division to restore power and order to the city of Algiers.[51] The launch of this counter, unconventional based campaign between the FLN and Paratroopers later became known as "Battle of Algiers."

C. FLN ORGANIZATION

The FLN was controlled by a five member committee called the Comite de coordination et d'Execution (CCE). In efforts to control the city of Algiers, the committee organized the city into Zone Autonome d'Alger (ZAA); the ZAA was divided into three regions and then broken down into sectors, subsectors, quarters, groups and cells. This structure formed a network designed to preserve anonymity and security. It was estimated that 750 to 1,000 militants were organized inside the ZAA.[52]

Algerian insurgency expert Martha Crenshaw argues that "The FLN organization was characterized by excessive local autonomy, collegial decision making, elaborate and complex clandestine networks."[53] All military activities inside the ZAA were under the leadership of Saadi Yacef. Yacef created a special sector as part of his network called Armée de Libération Nationale (ALN), or what he referred to as "reseau special bombes," in which he recruited students and technicians who were skilled in bomb making. The term reseau is a French word for network. Yacef's bomb network had a process, supervised by Ali la Pointe, which was strictly compartmentalized: laboratory work, transportation, storage, distribution and, finally, the placing of the bombs in chosen spots.[54] It was estimated that the ZAA possessed 150 bombs at the start of the "Battle of Algiers."

---

51 Matthew Connelly, A Diplomatic Revolution,(New York: Oxford University Press, 2002): 125.

52 Martha Crenshaw, Revolutionary Terrorism: The FLN in Algeria, 1954–1962 (Stanford: Hoover Institution Press, 1972): 10.

53 Martha Crenshaw, Revolutionary Terrorism, 12.

54 Martha Crenshaw, Revolutionary Terrorism, 10.

D. FRENCH DISMANTLING OF THE ALN BOMB SECTOR

Unable to control the insurgency through political means, France relied on military actions lead by General Massu. France's counterinsurgency plan was divided into an offensive strategy and a defensive strategy. Offensively, its objective was to disassemble the ALN's organization; defensively it aimed to protect the civilian population form terrorist attacks.[55]

The most notorious offensive clandestine operation was called la bleutie; headed by Captain Paul-Alain Leger, a counter-terrorism expert on the staff of the 10th Paratroop Division. Operation la bleutie took FLN activists and transformed them, primarily through the use of torture, into a network of agents under Leger's control. Some of these agents were sent back onto the streets of Algiers disguised as street sweepers and municipal workers to sabotage the FLN by creating distrust among its members. They mingled with FLN military units, planting incriminating forged documents and spreading false rumors of treachery.[56] This operation created disruption and confusion within the FLN, causing them to turn on each other.

Operation La bleutie's most valuable attribute was its ability to gather intelligence. Agents infiltrated the ALN network and discovered who the bosses were and their locations. This information became a key element in preventing ALN bombing attacks. Leger's first targets were Morad and Kamel, Yecef's chief bomb maker and his military deputy, respectively. Agents tipped off the Paratroopers that the two terrorists were in an apartment building in Impasse Saint-Vincent, and on August 26, the paratroopers raided the building in order to seize Mourad and Kamel. Capturing them alive was the number one priority because they might have information concerning Yacef's whereabouts. Kamel was shot, but paratroopers still succeeded in capturing him alive. Mourad, on the other hand, blew himself up by accidentally dropping a grenade

55 Martha Crenshaw, Revolutionary Terrorism: The FLN in Algeria, 1954–1962 (Stanford: Hoover Institution Press, 1972): 117.

56 France and the Algerian War 1962–63, ed. Martin Alexander, and J. F. V. Keiger, (London: Frank Cass, 2002): 7.

while trying to throw it at the paratroopers.[57] With Mourand and Kamel gone, the ALN was down to its top two leaders, Ali la Pointe and Yacef. One month after Kamel's capture, Leger's agents provided paratroopers with Yacef's location. A second raid captured Yacef, and once in custody, he gave up the location of Ali la Pointe, whose capture guaranteed the end of terrorist strikes committed by ALN members and effectively ending "The Battle Algiers."[58] Paratroopers lifted the city's curfew, schools were reopened and people were no longer afraid to fill shopping malls or go to the cinemas.

The actions taken by the 10th Paratroop Division should be a learning tool for all future counterterrorism operations aiming at tearing down a network. Alistair Horne, an Algerian historian and author of A Savage War of Peace: Algeria, illustrates the success Paratroopers had with their operational strategy of leadership targeting:

> No one could doubt that the paras had scored a major victory for the French army, the first clearly definable one of the war. They had faced up to a confrontation with the FLN and won hands down…he then quotes Massu saying "We had rounded up the leaders and broken up the system. There were no more assassination or bomb attempts."[59]

The paratroopers were successful in exposing ALN's network by forming their own clandestine network. Once they knew how the network functioned, they were able to diffuse it by eliminating the leaders. Leadership targeting did not help the French win the "big war," but it did successfully eliminate a terrorist cell inside Algeria. This is a military option that should be considered and available to all military leaders.

57 Alistair Horne, A Savage War of Peace, (New York: Viking Press, 1977): 212.

58 Alistair Horne, A Savage War of Peace, 212.

59 Alistair Horne, A Savage War of Peace, 218.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INDONESIA'S COUNTER-TERRORISM OPERATIONS

A. INTRODUCTION

Insurgents use terrorism as a strategy to achieve their political goals. Over the past two decades, we have seen a new form of terrorism spread dramatically. These insurgents have developed networks throughout the world composed of highly motivated individuals, and logistical support, to perform terrorist acts.[60] Through networks, insurgents have been able to gain funding, support and manpower to build explosives that cause devastation. Improvised Explosive Devices (IEDs) have become the weapon of choice for insurgents as well as the leading cause of death to service members deployed in Operation Iraqi Freedom and Operation Enduring Freedom.[61]

Networks that use IEDs have not only killed and terrorized the military, but civilians as well. A prime example is Noordin's network, a splinter group of Jemaah Islamiyah (JI), which terrorized Indonesia until its demise in 2009. Roberts and Everton believe that understanding the social network of an insurgency can provide an operational combat commander with a better understanding of the threat they face, which will result in better strategic decisions. They argue, "Understanding which strategic option to pursue and under what conditions remain more of an art than a science."[62] Both authors would agree, along with other social network analysis scholars, that there is no single option for defeating insurgencies. This theory has held true in Indonesia, where the Indonesians deciphered the structure of Noordin's network and understood that it would take more than leadership targeting to stop terrorist acts. Although Noordin Top's death, through leadership targeting, eventually lead to his network's demise, it did not solve the bigger problem of terrorist activities in Indonesia. The remnants of this network simply

60 Ioannis Michaletos,"The International Islamic Jihad: The first global terrorist movement in history," International Analyst Network (2010), http://www.analystnetwork.com/article.php?art_id=3446 (accessed February 04, 2011).

61 Yochi J. Dreazen, "IED Casualties Up Despite Increased Vigilance," National Journal (2011), http://www.nationaljournal.com/nationalsecurity/ied-casualties-up-despite-increased-vigilance-20110303 (accessed February 07, 2011).

62 Nancy Roberts and Sean Everton," Strategies for Combating Dark Networks," Journal of Social Structure, vol. 12, no. 2 (2012): 24.

evolved and took on a new face. Most of Noordin's key operators simply moved on and began operating with other terrorist cells. To stop the evolution of terrorist cells from reincarnating into new cells, Indonesia has worked to contain terrorism through rehabilitation and de-radicalization programs.

This chapter describes how Noordin created his network. It also shows the amount of information Indonesia was able to gather on Noordin's network and, yet, was still unable to defeat it through targeting the leadership alone. Next, it describes how Indonesia's Counter Terrorism (CT) success did not come from leadership targeting, but by working towards undermining the heart of the problem, the ideology that fed recruitment.

B. NOORDIN'S NETWORK

Noordin Mohammad Top, an explosive expert, was initially a member of Jemaah Islamiyah (JI). However, feeling that JI needed to do more, he left in 2006 to form his own splinter group, which he called Tanzim Qaedat al-Jihad, also known as Al-Qaeda in the Malay Archipelago.[63] While operating directly under JI, his network was responsible for the 2003 JW Marriot hotel bombing in Jakarta, the 2004 Australian embassy bombing in Jakarta, and the 2005 Bali bombing, the island's second major terrorist attack, which earned him a spot on the FBI's third major "most wanted list," in 2006.[64] These attacks made Noordin one of the most feared bomb makers in South East Asia and led to a conflict between Noordin and JI members because of high civilian casualties. Following the Bali bombing, an Indonesian task force began to crackdown on top JI members, and Noordin was forced to operate under his new cell, Tanzim Qaedat al-Jihad. Despite being well known by an Indonesian task force, which had infiltrated his network, Noordin was able to carry out the 2009 JW Marriot and Ritz-Carlton hotel bombings in Jakarta before being killed by Malaysian forces in 2009.

---

63 Jolene Jerard. "International Conference on Terrorist Rehabilitation (ICTR)." (Report on a conference organized by The International Centre of Political Violence and Terrorism Research (ICPVTR) Nanyang Technological University. Singapore, 2009). http://www.pvtr.org/pdf/Report/RSIS_ICTR_Report_2009.pdf. (Accessed March 09, 2011).

64 Jolene Jerard. "International Conference on Terrorist Rehabilitation (ICTR)," 35.

The success of Noordin's network can be attributed to the way in which he formed his network. He built a social network based on trust, which "networks consist of ramified interpersonal connections, consisting mainly of strong ties, within which people set valued, consequential, long-term resources and enterprises at risk to the malfeasance, mistakes, or failures of others."[65] Noordin relied heavily on people he knew through friendship, kinship, religious affiliation, and school affiliations.[66] In the bombings mentioned above, Noordin was able to recruit, gain financial backing, and evade police, all through the help of his social network. The ways in which Noordin used his network to execute the bombings in Jakarta in 2003 and 2004 are described below.

C. 2003 MARRIOTT BOMBING

Noordin's operational network for the 2003 Marriott Bombing consisted of nine members (see Table 2).[67] All of the members had strong ties linked together by personal relationships and through organizations that shared the same values, which gave each member a vested interest to see the operation succeed. In order for the bombing to be successful, each member had to depend on others to perform their roles. Azhari Husin, with the help of Noordin, planned the bombings. Asmar Latin Sani, who was the operation's suicide bomber, helped provide financial support along with Toni Togar, who robbed a bank in Medan to fund the operation. Ismail transported cash from Dunnai to Lampung, while Idris' job was to transport the explosives used in the operation which were stored at Siliwangi's house. Four of the members Noordin knew from school, and the others he knew through JI membership. Noordin often communicated through email by code to deliver instructions, but it was his personal relationships that generated trust amongst members and made this network strong.

65 Charles Tilly, Trust and Rule, (Cambridge University Press, 2005):12.

66 Nancy Roberts and Sean Everton," Strategies for Combating Dark Networks," Journal of Social Structure, vol 12, no. 2 (2011): 24.

67 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 4.

Name	Affiliation	Role
Noordin Moh. Top	School of Luqmanul Hakiem, JI member	Core of Network
Azhari Husin	School of Luqmanul Hakiem, JI member	Master Bomb Technician, Field Commander
Indrawarman alias Toni Togar	School of Ngruki, JI member	Raised funds for Bombing
Mohammed Rais	School of Luqmanul Hakiem, JI member, Noordins Brothern-law	Assisted Noordin with planning
Asmar Latin Sani	School of Ngruki, JI member	Facilitate financial transactions
Ismail alias Mohamed Ikhwan	School of Luqmanul Hakiem, JI member	Courier for Noordin
Sardona Siliwangi	School of Ngruki, JI member	House used to store explosives, Facilitated Financial transaction
Masrizal bin Ali alias Tohir	School of Luqmanul Hakiem, JI member	Surveyed targets, rented vehicles, and transported explosives
Mohamed Ihsan alias Idris	School of Ngruki, JI member	Explosive transporter

Table 2. Noordin's Marriot Bombers[68]

D. 2004 AUSTRALIAN EMBASSY BOMBING

After the 2003 Marriott hotel bombing, Noordin and Azhari attracted considerable police attention and were forced underground. While in hiding, Noordin depended heavily on his strong ties to help him evade the police. During this time, he pieced together a network similar to the one used in the 2003 Marriott Bombing that he would use in 2004 to bomb the Australian Embassy. He recruited his operational network from three sources: JI's East Java division, JI schools, and an old Darul Islam (DI) organization. This network, like the 2003 Marriott hotel bombing one, was based on trust and personal relations, but what made this network different was that he drew on the

68 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 4.

personal networks of others.[69] Similar to the 2003 Marriott Hotel bombing, the network was strong because members trusted each other and shared the same ideology and goals as Noordin (see Table 3).

Name	Affiliation	Role
Son Hadi	School of Ngruki, Darul Islam member, Associate of Fahim	Harbored Noordin & Azhari along with their lethal bomb making materials
Syaifuddin Umar alias Abu Fida	JI member East Java	Helped Noordin acquire bomb- material
Gempur Angkoro alias Jabir	School of Ngruki, JI member Central Java	Suicide bomb recruiter, Bomb maker
Bagus Budi Pranoto alias Urwah	JI member	Linked Noordin to Iwan Dharmawan
Lutfi Haidaroh alias Ubeid	School of Ngruki, JI member East Java	Courier for Noordin
Al-Anshori	School of Ngruki, JI member	Bomb-maker
Usman bin Sef	Head of JI wakalah East Java	Protected Noordin, Introduced Noordin to JI members
Iwan Dharmawan alias Rois	Ring Banten member	Field commander, connection to Darul Islam members

Table 3. Noordin's Australian Embassy Bombers[70]

From JI's East Java division, Noordin made contact with a fellow JI member, Fahim, who was head of JI's wakalah for East Java. Fahim provided both explosives and hiding. Fahim also made contact with one of his confidants, Son Hadi, in order to place Noordin and Azhari in hiding. After bouncing around from JI member to JI member, Son Hadi eventually placed Noordin with a business associate, Farouk, who was not a JI

69 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 5.

70 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 7.

member.[71] Noordin, who trusted Son Hadi because of his relationship with Fahim, now trusted Farouk because of Son Hadi's faith in him. Farouk then became a key person to the operations as he housed Noordin, along with his explosives.

Another non-JI member Noordin placed his trust in was a committed mujahidin by the name of Rois, who was tasked with setting up a training camp to select suicide bombers. From this camp Heri Golun was handpicked, and on September 9, 2004, he blew himself up in front of the Australian Embassy. Displaying how much trust Noordin had in his network, he made sure he met with every individual involved in the bombing, giving him a direct link to everyone.

E. INDONESIA'S CT OPERATIONS

Over the past decade, Indonesia has been devastated by numerous terrorist attacks. To date, Indonesia's approach to disrupting terrorist networks is believed by many to be the best counterterrorism strategy for combating terrorism. Instead of declaring war on terrorists, it treats terrorists as criminals by convicting them in courts. Indonesia takes this approach out of fear that military confrontation would only nurture further radicalization.[72] In 2003, the Indonesian government created Detachment 88, an antiterrorist police force, to uncover terrorist networks, hunt down and capture top militants.[73] This approach helped to decrease the terrorist threat, but Indonesia has learned that taking out key members and leaders is not enough to stop the network.

A popular CT theory suggests leadership targeting is an effective way to attack the network. While this approach has proven successful in some instances, it has not been the case for Indonesian officials. For example, from 2003–2009, Detachment 88 heavily pursued Noordin's splinter cell. Several members of Noordin's network were apprehended, but these arrests failed to eliminate the threat. For instance, in 2003 Mohammed Rais, who was Noordin's brother-in-law and helped in the early stages of the

71 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 7.

72 Hannah Beech, "What Indonesia Can Teach the World About Counterterrorism," Time, June 07, 2010 (accessed February 04, 2011).

73 Hannah Beech, "What Indonesia Can Teach the World About Counterterrorism."

Marriott bombing, was arrested in April prior to an August Marriot bombing. This did not deter Noordin, however; he simply replaced and carried out the attack.[74] Similarly, the arrest of JI leader Fahim, who provided Noordin with explosives and contacts to key contacts three months prior to the 2004 Embassy bombing, did little to stop the massacre from happening.[75] And in 2006 Detachment 88 successfully tracked and killed one of Noordin's partners, the master bomb maker, Dr. Azahari (he was responsible for making the bombs in the 2002–2005 attacks), but this did not stop future attacks, such as the 2009 JW Marriott and Ritz-Carlton bombings, from occurring.

Noordin's network was composed of members with the same salafi jihadist ideology, whom he trusted and pieced together from several organizations.[76] As Detachment 88 removed members of Noordin's network, a new member of Noordin's network stepped in to take his place. In other words, the terrorist organization was bigger than just one man; it was comprised of networks connected by an ideology. It was like other Jihadi groups, which do not disappear after waves of arrests; they evolve and mutate, taking on new form."[77] Noordin, himself, was just the face or "big ticket name" JI used to promote its cause.

After Noordin was killed in 2009, his splinter cell was soon replaced by another JI splinter cell headed by Dulmatin. Dulmatin became the new face of JI, and was used to recruit and terrorize. As predicted by research from Jordan and Crenshaw, removing top leaders did not put a stop to the terrorist network.[78] Terrorists, such as Urwah, Ubaid, and Toni Togar, who were formerly part of Noordin's network, joined Dumatin's network after Noordin's death, perpetuating the cycle.

---

74 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 4.

75 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 7.

76 International Crisis Group. (2006). Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114), (Brussels, Belgium: International Crisis Group): 19.

77 International Crisis Group (2010). Indonesia: Jihadi Surprise in Aceh, (No. Asia Report#189). (Brussels, Belgium: International Crisis Group): 15.

78 Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," Security Studies 18, no. 4 (2009): 745.

Anti-terrorism chief General Ansyaad Mbai, Indonesian official who coordinates their counter-terrorism policy, seems aware of this cycle and admits that killing the leader alone will not work.

> Today's terrorist leaders are the children, grandchildren, relatives or close associates of those executed in the past. As long as we do not neutralize their radical ideology, we will be unable to stop their movement.[79]

In efforts to "win the hearts and minds" of the radicals, the Indonesian government he adopted de-radicalization programs to counter the spread of these ideologies.[80] One government program provides prisoners who cooperate with better medical care and pay for their children's education. Another allows convicted terrorists to participate in community outreach programs. Detachment 88 also provides spiritual counselors who attempt to persuade militants that the teachings they hold are incorrect.[81] The Indonesian government's de-radicalization effort "has resulted in the development of an argument within the terrorist network that bombing served no purpose, failed to rally people to support their cause and was indeed counterproductive."[82] Sidney Jones, an anti-terrorism analyst, says "improvements in the social and political conditions in the country have made it harder for terrorist recruitment."[83] Jones acknowledges that Indonesia's threat of terrorism remains, but their policy to fight terrorism has begun to contain the problem.[84]

---

79 Warren P. Strobel, "Indonesia fights terrorism with power of persuasion," Mc Clatchy Newpapapers, October 22, 2008, http://www.mcclatchydc.com/2008/10/22/54612/indonesia-fights-terrorism-with.html (accessed February 05, 2011).

80 Bahtiar Effemdy, "Combating terrorism in Indonesia: Where are we now exactly," The Jarkarta Post, July 21, 2008, http://www.thejakartapost.com/news/2008/07/21/combating-terrorism-indonesia-where-are-we-now-exactly.html (accessed March 08, 2011).

81 Warren P. Strobel, "Indonesia fights terrorism with power of persuasion."

82 Bahtiar Effemdy, "Combating terrorism in Indonesia."

83 Brain Padden, "Indonesia Uses "Soft Approach" to Contain Terrorist Threat," Voice of America, January 18, 2010, http://www.voanews.com/english/news/asia/Indonesia-Uses-Soft-Approach-to-Contain-Terrorist-Threat-81960552.html (accessed March 05, 2011).

84 Brain Padden, "Indonesia Uses "Soft Approach" to Contain Terrorist Threat," Voice of America, January 18, 2010, http://www.voanews.com/english/news/asia/Indonesia-Uses-Soft-Approach-to-Contain-Terrorist-Threat-81960552.html (accessed March 05, 2011).

Indonesia's CT strategy is an operation the world can learn from. Their success is credited to their understanding of the terrorist network, which enabled them to carry out simultaneous applications of both a hard and soft approach. In particular, applying the soft approach, through the use of government programs, helped officials gain the cooperation of some former terrorists, such as Nasir Abbas and Ali Imron, which helped them gain an understanding of the kinship, friendship, and religious motives that foster terrorist networks in Indonesia. As in the case of Noordin's network, these factors have become the basis for the Indonesian police to build a systematic approach in dealing with terrorists.[85]

[85]"International Conference on Terrorist Rehabilitation (ICTR)," 36.

THIS PAGE INTENTIONALLY LEFT BLANK

V. OPERATION YARBOROUGH

A. INTRODUCTION

In 2003, the U.S. government spearheaded an invasion against Iraq with the aim of deposing Saddam Hussein and capturing the country's alleged Weapons of Mass Destruction. The U.S. military and Coalition forces succeeded in toppling Saddam's regime in a matter of days, but the smooth transition to a more representative, if not likeable, government did not occur. Instead, Iraq became a country teetering on the edge of collapse, vacillating between an insurgency and a civil war.

The following chapter will briefly cover the rise to power of Muqtada al-Sadr, the charismatic Shia cleric responsible for some of the attacks on coalition forces via his Jaysh al-Mahdi (JAM) militia. The 2003 break in the Sadrist movement, caused by a disagreement between Muqtada al-Sadr and his right hand man Qais Khazali, led to the creation of Shia Special Groups, which also fought coalition forces.[86] This chapter focuses on Operation Yarborough, executed in 2005, and the disruption of Shia insurgent operations in the south by a small "networked" group of U.S. Soldiers, which provides a unique perspective on how to successfully execute attack the network operations.

B. BACKGROUND

The al-Sadr family lineage has produced great Shia leaders who have lived and died in support of social, political and religious rights for Shia in Iraq. Grand Ayatollah Mohammed Baqir al-Sadr, cousin to Ayatollah Mohammed Sadeq al-Sadr and Muqtada al-Sadr's father-in-law, was a renowned Shia scholar who instilled Shia Nationalism in his followers.[87] He was the founder of the Dawa party, a political movement that currently controls the majority block of the government in Iraq, and he effectively

86 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, Institute for the Study of War, Washington, DC, 2009, 8.

87 Vali Nasr, The Shia Revival, 86.

mobilized Shia youth though his rhetoric and writing. His ability to mobilize the Shia brought unwanted attention from the Baathist Regime, eventually leading to his brutal murder in 1980.[88]

Ayatollah Mohammed Sadeq al-Sadr, Muqtada's father, was one of several leaders sought out by Saddam Hussein's regime in an attempt to settle Shia hostilities following the failed Shia uprising after the 1991 Persian Gulf War.[89] Sadeq established schools and mosques, particularly in the impoverished Baghdad neighborhood of Sadr city, issued a fatwa that reinvigorated Friday prayers for the Shia, which had been banned by the ruling Baathist regime, and effectively networked and gained mass appeal.[90] Through all of this, Sadeq emerged as a great leader of the oppressed Shia that possessed an innate ability to motivate his followers through his powerful rhetoric. The breaking point between Sadeq and Saddam's regime came in 1999, when Sadeq al-Sadr demanded the release of scholars and clergy still imprisoned for the 1991 uprising, a call that mobilized tens-of-thousands in protest. For this, he and two of his sons were gunned down less than a week later.[91]

Muqtada al-Sadr, Sadeq al-Sadr's only surviving son, was unable to direct the Sadrist movement following the death of his father because he was under house arrest. It is doubtful that even if he were a free man at the time of his father's death he would have garnered the necessary support because of his youth, lack of clerical status, and personal demeanor.[92]

Thus, in the wake of Sadeq al-Sadr's death, Sadeq al-Sadr's students ran the Sadrist movement. With the outbreak of the Iraq War in 2003, however, Muqtada emerged as one of several leaders of the Shia. Part of Muqtada's appeal was his name; he was a Sadr after all and referenced by the title "Sayyid," which denotes a direct

88 Vali Nasr, The Shia Revival, 187.

89 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 8.

90 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 10.

91 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 9–10.

92 He is reported to suffer from bipolar disorder Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadist Movement, 11.

descendant of the Prophet Mohammed. He also profited from the support of the Sadrist movement, which his father founded, via its networks and organization. Perhaps most important, the Ayatollah Kazem al-Haeri, a prestigious Iranian cleric in Qom Iran, appointed Muqtada his deputy and representative in Iraq. [93] With al-Haeri's direction, Muqtada al-Sadr immediately went on the offensive rhetorically and through the activation of the Jaysh al-Mahdi (JAM), a militia created to safeguard the Iraqi Shia. With a militia in place and a means to provide social services to the poorer segments of the Shia in Baghdad, Muqtada sought to form the Sadrist movement into a Hezbollah like organization that would control various ministerial offices and seats in Parliament.[94] Muqtada al-Sadr's more immediate focus, however, seemed to be the removal of U.S. and Coalition Forces from Iraq, which his Shia followers viewed as unwanted occupiers.

In 2004 JAM, under the direction of Muqtada, launched an offensive against Coalition Forces, which lasted for two months and resulted in serious losses for Sadr led JAM in terms of both men and credibility. Then in the beginning of 2005, a split emerged between Muqtada al-Sadr, who wanted to join in the Iraqi government, and those that insisted on maintaining a more militant stance, including Qais Khazali, a student of Sadeq al-Sadr and Muqtada's official spokesperson.[95] Qais Khazali eventually formed the Asaib Ahl al-Haq (AAH or League of the Righteous), which was trained by the Iranian Revolutionary Guard Corps—Qods Force (IRGC-QF).[96] The League of the Righteous along with other splinter Special Groups (SG) became masters of IEDs, small arm attacks, and the emplacement of explosively formed penetrators (EFPs).[97]

In early 2007, Muqtada al-Sadr declared a cease fire, deactivated JAM, and moved to Iran; however, his departure did nothing to stem the flow attacks by radicalized JAM members that wanted to continue in armed resistance and SGs actively targeting

93 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 11.

94 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 13.

95 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 15.

96 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 19.

97 Marisa Cochrane, Iraq Report 12: The Fragmentation of the Sadrist Movement, 6.

Coalition Forces across southern Iraq.[98] In April 2007, the British Military forces returned responsibility of Maysan Province, a Shia stronghold, to Iraqi forces. [99] Following the transition of authority, JAM-SG personnel operated without fear of consequence in the southern Province of Maysan and completely controlled the city of al Amarah.[100] Each of the organizations, radicalized remnants of JAM as well as various SG, represented separate entities but retained underlying linkages that produced a formidable network.

C. IT TAKES A NETWORK[101]

In order to combat the rising threat posed by Shia SGs, the U.S. military placed multiple Special Forces (SF) Operation Detachments Alpha (ODA) in the south. An ODA is a twelve man element designed to plan and conduct unilateral operations and function in remote and hostile environment for extended time with minimum external direction. SF ODAs also develop, organize, equip, train, and advise up to a battalion sized irregular indigenous force as well as train, advise, and assist multi-national forces and agencies.[102] In order to perform these tasks, an ODA must leverage reach-back capabilities provided by a larger military element, typically a SF Battalion located on an operational base, against the needs of the indigenous forces it is advising. An ODA, therefore, tends to function as part of a larger hierarchal organization when in garrison, and operate as a distributed and highly adaptable semi-autonomous unit when deployed in an advisory capacity. They act as the local bridge, or linking mechanism, between the larger forces and local forces during Major Combat Operations.[103]

---

98 Michael Harari, "Status Update: Shia Militias in Iraq," Institute for the Study of War (2010): 4, accessed March 18, 2011, http://www.understandingwar.org/files/Backgrounder_ShiaMilitias.pdf.

99 Duane Mosier, "The Road to Al Amarah," Small Wars Journal, November 2010: 5, accessed November 9, 2010, http://smallwarsjournal.com/blog/journal/docs-temp/593-mosier.pdf.

100 Duane Mosier, "The Road to Al Amarah," 6.

101 John Arquilla and David F. Ronfeldt, Swarming and the Future of Conflict (RAND Corporation, 2000): 22.

102 HQ, Department of the Army, Army Special Operation Forces Unconventional Warfare: FMI 3-05.130, 2008: 4–13.

103 David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010, 46. FM 3-05-130, 5–6.

In late 2007 and into early 2008, the U.S. military rotated approximately nine ODAs through southern Iraq to train and advise the Iraqi military.[104] Networked to a larger Army SF Battalion contingency, the twelve-man ODAs were also dispersed to facilitate Iraqi Security Forces (ISF) in quelling the violence and stabilizing the region. One of those teams was ODA 5331. ODA 5331 partnered with the city of an-Nasiriyah and the regionally based Iraqi Special Weapons and Tactics (ISWAT) Team for support in security operations[105]

On January 18, 2008, a fight broke out in an-Nasiriyah between the Iraqi police and a SG. In the first fifteen minutes of fighting, the SG had killed four of five Iraqi police commanders and severely wounded the fifth with headshots from snipers; the ISWAT commander was one of these casualties.[106] Upon request from the ISWAT deputy commander, ODA 5331 supplied necessary assistance in triage efforts, coordinating and consolidating the reorganization of the remaining troops, and reestablishing the command and control element. More importantly, ODA 5331 ensured accurate close air support to prevent collateral damage to the densely populated city.[107] This conscious effort to limit collateral damage paid off in two important ways; first, it reduced the threat of backlash from the population and, second, the limited air strikes proved the Iraqi troops could fight an extended engagement with minimal support and win.

The following day, ODA 5331, the remaining Iraqi Security leaders, and Major General Habib, the 10th Iraqi Army division commander, met to discuss the battle. The meeting produced a combined Army and police offensive aimed at quieting the violence in the city. The joint effort succeeded in establishing security by the afternoon and an important friendship began between Maj Gen Habib and ODA 5331.[108]

---

104 HQ, Department of the Army, Army Special Operation Forces: FM 3-05 (FM 100-25), 2006: 3–4. Duane Mosier, "The Road to Al Amarah," 1.

105 Duane Mosier, "The Road to Al Amarah," 1.

106 Duane Mosier, "The Road to Al Amarah," 4.

107 Duane Mosier, "The Road to Al Amarah," 5.

108 Duane Mosier, "The Road to Al Amarah," 6.

By February 2008, Maj Gen Habib and ODA 5331 were involved in planning Operation Yarborough, which aimed to drive JAM and related SG out of al Amarah. The plan was to conduct a disruption campaign that would incorporate tactical checkpoints, raids, deception operations, psychological operation leaflet drops and a whisper messaging campaign in order to apply constant pressure to JAM-SG personnel.[109]

Operation Yarborough started with hellfire missile eliminated insurgents who were setting an IED in the vicinity of a future tactical checkpoint. This attack was followed by a direct action raid, utilizing combined U.S. and Iraqi forces, designed primarily to achieve psychological effects. Joint efforts delivered two messages; the first, non-verbal, was that Iraqi forces would no longer allow JAM-SG to operate with impunity and the second, verbal, was that JAM-SG no longer had a safe haven in al-Amarah. This message campaign was followed by a tactical checkpoint that further emphasized the omnipotence of the government of Iraqi (GoI). Within days of these actions the affects were seen as the local population was already supporting GoI by stating at checkpoints they wanted the JAM criminals removed, and intelligence verified JAM's confusion and nervousness generated by the raid.[110]

The Joint U.S.-Iraqi team maintained constant pressure on JAM-SG between the checkpoints, leaflet drops, zero collateral damage bombings, and ongoing deception. In addition U.S. and Iraqi forces conducted targeted raids that spread the word that the insurgents would no longer be tolerated. The combinations of earlier JAM-SG clearance operations by networked ODA teams in cities like Basra funneled fleeing fighters into al-Amarah where Operation Yarborough continued the relentless pressure.[111] This pressure compelled the leadership to flee into Iran, leaving lower level members to plan operations, which they did ineffectively. The counter network operations proved so decisive that Brigadier General Qassem Suleimani, Commander IRGC-QF, helped assist

109 Duane Mosier, "The Road to Al Amarah," 11.

110 Duane Mosier, "The Road to Al Amarah," 13.

111 Marisa Cochrane, Iraq Report: Special Groups Regenerate, Institute for the Study of War, Washington, DC, 2008, 18.

in the negotiated ceasefire between GoI and the beleaguered militias.[112] This involvement of high-ranking Iranian in Iraqi peace negotiations further revealed the level of control the government of Iran had over the security situation in the province.

In the end, the twelve-man networked ODA's positive results were highly effective in defeating the combined opposing network. In developing targeting packages and focusing tactical operations they garnered an operational victory.

D. CONCLUSION

As mentioned in Chapter II, the application of SNA and its associated terms is more of an art than an exact science. In the real world, human interaction is not easily placed into specific categories. It is for this reason that both the ODA and the elements of JAM and the SG's can be flatter and more distributed units in an operational setting and still be networked into the larger hierarchal organization. Whether an organization is distributed or hierarchical, it is the ability to bridge the units together that effectively networks these organizations together. This concept is also visible in Indonesia's Detachment 88 battle against Noordin's network, described in Chapter IV, and Chapter III's description of the French SAS battle against the Algerian FLN.

In successfully attacking and disrupting the JAM-SG, ODA 5331 showed how understanding the context of a network not only provides multiple avenues for attack, but allows for effective tactics that can be employed according to the known situation. With reach back capability to confirm the context of targeted individuals, ODA 5331 maximized the output of their twelve-man element. The constant and directed pressure applied in Operation Yarborough debilitated the JAM-SG network and forced leaders into hiding in Iran.[113] Additionally, attention to detail, such as the close control of air support, gained the trust and favor of the local population. Operation Yarborough also helped to build the capacity and competency of Iraqi forces in defeating these insurgents.

112 Michael Harari, "Status Update: Shia Militias in Iraq," 1.

113 Marisa Cochrane, "Special Groups Regenerate," 23.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. A WAR OF CONTEXT

Command and Control Warfare (C2W), the unity of command that ties together all the operational functions and tasks, is considered one of the U.S. Military's greatest strengths.[114] In reaction to the post-September 11 security environment and the wars the United States is now fighting, there has been a shift in the organizational design of the U.S. military, including the structure of troops and requirements for specific skill sets. Gone are the "good old days" when war was against a clearly defined, dogmatically hierarchal military of another state. Present day adversaries are now mostly distributed and highly adaptable sub-state organizations. Terrorist network expert John Arquilla addresses this issue in his "Conflict in the Information Age" seminar, held at the Naval Postgraduate School. He advances the idea that, since there has been a shift in organizational design of our forces, then why should we not shift the term C2W to command and "something else?"[115] He then invites his class to fill in the blank. This sort of exercise could be just the right idea set to help the U.S. military to maintain its classical dominance in command and control. Instead of being bogged down by a term that was designed for a conventional fight, a new term could emerge that accurately depicts the types of conflicts in which the U.S. military is currently involved.

The intention of this thesis has been to fill in the blank of Arquilla's exercise with the word "context"—this is a fight to understand context. In other words, in order to defeat our adversaries, it is necessary to have an understanding of their background, structure, and how they relate to society and their peer group. Adopting this concept would encourage the military to reevaluate and redefine tactics, techniques, and procedures and this, in turn, would have a positive effect in reshaping doctrine to resemble the fight we are in as opposed to the fight we want. The change would also

[114] Command and control (C2) is the means by which a joint force commander (JFC) synchronizes and/or integrates joint force activities in order to achieve unity of command. C2 ties together all the operational functions and tasks, and applies to all levels of war and echelons of command across the range of military operations. Joint Publication 1: Doctrine for the Armed Forces of the United States, (20 March 2009): 18.

[115] The lecture discussion is based on the assigned reading: Martin Libicki's, *What is Information Warfare (NDU, 1995).*

provide the opportunity to stop "putting the square peg in the round hole," by introducing new concepts that would help inform new decision matrices.

The manufacture and proper placement of IEDs requires advanced skill and access to proper materials. This is what makes fighting the "War of Context" so vital in IED attack the network operations. Understanding the networks that provide training, financial backing, as well as motivation is not only essential to the infiltration of a network but is the key to uncovering the root of the problem and the associated linkages.

A. WHICH WAY TO THE FUTURE?

It is important for the military to continue to move forward and not stagnate. As humans, we are creatures of habit, and a habit deeply ingrained in military culture includes assumptions about how an organization must operate to survive "first contact." In the current environment, the U.S. military is not facing masses of troops aligned under a hierarchal organization. Today's reality is that the major adversary is a distributed organization that despises the west and the ideas of modernity, yet uses the internet and other tools of modernity on par with any "modern" society to attack and advance its goals. The enemy understands how to get their message out and, at least for now, can effectively execute their planned operations by providing guidance rather than orders.

A focused SNA approach would provide the framework to build and sustain knowledge of dark networks across time and unit rotations. At the operational level, SNA could provide the context that would then allow a commander to maximize the use of his resources. This economical use of force, as highlighted in the case studies, focuses limited yet technologically based assets to targeting nodes determined to be critical links of an organization. However, targeting critical nodes is not the only way to dismantle a dark network. SNA provides a strong framework for creating context, but is only one tool in a larger tool box at the commander's disposal.

SNA is not a new idea to counterinsurgency manuals, FM 3-24 appendix B, for example, addresses SNA.[116] FM 3-24's overview, however, does not provide a focused analysis for the time constrained operational commander. Chapters I and II of this thesis focused on providing an analytical tool for commanders who seek to understand the organizational structure of irregular armed forces. Chapter I did this through defining weak links. Weak links, or acquaintances, are the conduits that support the rapid diffusion of information and logistics across social clusters. Weak links, in other words, are the path of least resistance for the free flow of money and information. Attacking these links, therefore, has a great effect on disrupting the larger network's activities.

Chapter II, provided definitions for overall network types followed by an analysis of a few fundamental SNA concepts, specifically measures of centrality. These macro and micro measures were then placed into a matrix in order to provide a visual tool to assist in analysis of possible lines of operation, target selection, and combinations of the two. By advancing a limited set of ideas these chapters provide a focused look at SNA, so that the operational commander and his staff can rapidly assess individual group dynamics without thorough training in sociology or psychology.

Ultimately, in order for U.S. forces to "attack the network" and reduce their ability to use IEDs, they need to first understand the dark network and the context in which it functions.[117] IEDs provide a dark network an inexpensive, easy to manufacture, and force multiplying tactic against a superior force. The strategic influence of IEDs is a direct result of its lethality and the visceral reaction its victims and viewers experience.[118] In order for U.S. strategy to be successful it needs to go beyond the weapon and address the issues that caused the mobilization of the insurgency or a terrorist's organization. This is the War of Context.

---

116 HQ, Department of the Army, Counterinsurgency: FM 3-24 (MCWP3-33.5), 2006: B12–14.

117 Bruce Hoffman and Gordon McCormick, "Terrorism, Signaling, and Suicide Attack," Studies in Conflict & Terrorism 27, no. 4 (July 2004): 245.

118 J. K. Martin, Dragon's Claws: The Improvised Explosive Device (IED) as a Weapon of Strategic Influence. Naval Postgraduate School Monterey CA, 2009, 4.

The objective of the case study section was to look at three random cases where a formal government showed some form of success when combating an insurgency or terrorist organization, whose strategic approach focused on the use of IEDs. A common trait, in each of the three cases, was that the State actors understood "The War of Context." The French had a great understanding of the FLN's ideology and their way of thinking in Algeria, which allowed them to a get inside the terrorist organization to illuminate and expose key leaders in the network. Because of their understanding, the French knew how to create disruption between ALN members and originate false documents that would raise distrust in the organization. It was in knowing their oppositions' way of thinking and "who's who" that lead to the dismantling of the ALN. The French achieved an operational victory in defeating the FLN's bomb ALN network but, ultimately, other methods used such as torture, for example, caused a strategic failure. Not understanding the "big picture" and how their actions affected the people of Algeria, they could not stop the FLN from gaining supporters and lost the overall "big war". The French operation provides a unique example of how the understanding of war being fought affects, both positively and negatively, the strategic aims of a nation.

As in the Algerian case study, the same principles hold true in the disruptions of Noordin's network. The Indonesians set out to understand their opponents. Detachment 88's success came from their ability to discover the links and nodes between Noordin and his affiliates. Through careful preparation, Detachment 88 was able to track and assassinate Noordin, thus bringing an end to his network. With proper context, operational, commanders are able to develop lines of operation to attack and disrupt enemy networks.

As in any other terrorists' organization or oppressed society, a new leader or uprising can form because there has not been change in the local environment. Although Indonesia knew they could not stop new groups from forming, they saw the "big picture" and created a governmental de-radicalizations program changing the mind set of terrorists. Instead declaring a war on terrorism or banning JI members, Indonesia decided

to attack the ideologies that made terrorist violent. By educating terrorist on the fallacies within their beliefs and allowing them to express their religious beliefs, Indonesia is able to contain violent acts of terrorism.

In Iraq, ODA 5331 repeated the logic of understanding the enemy and attacking via multiple lines of operation. ODA 5331 proved this concept as they applied aspects of deception, psychological manipulation, and node targeting against the information they had on the composition of the enemy's network. The constant and directed pressure applied in Operation Yarborough debilitated the JAM-SG network. By successfully securing al-Amarah ODA 5331 helped to build the capacity and competency of Iraqi forces in defeating the Shia insurgents.

Just as defeating IEDs at the operational and tactical level require going beyond the weapon, a Strategy of Context must involve the interagency powers inherent in the Department of State and the Department of Defense in order to defeat the wider context in which these networks emerged.[119] This wider Strategy of Context focuses on the structure of the state. The Strategy of Context can then be expected to revolve around two major points; the definition of what constitutes a state and how much time will be allotted to resolve this dilemma. Charles Tilly, Ghani et al. and Robert Rotberg are only a few of the scholars that have provided a structure that defines a functional nation-state, yet complete agreement amongst these lists does not exist.[120] Security of the included citizenry seems to rank high with each, yet the differences highlight the lack of consensus within academia on what constitutes a state. The challenge, for the political-military professionals, then becomes what criteria are applicable, which aspects matter and how to maximize assets to fix or re-build the State.

---

[119] Martha Crenshaw, "How Terrorism Declines," *Terrorism and Political Violence* 3, no. 1 (1991): 69. A. K. Cronin, "How al-Qaida Ends: The Decline and Demise of Terrorist Groups," *International Security* 31, no. 1 (2006): 7–48. Crenshaw and Cronin have both written extensively on terror organizations. The two citations are recommended for a deeper look at ending terror networks.

[120] Charles Tilly, *The Formation of National States in Western Europe*, (Princeton University Press, 1975), 27. A. Ghani, C. Lockhart, and M. Carnahan, "Closing the Sovereignty Gap: An Approach to State-Building," *Overseas Development Institute* (London: 2005), 6. Robert I. Rotberg, "Strengthening Governance: Ranking Countries Would Help." *The Washington Quarterly* 28, no. 1 (2004): 71–81.

Secondly, and arguably equally if not more important, is the expectation and value of time. This is the time that it takes the U.S. governmental bureaucracy to analyze a situation and organize a response to terrorist and insurgent behavior.[121] The time citizens of the U.S. will allow the military to remain in a country as well as the amount of time an indigenous population will accept a large U.S. presence. Time, also, allows a terror organization or insurgency to build its message as well as its base and become a self-sustaining force.[122]

The conundrum posed by the composition of the state and time to solve this problem are clearly not just problems for the military, therefore, it requires more than the military to fix. Short of a combined Strategy of Context, that harnesses the power of the interagency, the war will not be won and the U.S. military will need to remain or return to the same areas until these underlying issues are resolved.

121 Martha Crenshaw, "How Terrorism Declines," 86.

122 Martha Crenshaw, "How Terrorism Declines," 79.

LIST OF REFERENCES

Alexander, Martin S. and John F. V. Keiger. *France and the Algerian War, 1954–62: Strategy, Operations and Diplomacy*. London; Portland, OR: Frank Cass Publishers, 2002.

Arquilla, John, and David F. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand Corporation, 2001.

———. *Swarming and the Future of Conflict*. RAND Corporation, 2000.

Beech, Hannah. "What Indonesia Can Teach the World about Counterterrorism." *Time*, June 7, 2010. http://www.time.com/time/magazine/article/0,9171,1992246,00.html. (assessed February 7, 2011).

Carley, Kathleen M, Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections* 24, no. 3, 2001.

Carley, Kathleen M, Matthew Dombroski, Max Tsvetovat, Jeffrey Reminga, and Natasha Kamneva. "Destabilizing Dynamic Covert Networks." In proceedings of the 8th international Command and Control Research and Technology Symposium, Pittsburg, Pennsylvania, 2003.

Cochrane, Marisa. *Iraq Report 12: The Fragmentation of the Sadrist Movement.* Institute for the Study of War. Washington, DC. 2009.

———. *Iraq Report: Special Groups Regenerate.* Institute for the Study of War. Washington, DC. 2008.

Connelly, Matthew James. *A Diplomatic Revolution: Algeria's Fight for Independence and the Origins of the Post-Cold War Era*. Oxford; New York: Oxford University Press, 2002.

Crenshaw, Martha. "How Terrorism Declines." *Terrorism and Political Violence* 3, no. 1, 1991.

———. *Revolutionary Terrorism: The FLN in Algeria, 1954–1962*. Hoover Institution Publication; 196. Stanford, CA: Hoover Institution Press: 1978.

Cronin, Audrey K. "How al-Qaida Ends: The Decline and Demise of Terrorist Groups." *International Security* 31, no. 1, 2006.

Daft, Richard L. *Essentials of Organization Theory and Design*. Mason, OH. 2003.

Dodds, Peter S., Roby Muhamad, and Duncan J. Watts. "An Experimental Study of Search in Global Social Networks." *Science*, 2003.

Dreazen, Yochi J. "IED Casulaties Up Despite Increase Vigilance." National Journal March 3, 2011. http://mobile.nationaljournal.com/nationalsecurity/ied-casualties-up-despite-increased-vigilance-20110303 (accessed March 3, 2011).

Easley, David, and Jon Kleinberg. *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*. Cambridge University Press, 2010.

Effendy, Bahtiar. "Combating terrorism in Indonesia: Where are we now exactly." The *Jarkarta Post*, July 21, 2008. http://www.thejakartapost.com/news/2008/07/21/combating-terrorism-indonesia-where-are-we-now-exactly.html. (accessed March 08, 2011)

Freeman, Linton C. "Computer Programs in Social Network Analysis." *Connections* 11, no. 2 (1988): 26–31.

———. *The Development of Social Network Analysis: A Study in the Sociology of Science*. Empirical Press, 2004.

Ghani, Ashraf, Clare Lockhart, and Michael Carnahan. "Closing the Sovereignty Gap: An Approach to State-Building." *Overseas Development Institute.* London: 2005.

Granovetter, Mark S. "The Strength of Weak Ties." *American Journal of Sociology* 78, no. 6, 1973.

Gulaula, David. *Counter-insurgency Warfare*, New York: Frederick Praeger, 1964.

Harari, Michael. "Status Update: Shia Militias in Iraq." Institute for the Study of War (2010): 10. http://www.understandingwar.org/files/Backgrounder_ShiaMilitias.pdf. (accessed March 18, 2011).

Hart, Basil H. Liddell. *Strategy: Second Revised Edition*. 2nd ed. Plume. 1991.

Hoffman, Bruce, and Gordon McCormick. "Terrorism, Signaling, and Suicide Attack." *Studies in Conflict & Terrorism* 27, no. 4, July 2004.

Horne, Alistair. *A Savage War of Peace: Algeria, 1954–1962*. New York: Viking Press, 1978; 1977.

HQ, Department of the Army. *Army Special Operation Forces: FM 3-05 (FM 100-25).* 2006.

———. *Army Special Operation Forces: Unconventional Warfare: FM 3-05.130*. 2008.

———. *Counterinsurgency: FM 3-24 (MCWP 3-33.5). 2*006.

International Crisis Group. Indonesia: Jihadi Surprise in Aceh (No. Asia Report#189). Brussels, Belgium: International Crisis Group, 2010.

International Crisis Group. Terrorism in Indonesia: Noordin's Networks (No. Asia Report#114). Brussels, Belgium: International Crisis Group, 2006.

Jerard, Jolene. "International Conference on Terrorist Rehabilitation (ICTR)." Report on a conference organized by The International Centre of Political Violence and Terrorism Research (ICPVTR). Nanyang Technological University. Singapore, 2009. http://www.pvtr.org/pdf/Report/RSIS_ICTR_Report_2009.pdf (accessed March 09, 2011).

Joint Publication 1: Doctrine for the Armed Forces of the United States. 20 March 2009.

Jordan, Jenna. "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation." *Security Studies* 18, no. 4, 2009.

Krebs, Valdis E. "Mapping Networks of Terrorist Cells." *Connections* 24, no. 3, 2002)

Martin, J. K. *Dragon's Claws: The Improvised Explosive Device (IED) as a Weapon of Strategic Influence*. Naval Postgraduate School Monterey CA, 2009.

McCormick, Gordan H. and Frank Giordano. "Things Come Together: Symbolic Violence and Guerrilla Mobilisation." *Third World Quarterly* 28, no. 2, January 1, 2007.

Michaletos, Ioannis. "The International Islamic Jihad: The first global terrorist movement in history." International Analyst Network, April 29, 2010. http://www.analyst-network.com/article.php?art_id=3446. (accessed February 04, 2011).

Mosier, Duane. "The Road to Al Amarah." Small Wars Journal (November 2010): 20. http://smallwarsjournal.com/blog/journal/docs-temp/593-mosier.pdf. (accessed November 9, 2010).

Nasr, Vali. *The Shia Revival: How Conflicts within Islam Will Shape the Future*. 1st ed. W. W. Norton, 2006.

Onnela, Jukka-Pekka, Jari Saramäki, Jaakko Hyvönen, Gyorgy Szabó, David Lazer, Kimmo Kaski, János Kertész, and Albert-Lásló Barabási. "Structure and Tie Strengths in Mobile Communication Networks." *Proceedings of the National Academy of Sciences of the United States of America* 104, no. 18, May 1, 2007.

Padden, Brian. “Indonesia Uses “Soft Approach” to Contain Terrorist Threat.” Voice of America, January 18, 2010. http://www.voanews.com/english/news/asia/Indonesia-Uses-Soft-Approach-to-Contain-Terrorist-Threat-81960552.html. (accessed March 05, 2011).

Roberts, Nancy, and Sean F. Everton. “Strategies for combating dark networks.” *Journal of Social Structure* Vol 12. No 2. 2011.

Rodríguez, José A. “The March 11th Terrorist Network: In its Weakness Lies its Strength.” Working Papers EPP-LEA, 2005.

Rogers, Everett M. *Diffusion of Innovations, 5th Edition*. Original. Free Press, 2003.

Simpson, Howard R. *The Paratroopers of the French Foreign Legion: From Vietnam to Bosnia*. Washington, DC: Brassey's, 1997.

Rotberg, Robert I. “Strengthening Governance: Ranking Countries Would Help.” *The Washington Quarterly* 28, no. 1, 2004.

Strobel, Warren P, “Indonesia fights terrorism with power of persuasion.” Mc Clatchy Newpapapers, October 22, 2008, http://www.mcclatchydc.com/2008/10/22/54612/indonesia-fights-terrorism-with.html. (accessed February 05, 2011).

Tilly, Charles. *The Formation of National States in Western Europe*. Princeton University Press, 1975.

Travers, Jeffrey, and Stanley Milgram. “An Experimental Study of the Small World Problem.” *Sociometry* 32, no. 4, December 1, 1969.

Wasserman, Stanley, and Katherine Faust. *Social Network Analysis: Methods and Applications*, 1st Edition. Cambridge University Press, 1994.

Watts, Duncan J. "Networks, Dynamics, and the Small-World Phenomenon." *American Journal of Sociology*, 1999 105:493–527.

———. *Six Degrees: The Science of a Connected Age*. New York: W. W. Norton & Company, 2003.

———. *Small Worlds: The Dynamics of Networks Between Order and Randomness*. Princeton, NJ: Princeton University Press, 1999.

Wellman, Barry, Peter J. Carrington, and Alan Hall. “Networks as Personal Communities.” In *Social Structures: A Network Approach*, edited by Barry Wellman and S. D. Berkowitz, 130–184. Cambridge University Press, 1988.

Wellman, Barry. “Toolkit Essay.” Review of *The Development of Social Network Analysis: A Study in the Sociology of Science*, by Linton Freeman. *Contemporary Sociology*, May 2008, Vol. 37, No. 3, Book Review: 221–223.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Heather Gregg
   Naval Postgraduate School
   Monterey, California

4. Professor Sean Everton
   Naval Postgraduate School
   Monterey, California

5. Professor Doowan Lee
   Naval Postgraduate School
   Monterey, California