NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DIM NETWORKS: THE UTILITY OF SOCIAL NETWORK ANALYSIS FOR ILLUMINATING PARTNER SECURITY FORCE NETWORKS

by

Antione C. Fernandes
Travis J. Taylor

December 2015

Thesis Advisor: Douglas Borer
Second Reader: Ian Rice

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE DIM NETWORKS: THE UTILITY OF SOCIAL NETWORK ANALYSIS FOR ILLUMINATING PARTNER SECURITY FORCE NETWORKS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Antione C. Fernandes and Travis J. Taylor			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A___.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

As the security landscape changes, the importance of strong and influential partnerships for security cooperation (SC) increases. The process of selecting the best possible partners should not be neglected; tools to accomplish this task may already exist. Recently, the use of social network analysis (SNA) has allowed the military to map dark networks of terrorist organizations and selectively target key elements. SNA data collection and analysis efforts remain focused on these terrorist networks, whereas friendly or light networks have been relatively neglected.

This thesis highlights the importance of analyzing light networks for SC and introduces the concept of dim networks. These are networks that consist of friendly actors whose connections to external organizations may not be public. This thesis has potential to improve partner security force engagement selection through the use of SNA principles, methods, and software, yielding several dividends. First, it provides a commander with a detailed understanding of the foreign units involved in SC, which allows for development of a more focused engagement strategy. Second, it allows SC planners to invest time and resources on the partner security forces that most effectively advance the commander's engagement priorities. Third, it reinforces the collection of network-related data on organizations the U.S. military cooperates with and the importance of analyzing that empirical data to improve SC.

14. SUBJECT TERMS social network analysis, dark networks, light networks, dim networks, security cooperation, Southeast Asia, network, Special Operations, Philippines			**15. NUMBER OF PAGES** 121
			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

DIM NETWORKS: THE UTILITY OF SOCIAL NETWORK ANALYSIS FOR ILLUMINATING PARTNER SECURITY FORCE NETWORKS

Antione C. Fernandes
Major, United States Army
B.A., Rutgers University, 2004

Travis J. Taylor
Major, United States Army
B.A., The Citadel, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Douglas Borer
Thesis Advisor

Ian Rice
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the security landscape changes, the importance of strong and influential partnerships for security cooperation (SC) increases. The process of selecting the best possible partners should not be neglected; tools to accomplish this task may already exist. Recently, the use of social network analysis (SNA) has allowed the military to map dark networks of terrorist organizations and selectively target key elements. SNA data collection and analysis efforts remain focused on these terrorist networks, whereas friendly or light networks have been relatively neglected.

This thesis highlights the importance of analyzing light networks for SC and introduces the concept of dim networks. These are networks that consist of friendly actors whose connections to external organizations may not be public. This thesis has potential to improve partner security force engagement selection through the use of SNA principles, methods, and software, yielding several dividends. First, it provides a commander with a detailed understanding of the foreign units involved in SC, which allows for development of a more focused engagement strategy. Second, it allows SC planners to invest time and resources on the partner security forces that most effectively advance the commander's engagement priorities. Third, it reinforces the collection of network-related data on organizations the U.S. military cooperates with and the importance of analyzing that empirical data to improve SC.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AtN	Attack the Network
CMSE	Civil Military Support Element
DOD	Department of Defense
GCC	Geographic Combatant Commander
GPH	Government of the Philippines
ICG	International Crisis Group
JCET	Joint Combined Exchange Training
JSOTF-P	Joint Special Operations Task Force – Philippines
MNLF	Moro National Liberation Front
NGO	Nongovernmental Organization
NSS	National Security Strategy
ORA	Organizational Risk Analyzer
RME	Rogue Moro National Liberation Front Element
PACOM	Pacific Command
PNP	Philippine National Police
PSF	Partner Security Force
SC	Security Cooperation
SOCPAC	Special Operations Command Pacific
SODARS	Special Operations Debrief and Retrieval System
TSCP	Theater Security Cooperation Program
TSOC	Theater Special Operations Command
USSOCOM	U.S. Special Operations Command
USSOF	U.S. Special Operations Forces

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to extend our heartfelt thanks to all those that have assisted us in completing this thesis. The hours of discussion in our advisors' offices were instrumental in the creation and evolution of this thesis. Thank you, Dr. Doug Borer and Colonel Ian Rice, for your patience and always-insightful conversations in guiding us down the path to publication and for assisting in the exploration of the idea of dim networks. Additionally, we would like to thank the staff of the CORE Lab, specifically Dr. Sean Everton and Daniel Cunningham, for their contributions to our education as we developed the concepts that went into this thesis. We appreciate the time and effort of the Naval Postgraduate School Graduate Writing Center staff and offer a special acknowledgment to Chloe Woida and her exceptional coaching. The countless hours you spent correcting our unique writing style and molding it into something we can be proud of is greatly appreciated. Your type of dedication has not been seen since the dawn of time; you represent the true social fabric of society. To Mrs. Peggy Rawl and Alison Cameron, thank you for taking the time to proofread our thesis and other papers. Last but most important, we would like to thank all our friends and family who have stood by us along the way. Knowing we had your unwavering support was greatly appreciated and priceless. We are truly blessed to have you in our lives.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> "*Today we are faced with the preeminent fact that, if civilization is to survive, we must cultivate the science of human relationships—the ability of all peoples, of all kinds, to live together and work together, in the same world, at peace.*"[1]
>
> —President Franklin D. Roosevelt

The idea of "peacetime engagement" through security cooperation (SC) is reemerging as the predominant national policy of the United States because of the official ending of both the wars in Afghanistan and Iraq.[2] The end of Operation Enduring Freedom after 13 years of combat has slowly transitioned military activity across the globe to a perpetual war state in which irregular warfare places fresh demands on security cooperation. This transition requires network building to occur during overseas military engagements. We refer to peacetime engagement as the policy that includes a fusion of political, economic, and military means to achieve the ends of international partnership for peace, stability, conflict deterrence, and power projection for this thesis. Last, we will focus on U.S. Special Operations Forces (USSOF) as the means to execute this national policy, more specifically Special Operations Command Pacific (SOCPAC) and the forces assigned to that command.

U.S. Special Operations Command (USSOCOM) defines the human domain as "The totality of the physical, cultural, and social environments that influence human behavior to the extent that success of any military operation or campaign depends on the application of unique capabilities that are designed to fight and win population centric conflicts."[3] The ability for USSOF to achieve success and shape environments is rooted

---

1 Franklin D. Roosevelt, "Undelivered Address Prepared for Jefferson Day." (April 13, 1945), http://www.presidency.ucsb.edu/ws/?pid=16602.

2 Department of Defense, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, 2014).

3 U.S. Special Operations Forces, *Operating Concept* (MacDill Air Force Base, FL: United States Special Operations Command, 2013), 5.

in its ability to understand this complex and evolving domain. This area is one of the most critical aspects of global security because it is the defining factor in all conflicts. The following is a statement made in a recent white paper organized by top-level military leaders in the Marine Corps, Army, and Special Operations:

> Land operations have a uniquely significant role, in both peacetime and conflict, in addressing human factors. This assertion rises from the recognition that: 1) the Army, Marine Corps, and Special Operations Forces significantly contribute to the activities central to influencing the "human domain" short of war, such as peacekeeping, comprehensive military engagement, security force assistance, building partner capacity, and stability operations; 2) in conflict, the same forces are those most intimately and closely involved with the human networks – friendly, enemy, and neutral—that comprise the "human domain"; and 3) strategic success or failure most often occurs within the land domain, especially in the shared space between humans and the land, and potentially in the shared space between humans and the cyberspace domain.[4]

The combination of the different services contributing to this white paper signals that a gap exists in understanding the operating environment. It is important to note the emphasis placed on human networks, and that they comprise not only enemy elements but also those of friendly and neutral elements.

The U.S. government uses combatant commands' theater engagement plans to project power, build and strengthen alliances, and maintain influence in areas throughout the world. As part of the combatant command's theater campaign plans, the Department of Defense (DOD) conducts military training to build up and strengthen the defensive capabilities of its allies. Often, during the execution of these exercises, USSOF partner with their equivalents in foreign countries (i.e., a Special Forces team will partner and train with the partner nation's Special Forces unit). This can come with a cost when a lack of understanding exists of how that security force is networked or positioned within their country. In a time of crisis, it is unclear whether this unit will have the optimal political connectivity and resources at its disposal that are necessary to prevent threats from emerging or before they have the ability to inflict significant devastation.

---

4 Army Capabilities Integration Center, *Strategic Landpower: Winning the Clash of Wills.* May 6, 2013.

Introducing a new concept called "dim networks," this thesis will use case study analysis to explore how the utilization of social network analysis may optimize partner security force selection. Key ideas of dark networks and light networks within SNA will be used. Dark networks will be defined as covert organizations that engage in illegal activities and have inflicted harm to others, whereas light networks are open and overt and do not set out to intentionally harm people.[5] Within this spectrum of networks—and unique to this research—is the idea of focusing on the dim networks surrounding military engagements overseas. Dim networks are located in the middle of the dark-light network spectrum and can take on characteristics of either and are defined as a network that displays both overt and covert tendencies. A new dimension within this spectrum is a dim network. They tend to be informal, unpublicized relationships between entities yet can be open; however, information to illuminate these networks is missing. The goal is to transition a dim network to a light network or dark network. In Chapter III, dim networks and the dark-light network spectrum will be discussed and analyzed further.

This thesis will include case studies that highlight examples of the effective use of SNA that provide elevated situational awareness and understandings of organizations. These insights allow for decisions to be made that shape the operational environment and therefore build a case supporting the use of this analysis in the SC planning process, focused specifically around engagement selection. Additionally, a proof of concept through the simulation of a SNA approach to a SC network in a notional country is provided to demonstrate the process and provide examples of the data required that would allow for detailed analysis. The simulation demonstrates the utility of SNA in engagement selection. This framework may help to provide tools to facilitate structured data collection that could lead to effective analysis.

One of the methods to determine the "success" or results of SC events achieving national level objectives is through the lens of network theory. To determine which forces are selected, quantitative measures and assessments must be developed that capture the causal relationships between the military aid, skill sets, and resources obtained by the

5 Jörg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory*, J-Part 13, no. 4 (2003): 413–439.

host nation. Understanding how forces use these capabilities within their own networks will impact how future bilateral and multilateral military engagements are conducted because the network aspect of engagements may determine the direction of an engagement strategy. However, focused collection efforts need to be prioritized in order to gather the necessary data to visualize these networks and close knowledge gaps about the operating environment.

A. PROBLEM

"Why are we training this unit? What are the long-term objectives we are trying to achieve by training this particular unit? What is the desired end-state for this unit? Why is this particular unit important?" These are common questions that USSOF teams ask before carrying out a security cooperation-training event, and all too often, these questions go unanswered before the execution of the training. Both authors of this research have similar experiences with this type of situation in SC events.

Two anecdotes derived from personal experiences of each author illustrate discrepancies in SC events that relate to the research. In the winter of 2010, Captain Travis Taylor was in command of a Special Forces Operational Detachment Alpha. His detachment was deployed to a Central Asian country with a mission to train a specific security force in counter narcotics and tactics. The Special Forces Operational Detachment Alpha coordinated with the Operational Planning Team, located at Special Operations Command Central, to ensure that their plan and program of instruction was nested with the Special Operations Command Central commander's desired end state for the Partner Security Force (PSF) unit. Unfortunately, no such end state or guidance was available. In fact, there was no unit specific long-term plan at that time, which undermined the purpose of the training. Additionally, the host nation continued making last-minute changes, causing the engagement to be changed three separate times. This would become a familiar situation for many other teams charged with the mission to train the security forces in that country, whereby no two training events seemed connected; each was separate, without a clear purpose to advance any line of operation or line of effort of the Theater Special Operations Command (TSOC) or the host nation.

The second example shows similar experiences during a Civil-Military Engagement mission in Southeast Asia. Captain Antione Fernandes was in charge of developing a comprehensive "build partner capacity" program to develop civil military operations with a host-nation unit. Additionally, he was asked to coordinate and synchronize all SC events that took place in country. Each engagement had a similar theme: the lead planners did not know why they were engaging with a specific unit over other units, nor did they have any sense of how that unit progressed from the previous exercise. Captain Fernandes had only a mere recommendation that he could dictate to the unit being trained, the location where the engagement would take place, and/or the point of instruction, yet he could not base these recommendations on anything tangible other than his 2- to 3-month observations while in-country. Although he held substantial influence from his position, he could not objectively rationalize the exercises the planners intended to execute or even his recommendations to them to help "improve" their events.

Conversations with other officers with similar experiences led to the belief that these circumstances are more common than not. According to reports obtained from the Joint United States Military Advisor Group-Philippines in fiscal year 2015, there were 199 separate SC events scheduled for the Pacific Command (PACOM) area of responsibility. SOCPAC units carried out 68 of those 199 events.[6] Despite a high number of individual events, many were not connected to each other. Those that were seem to only be connected to subsequent events that were conducted by similar unit. First Special Forces Group (Airborne) carried out the majority of the SOCPAC events. These units will typically work with the same units or a group of host nation units. Unfortunately, even under these circumstances, many of the events may not be connected nor are the units that are trained consistent with each event.

B. RESEARCH QUESTION

How can SNA assist in identifying the most influential, military units to partner with when applied to partner security force networks? Furthermore, are the data required

[6] Theodore T. Liebreich, "JCET Program Overview for PNP MG," (Joint United States Military Advisory Group reporting, Philippines, 2014).

to illuminate dim networks available and organized in such a way to allow planners to use SNA?

C. CLAIM AND METHODOLOGY

This thesis proposes the utilization of SNA to examine the dim networks surrounding U.S. partner security forces. These networks are typically referred to as "light" or "bright" networks when illuminated. However, we believe they are more accurately described as "dim networks" because of the lack of collective information about them. For these networks to be fully understood and used, they must be illuminated or mapped. If the network is visualized, it can be more easily influenced. SNA is uniquely suited to provide the necessary process to do this.

1. Overview

If what we propose is true, then we should see evidence of these partner networks in the areas where USSOF operate as well as be able to identify if those networks had an impact on certain operations or events. The variable we will focus on is the "partnered force" or "partnered unit" with which USSOF engages. To study the application of SNA toward engagement selection, we selected case studies that describe in detail how SNA has been operationalized in the past to illuminate dark and dim networks. It is necessary to show how the principles and methods within SNA are effective regardless of the type of network, the purpose of illuminating that network, or how the actors or organizations in the network influenced their environment.

Because SNA comprises many different social science disciplines, it is common for theories within this field to have the same definition but a different terminology. For example, the term "individuals" can also be referred to as "actors," "nodes," or "vertices."[7] Additionally, different social network analysts adopt different methods when conducting fieldwork. Although differences can be observed based on their backgrounds and level of expertise, the lessons can still be beneficial to incorporate within this research.

7 Christina Prell, *Social Network Analysis: History, Theory & Methodology* (London: SAGE Publications Ltd, 2011), 8.

The military has predominantly used SNA to disrupt or dismantle dark networks. It is necessary to describe how the application of SNA can support the Geographic Combatant Commands (GCC) Theater Campaign Plan and the TSOC's Theater Security Cooperation Program (TSCP) through the use of historical case studies. Within each case study, the important attributes[8] used will be examined to determine which strategy would be most effective in either influencing or combating the network. Additional benefits of this analysis can provide opportunities to adjust the types and purpose of engagements based on the dynamics of the network. The goal would be to shape the operational environment so that these "SOF networks" have the ability to successfully respond to threats.

In Chapter IV, a case study will include an examination from two perspectives. This case study involves a crisis situation that occurred in the Philippines in 2013 that one of the authors witnessed firsthand. This crisis included agencies and officials from the national government, local government, key nongovernmental organizations (NGOs), and the majority of the security force units in the country. The first portion will include a retrospective analysis to indicate focus areas required for this analysis. This case tests the network theory and determines what information is necessary to construct a beneficial organizational network picture or indicate ways to improve upon the presented method of analysis.

Additionally, Chapter IV will describe what changes are needed to move forward with efforts to incorporate SNA into PSF selection by examining current USSOF SC reporting requirements. Each mission that USSOF executes requires the creation and filing of numerous reports. One such report includes a Special Operations Debrief and Retrieval System (SODARS). By examining this robust report, we can determine whether reporting is a priority and if current arrangements support conducting SNA on light networks. The authors will attempt to construct a network based on existing reporting to reconstruct the government of the Philippines' response network during the Zamboanga City Crisis.

8 Sean F. Everton, *Disrupting Dark Networks* (Cambridge University Press, 2012), 14. *Note:* An attribute is defined as a characteristics of individual actors (e.g., race, gender, ethnicity).

Chapter V will include a simulated network that displays organizations and their relationships with each other as a proof of concept. This simulated network will use the concepts outlined in this thesis to provide a visualization of how SNA could illuminate dim networks to determine which organizations should be engaged. This determination will be based on simple SNA centrality measures, total degree,[9] betweenness,[10] closeness,[11] and Eigenvector.[12]

2. Case Selection

Of the two case studies highlighting existing SNA research, the focus will be on SNA as applied to the dark network of the Indonesian terrorist group Noordin Top.[13] This case study will demonstrate the application of SNA on dark networks to understand and visualize key influential actors and target them for exploitation or elimination. This thesis seeks to expand the use of SNA beyond kinetic targeting and present the argument that the principles of this analysis can be applied to the "targeting" of PSF. This peacetime targeting is geared for the purposes of focusing the developmental effort on units that will best serve the security interests of not only their country, but also that of the United States. To do so, it is necessary to apply the SNA to a light network. Our second case involves the Humanitarian Assistance Network in Tajikistan,[14] which will provide insights into how dim networks can become light.

---

9 Total degree centrality is the number of a node's ties.

10 Betweenness centrality measures the range to which each node lies on the shortest path between all other nodes in a network.

11 Closeness centrality measures how close each node is to all the other nodes in a network by their path distance.

12 Eigenvector centrality assumes that ties to central nodes are more important than ties to exterior nodes and therefore weighs the nodes' connections to others by their centrality scores.

13 This network was mapped using data drawn originally from *Terrorism in Indonesia: Noordin's Networks*, a publication of the International Crisis Group. Military students at the Naval Postgraduate School participating in a class entitled, Tracking and Disrupting Dark Networks initially coded the data. This class was a part of a Common Operational Research Environment (CORE) Lab sub-curriculum instructed by Professor Sean Everton, Co-Director of the CORE Lab.

14 Jeffery S. Han and Ryan Schloesser, "Joining the Helping Hands: Understanding the Humanitarian Assistance Network in Tajikistan" (Unpublished paper, Naval Postgraduate School, March 27, 2014).

We selected our cases based on the following conditions: (1) the case analysis and research originated from and was completed by a military-related source; (2) the individuals or organizations in each case are located in an country where USSOF conducts SC events; (3) the case takes a previously unmapped network whether dark (covert) or light (overt) and maps them; and (4) the results of each case were derived and presented through the primary use of SNA.

Both of the cases in Chapter IV contain examples of networks developed through the use of SNA tools and methodology. Each network is understood to have existed before the analysis; however, no visual representation of the networks existed. The visual representation through tools from this analysis is paramount to the dissection and examination of each network and their nodes or parts. Although both cases exist in different environments and reflect different circumstances, their similarities allow us to determine how this analysis was effective in providing necessary information to allow for improved decision-making. This information is also representative of a detailed understanding of how networks affect the operational environment in which they exist.

3. Data Sources and Procedures

Currently, there is limited research that attempts to integrate SNA to analyze effects of SC events; therefore, many different sources were used throughout the course of this research. After-action reports from SOCPAC and the host nation were used to study how both sides viewed SC. At a deeper level, the USSOF reports were used to determine if the information needed to understand friendly networks was collected by operators and prioritized by higher commands. The next phase included taking these reports and inputting them into SNA programs to visualize any networks that emerged. To supplement missing information, open news sources were used by reputable news agencies within the United States and the Philippines. Additionally, for this approach to be effectively implemented across different theaters, a simulated network was created. This network includes a step-by-step process describing the information necessary to collect, and how to use SNA metrics such as centrality, to understand networks.

4. Assumptions

The following assumptions substantially guided the research conducted:

> Assumption One: There are enough accessible data from the theory development case that contain the information needed to extract the relational data required to map out the networks without conducting interviews.
>
> Assumption Two: The simulated data will allow for this model to be used in other environments to measure friendly networks appropriately.
>
> Assumption Three: The SNA measures will reveal network characteristics of the PSF, including relationships with outside organizations that will enable decision makers to adjust future engagement strategies.

D. FRAMING THE SITUATION

Numerous National Capital Region policy documents impact how the DOD trains, equips, and fights. The National Security Strategy (NSS) published in February 2015 presents a common theme of "global complexity." The NSS also expressed the need to ensure that the United States maintains its global partnerships and continues to build partner capacity in order to prevent conflict, to secure international order, and to strengthen our national defense.[15] Additionally, throughout the document, President Obama reemphasized the rebalance to the Asia-Pacific region. This is echoed in the Defense Strategic Guidance of 2012, which specifically states, "We will also expand our networks of cooperation with emerging partners throughout the Asia-Pacific to ensure collective capability and capacity for securing common interests."[16] In the 2014 *Quadrennial Defense Review*, then-Secretary of Defense, Chuck Hagel, eloquently described his vision for the future of U.S. defense strategy:

> Our sustained attention and engagement will be important in shaping emerging global trends, both positive and negative. Unprecedented levels of global connectedness provide common incentives for international

15 Barack Obama, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2015). www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

16 Department of Defense, *Defense Strategic Guidance* (Washington, DC: U.S. Department of Defense, 2012) http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf.

> cooperation and shared norms of behavior, and the growing capacity of some regional partners provides an opportunity for countries to play great and even leading roles in advancing mutual security interests in their respective regions. In addressing the changing strategic environment, the United States will rely on our many comparative advantages, including the strength of our economy, our strong network of alliances and partnerships, and our military's human capital and technological edge.[17]

Hagel emphasizes many key themes surrounding partnership and engagement, capacity of our allies, and networks within his vision. Although the United States has always relied on treaties and allies for international cooperation, the anticipated changes within the global environment call for a substantial increase in global partnerships. Hagel goes on to describe the DOD's role in this strategy:

> The role of the Department of Defense in supporting U.S. interests is rooted in our efforts to reduce the potential for conflict, by deterring aggression and coercive behavior in key regions, and by positively influencing global events through our proactive engagement.[18]

Once again, the predominant theme is about global complexity and the priority placed on maintaining our engagement strategy as a means to shape the global security environment and ensure U.S. national security. In this case, the term "proactive engagement" is extremely important in times of the diminishing manpower, budgets, and additional resources needed to project global power. Engagement strategies will need to be renewed and focused to meet the demands established in the Quadrennial Defense Review.

The 2015 National Military Strategy, echoes the NSS with a continued call for the "military to remain globally engaged to shape the security environment and to preserve our network of alliances." Networks are once again used to formulate the thinking behind this strategy. Outlined in the NSS, the national military objectives provide succinct end states for our military: "Deter, deny, and defeat state adversaries; disrupt, degrade, and defeat violent extremist organizations; and strengthen our global network of allies and"

17 Department of Defense, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, 2014) http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

18 Ibid.

partners.[19] Each set of objectives is critical to the rebalance to Asia. The NSS emphasizes the importance of the presence of U.S. Forces in key locations to meet these objectives as well as to provide necessary early warning and response to impending crises. The question remains: How exactly will the small footprint of U.S. Forces strategically positioned globally be able to tap into the "networks of allies and partners" in a time of crisis?

Retired Navy Admiral William McRaven, former commander of USSOCOM, outlined clear strategic ends for USSOCOM in the 2013 USSOCOM USSOF Operating Concept. Building on the Defense Strategic Guidance, McRaven articulated his vision for the future of USSOF operations in the twenty-first century within each preceding document for defense strategy. McRaven highlighted USSOF's role in enduring global engagements through long-term, scaled, and distributed operations. In doing so, he stressed that USSOF will be positioned to enable, create, and maintain partnerships that endure, prevent conflicts, and prepare to fight and win our nations wars.[20] SOCOM is forming ways to meet the requirements that establish the global networks outlined in the National Capital Region documents. McRaven has created a requirement for USSOF to spearhead and maintain these networks, essentially becoming the force of choice to shape future USSOF engagements that focus on building the global networks worldwide.

Moving downward to the theater level, SOCPAC's lines of effort are additionally nested with the guidance provided by higher echelons, including those of USSOCOM. SOCPAC's lines of effort address understanding theater strategy and move toward accomplishing strategic objectives. Those lines of effort are as follows.

1. Gain visibility and understanding of the environment.
2. Prepare for the environment.
3. Shape the operational environment.
4. Build partner capacity.
5. Attack the threat.[21]

---

19 Joint Chiefs of Staff, "National Military Strategy of the United States of America, 2015. The United States Military's Contribution To National Security" (Washington, DC: U.S. Joint Chiefs of Staff, 2015) http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

20 U.S. Special Operations Command, *Operating Concept* (MacDill Air Force Base, FL, 2013), 3,

21 Data for this study originate from unclassified portions of the Special Operations Command Pacific that are available from the special operations command Pacific (SOCAC) portal.

It is apparent that, within our defense structure, the importance of building and maintaining networks and alliances of partners that share the same norms of security and international order is recognized as a priority. Although there is a network theme from the national region to the tactical level, very little is known or understood about these networks. This creates opportunities to accomplish the other lines of effort identified previously by correcting this void. By leveraging the networks of partners, SOCPAC will be positioned to develop a better understanding of the environment and thus be able to conduct more effective preparation and shaping operations. By building the capacity of partner forces, SOCPAC is investing within these global networks to increase its ability to deal with future threats unilaterally. However, the argument is not "if" we should engage or build partner capacity, nor is it particularly "when" we should do it; the question is "with whom" we should engage. Furthermore, in an era of long-term fiscal austerity and force reductions, USSOF remains the preeminent solution for sustained, low-cost, low-signature, persistent engagement.

As the DOD continues to downsize to a postwar structure, cost-effective measures must be implemented to optimize military activities worldwide. Fiscal austerity has become the new "norm," and USSOF specifically has to evolve from a force that previously had a bottomless budget to a force that must do more with less. A region where this mindset has overshadowed the primacy of expensive direct action is the Asian Pacific.

E. ASIA-PACIFIC PIVOT

Due in part to the perceived expansion of Chinese influence, President Obama announced a "pivot" or "rebalance" to Asia in 2012. In a 2011 op-ed for *Foreign Policy Magazine*, "America's Pacific Century," Hillary Clinton, then-Secretary of State, addressed the importance of reinvesting in the Pacific saying, "The future of politics will be decided in Asia, not Afghanistan or Iraq, and the United States will be right at the center of the action." Additionally, she wrote, "In the last decade, our foreign policy has transitioned from dealing with the post-Cold War peace dividend to demanding commitments in Iraq and Afghanistan. As those wars wind down, we will need to

accelerate efforts to pivot to new global realities."[22] More recently, the Asian-Pacific region pivot has reemerged as a focal point for U.S. national security by President Obama's push for the Trans-Pacific Partnership[23] and his guidance to rebalance or pivot to Asia.[24]

This effort to reinvest in the Pacific, specifically with regards to regional security and stability, would call upon USSOF to spearhead this campaign of engaging with strategic and influential PSF throughout the Pacific as identified in the 2013 USSOF Operating Concept. SOCPAC has operational control of all special operations conducted in the region. They have and will continue to be very active in this region by maintaining a near-permanent presence that conducts numerous SC operations in a total of nineteen countries.[25] Strengthening the security environment and the military forces of U.S. partners in this region has become a top priority for the current administration and the DOD. In addition to persistent instability in the Middle East, Russia's recent activity in Ukraine and China's activity in the South China Sea are part of their attempts to become the superpower in those regions: a challenge and threat to U.S. hegemony. Such actions have significantly influenced U.S. foreign policy priorities and initiatives.

F. U.S. SPECIAL OPERATIONS ROLE IN SECURITY COOPERATION

Partnership, peace, stability, and success are all at stake in the complex and persistent struggle for regional and global security. USSOC is charged with shaping these ambiguous and constantly evolving environments in a way that is more conducive to advancing U.S. national security interests. USSOF are well suited to operate on this strategic stage, but must continue to adapt to emerging trends that will impact their

22 Hillary Clinton, "America's Pacific Century," *Foreign Policy*, October 11, 2011.

23 The Trans-Pacific Partnership (TPP) is an economic trade agreement among twelve Pacific Rim countries. The agreement was reached on October 5, 2015, after 5 years of negotiations. According to the Office of United States Trade Representative Office's website, the "TPP is a platform for engagement and growth in the Asia Pacific Region. It solidifies relationships with our allies and firmly establishes the United States as a leader in the Pacific." More information can be found at their website, https://ustr.gov/tpp/.

24 The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2015).

25 Data for this study originate from unclassified portions of the Special Operations Command Pacific that are available from the special operations command Pacific (SOCAC) portal.

operational capabilities and present challenges. The redistribution and diffusion of global power, the rising role of non-state actors, the increase in accessibility of advanced technology, rapid growth and expansion of urban spaces, and the continued fragility of the economic health of the United States and its partners will all influence the conditions around which USSOF will have to plan, provide resources, and execute operations.[26] In his statement about the situation to the House Armed Services Committee, Subcommittee of Emerging Threats and Capabilities, General Votel explained "The diffusion of power is decreasing the ability of any state, acting alone, to control outcomes unilaterally. Globalization has created networked challenges on a massive scale. Only by working with a variety of security partners can we begin to address these issues."[27]

The majority of USSOF operations will encompass the full spectrum of SC through peacetime engagement. The Defense Security Cooperation Agency's Security Assistance Management Manual provides the definition and purpose SC as follows.

> All activities undertaken by the Department of Defense (DOD) to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DOD interactions with foreign defense and security establishments, including all DOD-administered Security Assistance (SA) programs, that build defense and security relationships; promote specific U.S. security interests, including all international armaments cooperation activities and SA activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations. It is DOD policy that SC is an important tool of national security and foreign policy and is an integral element of the DOD mission. SC activities shall be planned, programmed, budgeted, and executed with the same high degree of attention and efficiency as other integral DOD activities. SC requirements shall be combined with other DOD requirements and implemented through standard DOD systems, facilities, and procedures.[28]

---

26 Joint Special Operations University (JSOU), *Special Operations Forces Reference Manual*, 4th edition (Tampa, FL: JSOU Press, 2015), 1–3.

27 General Joseph L. Votel, Statement to The House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, March 18, 2015. http://fas.org/irp/congress/2015_hr/031815votel.pdf.

28 Defense Security Cooperation Agency, *Security Assistance Management Manual*, C1.1.1 (Washington, DC: Defense Security Cooperation Agency).

Each engagement has the potential to have positive and negative strategic impacts. The possibility of negative impacts is critical, with many different variables that must be accounted for in order to mitigate them.

The origins and evolution of the current TSCP for the USSOCOM began long before the organization was established. After World War II, the U.S. military was used in various fashions to promote democracy and assist many war-torn nations to rebuild not only their fighting forces, but also their diplomatic capabilities.[29] The creation of the modern U.S. Special Forces in 1952 was largely brought about from the need to have U.S. elements positioned in specific former Soviet countries to train and equip guerrilla forces to combat the possible Soviet threat to Western Europe. The training of foreign militaries in unconventional warfare by these forces became the cornerstone of U.S. special operations.[30]

Today, USSOF continue this legacy through military engagements in more than eighty countries.[31] These engagements range from Joint Combined Exchange Training (JCET), which permits USSOF to train through interaction with friendly foreign forces,[32] to civil-military subject matter expert exchanges that focus on sharing knowledge between a foreign military and the U.S. military. These exchanges represent a complete joint effort, with all four branches conducting similar engagements across the globe. All are central to USSOCOM's establishment of a global network of partners, and each engagement serves to further expand this network that in essence could serve as future conduits of information, intelligence, alliance, and support.[33] Furthermore, TSCP engagements are an extension of U.S. foreign policy; they act as physical manifestations of U.S. resolve in combating international and transnational threats globally.

---

29 Earl F. Ziemke, *The U.S. Army in the Occupation of Germany 1944–1946* (U.S. Government Printing Office, Washington, DC, 1975), iii.

30 Special Forces Association, "The Origin of Special Forces."

31 Votel, Statement to The House Armed Services Committee Subcommittee on Emerging Threats and Capabilities.

32 Joint Report to Congress, Foreign Military Training, Volume 1, Fiscal Years 2008 and 2009.

33 Thomas S. Szayna and William Welser IV, *Developing and Assessing Options for the Global SOF Network* (Santa Monica, CA: RAND, 2011), 1.

SOCPAC is a subunified command under PACOM located at Camp Smith, Hawaii, that "coordinates, plans, and directs special operations and related activities in the Pacific Theater."[34] SOCPAC's mission supports the PACOM commander's objectives in the region through the deterrence of aggression, providing forces to respond to emerging crisis, and advancing SC with PACOM partners through peacetime engagements. SOCPAC's strategy uses an indirect approach that focuses on three specific lines of operation to meet PACOM objectives: "(1) increasing partner nation security capacity, (2) improving information gathering and sharing, and (3) securing the support of the population."[35] The pursuit of these objectives as part of the overall strategy of SC requires an adaptive and agile force that understands the networks that exist wherever the force operates.

This thesis highlights the importance of networks and their role in engagement selection within SC.[36] More specifically, this thesis will explore how SNA can assist in the determination of which entities the U.S. military should engage through the illumination of dim networks that could be instrumental in improving U.S. engagement capabilities. The lessons learned from studying terrorist organizations through SNA could be directly applied to the study of the PSF networks to uncover a greater awareness about potential allies, their capabilities, and the reach and depth of their influence. These networks can assist SC planners in understanding the potential influence each available unit has within a particular region and therefore provide them with necessary insight on how to best leverage that influence through selective engagement for the purposes of protecting U.S. national security interests.

34 JSOU, Special Operations Forces Reference Manual, 2–19.

35 Ibid.

36 We refer to the process of determining which PSF unit USSOF will partner, train, or work with as engagement selection. An engagement is any event that falls under the Building Partner Capacity Programs. This list can be found in the DSCA Security Assistance Management Manual, C15.1.4. http://www.samm.dsca.mil/chapter/chapter-15.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW AND BACKGROUND

Chapter I described the major transition of the DOD from a wartime military back to a peacetime military, and emphasized the significance of the directed rebalance to Asia. This change is occurring even as contests throughout the world continue to challenge peace and stability. Chapter I also highlighted the importance of understanding and engaging human networks and ways in which the USSOF can be prepared to operate in the complex human domain. This chapter reviews the literature on networks, social networks, and the methodology of SNA. Additionally, this review will highlight the military focus on dark networks overpowering concepts related to network theory. This focus has resulted in the absence of developing and implementing extensive methodologies to illuminate dim PSF networks.

A. NETWORKS

> *"Networks are seen as an ideal arrangement to preserve organizational independence and flexibility while offering multiple organizations the possibility of reaching common goals in limited areas such as research and development or enhancing delivery of certain goods and service*."[37]
>
> —Jörg Raab and H. Brinton Milward

The terms "networks" and" networking" have gained increasing popularity in the past 15 years. Both terms are often used interchangeably, albeit incorrectly, it is important to understand how they differ. Networking relies on the use of networks or, "a set of relations between objects which could be people, organizations, nations"[38] to understand the number or type of existing relationships and/or attempts to establish beneficial connections within the networks itself. "Networks are based on trust, reciprocity, and shared experience"[39] to achieve any sizable benefit from an established

37 Raab and Milward, "Dark Networks as Problems," 418.

38 Charles Kadushin, *Understanding Social Networks: Theories, Concepts, and Findings* (Oxford, U.K.: Oxford University Press, 2012.

39 Raab and Milward, "Dark Networks as Problems," 426.

network, users must understand the interplay surrounding the network (e.g., who has important relationships or how that network is connected or just as important, how it is not connected within their environment).

Scholars have written about the importance of understanding networks in the periods of increased nonstate actor violence toward states. In his 2009 article, "How to Win," John Arquilla discussed the importance of understanding network dynamics from a state perspective, explaining that, "if nations are to have any hope of ultimately defeating terrorism, they must understand networks as a distinct organizational form, not just a handy labeling device."[40] During the time Arquilla's article was published, a paradigm shift was giving rise to the development of methods to examine covert networks (i.e., terrorist organizations). Yet the focus on network analysis remained fixated on developing methods to understand the networks surrounding threats against American security interests and not of U.S. allies.

According to Albert-László Barabási, "Networks exist for a reason. They spread ideas; they spread knowledge; they spread influence";[41] to understand this allows for a greater realization of how and why particular events are caused by specific actors in various social situations. A thorough understanding of a network can lead to the development of a comprehensive approach to select ideal partner networks based entirely upon the type and amount of connections. Analysts and/or practitioners may essentially increase their ability to leverage, disrupt, or destroy networks by simply understanding how networks function and how they are structured as a method to uncover correlations that could help predict future behavior.

Networks exist everywhere. Barabási provides examples of networks dating back to early Christianity and also to modern times with the use of the Internet and terrorism. Each example that Barabási uses includes actors that in some way share a connection

40 John Arquilla, "How to Win," *Foreign Policy*, October 12, 2009.

41 Albert-László Barabási, *Introduction and Keynote to a Networked Self*, ed. Zizi Papacharissi (New York, NY: Routledge, 2011), 12.

with others.[42] The understanding of networks is increasingly important as network development begins to shape how our world conducts business and fights wars.

B. SOCIAL NETWORKS

Network theory provides extensive insights into the reasons why particular people are connected to one another. Networks and networking exist in a variety of forms from computer networks and satellite networks to unions and organized crime. All of these appear to have one characteristic in common: human social interaction at some level. Connections exist at a human level even with the utilization of technology. People interact with each other and create social networks. This section will focus on how items or information are transferred and/or distributed to different individuals throughout social networks. The idea behind social networks is significant to this research because PSFs that are engaged during SC events are truly members of social networks. Understanding these particular social networks is what this research aims to do.

John Barnes, credited with coining the term "social network" in his 1954 study "Class and Committees in a Norwegian Island Parish," explains that members of society interact with each other in a regular and organized fashion. Furthermore, this interaction occurs within the same sphere of discourse and is influenced by different aspects of that society, such as class. Barnes defined the social network in the Norwegian Island Parish as "a system of ties between pairs of persons who regard each other as approximate social equals." Christina Prell defines a social network as "a set of relations that apply to a set of actors, as well as any additional information on those actors and relations."[43] These definitions begin to build on network theory by focusing on networks that are influenced by the human element as opposed studying inanimate objects that share connections. The study of social networks has led to the "small-world phenomenon," or "six degrees of separation" idea, that two humans are connected through an average of five to six steps. Stanley Milgram pioneered this idea in his 1967 article, "The Small-World Problem."

---

42 Albert-László Barabási, *Linked: How Everything Is Connected to Everything Else and What it Means for Business, Science, and Everyday Life* (New York, NY: Plume, 2009), 3–7.

43 Prell, *Social Network Analysis: History, Theory & Methodology*, 9.

More recent studies have identified these characteristics to be prevalent in networks originating from nature as well as technology.[44] In other words, social networks have similar characteristics across different types of networks.

Different types of social networks exist around us. When we analyze a complex society, we begin to see examples of how different types of connections within these different social networks affect the transfer of information or ideas. Friendly networks often maintain a wide assortment of relational ties. Understanding how these ties affect social networks is important. Two prominent types of ties identified and introduced by Mark Granovetter are *strong ties* and *weak ties*.[45] In considering the differences between both categories of ties, analysts acquire a broader sense of how people interact with one another and can extrapolate different natures of patterns.

These different ties have increasingly come to light with the advent of social media and the ability for people to maintain connections they would not normally maintain if not for the ability to communicate instantaneously through technology. Most people maintain close relationships with certain people, such as immediate family and close personal friends. These kinds of ties typically help shape certain beliefs and personal characteristics and are characterized as strong ties. The ties we maintain with those outside this intimate circle are those that help us address everyday issues; these are labeled as weak ties. Granovetter's research on the concept of weak ties argues that focusing on the micro-level or small-circle strong ties does not allow for connections to be made to the macro-level patterns. The weak ties act as bridges to facilitate diffusion within a network, allowing for micro-level interaction to feed into macro-level patterns and back to the small group.[46] The idea of "strength of weak ties" is directly applicable to certain military use of network analysis. The need to understand the dynamics of social

---

[44] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi, "Internet: The Diameter of the World Wide Web." *Nature* 401, (1999), 103; Henry Kautz, Bart Selman, and Mehul Shah, "Referral Web: Combining Social Networks and Collaborative Filtering," *Communications of the ACM*, 40 (March 1997), 3.

[45] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78 (1973), 1360.

[46] Ibid.

networks for the specific intentions of influencing a network, predominantly a hostile network, has led the military to use SNA.

SNA within the military construct has focused on dark networks. There appears to be a lack of focus on light networks and their importance to military operations and objectives; therefore, the new concept of dim networks will show the importance of studying light networks while also demonstrating shared characteristics with dark networks. Light networks are overt, open, and nonthreatening, but they are also public, and their connections are to some extent publicized. Connections may be more personal, more informal, and possibly of a more sensitive nature, whereas dim networks, although also nonthreatening, are not necessarily so public. This is a characteristic that dim networks share with dark networks. Dim networks exist in in between the dark-light network spectrum. Characteristics from both dark and light networks can be applied to a methodology focused on dim networks.

C. SOCIAL NETWORK ANALYSIS

In his book, *Disrupting Dark Networks,* Dr. Sean F. Everton defines SNA as "a collection of theories and methods that assume that behavior of actors is profoundly affected by their ties to others and the networks in which they are embedded."[47] This section will focus on three areas relevant to SNA, namely: (1) how SNA is used across different domains to include social science and the business world, (2) major concepts within the field to include common SNA metrics, and (3) the concept of nodes, including types and corresponding roles, and the importance of sociograms. We will also look at the military application of SNA, including different scholarly approaches and current military execution and doctrine. Presently, SNA focus within the military has been exclusively on dark networks, which was extremely important during the wartime focus in combat operations. However, by failing to focus on friendly networks diminished efforts to achieve any long-term progress in the Middle East has become apparent. This research will attempt to illustrate that by transforming the dim networks of the U.S. PSF

47 Everton, *Disrupting Dark Networks*, 2.

to light networks can theoretically increase the success of U.S. long-term achievements in various types of operating environments.

1. Origins of SNA in Social Science and Business

SNA has been used in several disciplines to study group interactions and behaviors. Theories have originated within the social sciences and have then been implemented in the business world. Bernice Pescosolido's 2007 article, "The Sociology of Social Networks," describes the evolution of the use of SNA within social sciences. Pescosolido's evolution describes the origins of social networks and how they implicitly signaled the existence of social ties to more current social network theories being used to show causation of events. A strength or limitation of current network theories within social science is that each maintains slightly different theories.[48] An example of how business is using SNA can be seen in the book by Robert Cross and Robert Thomas, *Driving Results through Social Networks: How Top Organizations Leverage Networks for Performance and Growth*, which describes in detail how executives and managers can obtain significant performance and innovation advantages by leveraging networks.[49] The business world has begun to see the utility of SNA as a tool within their domain to maintain competitive advantages and relevance.[50] Both fields share commonalities that can be analyzed to determine best practices, which helps us understand how and why engagements are selected.

2. SNA Building Block Concepts

The recent integration of the different approaches within SNA helped pave the way for the formation of a modern approach. Though applications of SNA vary, they are generally characterized by: structural institution based on ties, systematic empirical data,

---

[48] Bernice Pescosolido, "The Sociology of Social Networks," in *21st Century Sociology,* ed. C. Bryant and D. Peck (Thousand Oaks, CA: SAGE Publications, Inc, 2007), pp. I-208-I-218.

[49] Cross, R. and Thomas, R. *Driving Results Through Social Networks: How Top Organizations Leverage Networks for Performance and Growth* (New York, NY: Jossey-Bass, 2009).

[50] Pescosolido, "The Sociology of Social Networks."

pulls on graphic imagery, and heavy use of mathematical models within the theory.[51] Appropriate data can be used to construct mathematical-based graphs. These graphs display important and often concealed interpretations of that organization. This is one way to become familiar with the networks that the U.S. military creates, or the networks that already exist within the global special operations network.

a. Nodes

Actors or "nodes" within a network can considerably affect how the network functions. Karen Stephenson identifies examples of network nodes that have influential power and can significantly alter network dynamics, such as hubs, pulsetakers, and gatekeepers.[52] According to Stephenson, each type of node has the ability to shape specific outcomes when this information is made available and is strategically used by organizational leaders. Although each type will be expressed as individuals, they can also take on organizational appearances as well. A crisis situation will be used here as it relates to the theory development case presented in a later chapter.

The first characteristic type is a "hub," or the "kind of person who becomes a gathering and sharing point for critical information."[53] Hubs will have many connections in the network that allow them to channel information and resources around the network with ease. During a crisis, hubs can be difficult to spot in the midst of chaos. There are usually several separate operations centers used by the police, military, the local government, the national government, and developmental agencies involved during a crisis. If and when these agencies ultimately come together, it is done in an ad hoc manner with minimal understanding of how the multitude of agencies can effectively collaborate toward a common goal. When placed in the correct position, hubs can act as connectors to these organizations and filter information more efficiently throughout the

51 Linton C. Freeman, *The Development of Social Network Analysis* (Vancouver, B.C., Canada: Empirical Press, 2004), 3.

52 Art Kleiner, "Karen Stephenson's Quantum Theory of Trust," *Strategy + Business*, 29, Fourth Quarter (2002).

53 Ibid., 8.

larger network. Information about military units that display hub-like tendencies within their environments is essential when planning or conducting SC events.

Stephenson's second type of node features pulsetakers who "carefully cultivate relationships that allow them to monitor the ongoing health and direction of the organization."[54] This type of actors are extremely beneficial to have in the correct position during a time of crisis as they measure what is going on and help craft appropriate responses. A pulsetaker has the ability to act as a useful liaison with external organizations to increase coordination and collaboration efforts. This person can also make the needed organizational changes during time-sensitive situations in crisis when often-decentralized organizations emerge. This individual type is fundamental to increasing network ties through meaningful connections from either internal or external ties or a combination of the both.

The third and final types are gatekeepers, who are the "information bottlenecks, controlling the flow of contact to a particular part of the organization, thus making themselves indispensable."[55] Knowing who gatekeepers are during a crisis would allow leadership to effectively disseminate pertinent information or resources for rapid decision-making purposes. Gatekeepers can shape decisions using their ability to pass certain fragments of information through a network. In *Managing with Power*, Jeffrey Pfeffer illustrates that a person in a gatekeeper position can alter the decision process of a company depending on the bias of the individual and how they decide to channel information.[56] If left unchecked, a gatekeeper possesses great influential power within a network—power that can be used undesirably. This type of node can be instrumental to have in a joint operations center coordinating efforts or in close proximity to leadership. The wrong time to find out an individual has gatekeeper tendencies is after the crisis is over or after the information value has decreased. Having access to the right host nation

54 Ibid., 8.

55 Ibid., 9.

56 Jeffrey Pfeffer, *Managing with Power: Politics and Influence in Organizations* (Cambridge, MA: Harvard Business Press, 1992), 114–115.

contact that can make important decisions before, during, and after SC events is a necessary step to achieving long-term success.

b. SNA Metrics

Networks take on different functions depending on their makeup, so it is vital to know and understand common SNA metrics such as size, density, degree of connection, centrality, closeness, betweenness, and clusters.[57] These metrics enhance the understanding within network analysis by looking at the interaction between nodes and ranking, of which node scores highest between the different measures.

There are methods in which nodes can be intermixed to have optimal results to improve organizational productivity in specific situations. Art Kleiner describes how placing a gatekeeper in an innovative network and having that individual tied with a pulsetaker in an expert network can increase learning in a company.[58] The informal connections within a network structure are extremely important to know so they can be effectively used to improve organizational capacity and capability. Organizations would be remiss not to include personnel that resemble Stephenson's hubs, pulsetakers, and gatekeepers strategically around their organization.

Organizations may take on different and/or multiple types of social networks at the same time, such as trust, communication, and friendship networks.[59] Running SNA metrics against each of these social networks within or across organizations will reveal information relevant to understand how particular networks function. SNA metrics can also reveal key patterns in different social networks within a single organization. The structural characteristics should be weighed differently depending on the type unit/organization being looked at.

---

57 Stuart Koschade, "A Social Network Analysis of Jemaah Islamiyah: The Application to Counterterrorism and Intelligence," *Studies in Conflict & Terrorism* 29, no. 6 (2006), 567.

58 Kleiner, *Karen Stephenson's Quantum Theory of Trust*, 9.

59 Koschade, "A Social Network Analysis of Jemaah Islamiyah: The Application to Counterterrorism and Intelligence," 567.

c. Sociograms

SNA "sociograms" are "a visual representation of a network developed through theory with the actors represented by nodes, and their relationships represented by links or lines"[60] (Figure 1). As an analytical tool to explain network data, sociograms date back to J.L. Moreno's sociology studies in the 1930s. To explain the relationships within his data, Moreno used graphic to map the relationships of individuals.[61] Figure 1 was one of the first documented cases in which graphs were used to help visualize and analyze network data. When applied correctly to analysis, sociograms help to leverage networks at different times across different environments. This leverage can manifest itself in ways that strengthen or weaken a network depending on the situation. Pfeffer summarized that an organization that has strategic relationships will have more influential power. He stated that "to develop influence, we need to be plugged into the structure of communication and interaction, and that means seeking out interactions, even social interactions strategically."[62] There are many ways to adjust how PSFs can build influence and thus increase their ability to project power and also deter malignant actors. After analysis is completed on PSF networks, a consensus must be made to use its capabilities based on their external network dynamics to include shared formal and informal ties, current level of influence, and political connectivity.

3. Current Military SNA Approaches

SNA demonstrates that understanding and hypothetically predicting future behavior of a group can be achieved by identifying how individuals are structurally located and connected within that group. The ties observed within a network can reveal network characteristics that can often be missed by casual observers. For example, since the aftermath of the attacks on September 11, 2001, the DOD and U.S. intelligence communities have explored new ways to study terrorist organizations. One useful discipline that emerged was SNA. This discipline indicated that by capturing the right

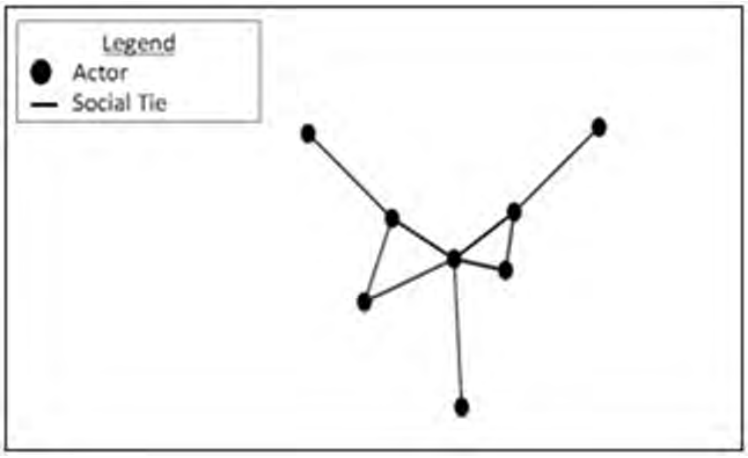
60 Ibid.

61 Pescosolido, "The Sociology of Social Networks," I-208-I-218.

62 Pfeffer, 124.

information about an organization, analysts could gain insight into their motivations, overall structure, and interactional features. This could also be used together to theoretically predict future behavior.

Figure 1. Sociogram highlighting actors (dots) and social ties (lines)[63]



a. The Academic Approach

There is limited literature on the application of SNA for the military and even less on USSOF-specific applications. The current and narrow literature available predominately focuses on counterterrorism examples and studies that examine terrorist and other covert organizations. The United States has successfully dedicated resources to understanding dark networks but has yet to develop methods to the study of friendly organizations. The first step to broaden the application of SNA within the military is to compare and contrast how social network theorists like Jörg Raab and Marc Sageman apply SNA processes to the study of dark networks. Then we will be able to postulate ways in which USSOF can use the same tools for SC events to properly select the most optimal units with which to engage.

63 Molly MacCalman, Alexander MacCalman, and Greg Wilson, "Visualizing Social Networks to Inform Tactical Engagement Strategies That Will Influence the Human Domain." *Small Wars Journal* (2013)

In the early 2000s, Raab conducted research and studies on how network characteristics of organizations affect themselves, external organizations, and their environments. He analyzed multiple aspects of how some dark networks can be resilient and how certain network characteristics and external pressures can affect network capabilities. In *Dark Networks as Organizational Problems*, Sageman, Raab, and H. Brinton Milward provided analysis that demonstrates how terrorist organizations undergo network characteristics changes and evolution in order to prevent their destruction.[64] By listing out and observing how dark networks adjust to external pressures Raab provided insights that certain behaviors were essential for survival.

Sageman challenged the mainstream thinking of terrorist organizations in understanding terror networks. In the past, government counterterrorism programs were based on traditional understanding of terrorism that stood in contract to the types of terrorist organizations emerging during the past 15–20 years. Sageman offered a new perspective that allowed countries engaged in counterterrorism to develop new and effective strategies to disrupt or influence dark networks. By using SNA to dissect Al-Qaeda using open source research, Sageman discovered valuable insights that explained their recruitment, evolution, resiliency, and motivations. His research proved that preexisting social ties are usually the precursor for terrorist organizations to acquire new members.[65] If we want to broaden the application of SNA outside of dark networks, we have to look at what these scholars have written and apply those principles to dim networks.

SNA has developed an understanding of the structure of illegal and covert groups by examining the groups' identified relations. When working against covert groups, scholars and policy makers alike categorize groups to identify their goals and motivations. This categorization leads to strategies designed to influence these groups. Whether that influence manifests as tactics to ally with or destroy that organization depends upon the category to which a group is assigned.

---

[64] Jörg Raab, "Dark Networks as Organizational Problems: Elements of a Theory," *International Public Management Journal*, 9, no. 3 (2006), 334.

[65] Marc Sageman, *Understanding Terrorist Networks* (Philadelphia, PA: University of Pennsylvania Press, 2004), 36.

b. Military Doctrine and Publications

Published works on the application of SNA to light networks that exist in a military context are more limited. However, the DOD recently invested in reevaluating how the military wins and fights war doctrinally to ensure it maintains relevancy in the twenty-first century. Two documents were uncovered that illustrated a small advancement in network thinking for the DOD. These useful publications were a Joint Warfighting Center publication titled *Commander's Handbook for Attack the Network* and a Joint Publication 3–15.1, *Counter-Improvised Explosive Device Operations.* Although both publications are getting the U.S. military to think differently and smarter about engaging networks, each title indicates that the emphasis is still focused on threats. The military developed a framework within recent publications labeled Attack the Network (AtN) to better equip deploying units to be more efficient at Counter Improvised Explosive Device operations. The commander's handbook defines AtN as:

> A focused approach to understanding and operating against a well-defined enemy activities—such as terrorism, insurgency, and organized criminal actions—that threatens stability in the operational area and is enabled by a network of identifiable nodes and links.[66]

AtN's methodology discusses the need to synchronize kinetic and nonkinetic targeting, going beyond neutralizing dark networks or threats, to support friendly networks, and influence neutral networks.[67] The handbook provides a detailed description of concepts geared toward engaging, influencing, and eliminating threats within an operational environment—a marked improvement over historical publications originating within the Joint Force. AtN also incorporates SNA methodologies as a means to interdict threat networks. Nonetheless, within the AtN framework, emphasis is placed on engaging and understanding all elements of the human domain. This idea is discussed throughout the publication; however, the conversation on actual procedures to support friendly networks is substituted for interdicting IED threat networks. Although the

---

[66] U.S. Joint Forces Command, *Commander's Handbook for Attack the Network* (Washington, DC: U.S. Government Printing Office, 2011), GL-11.

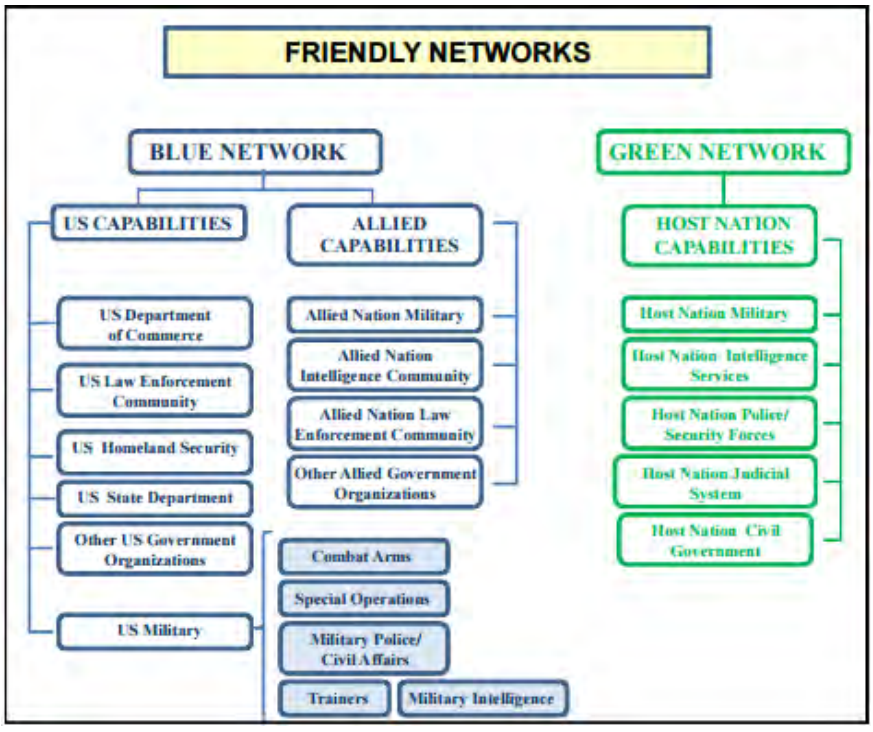
[67] Ibid., i-iii.

handbook is not approved for joint doctrine, Joint Publication 3–15.1 incorporates the ideas fully throughout the Counter Improvised Explosive Device publication.

> To AtN, commanders and staffs must first understand the operational environment in network terms. An important feature of any network is adaptability to a changing environment; one change to a node or link may substantially affect the entire network.[68]

At the time this publication was written and distributed, the wartime focus was on eliminating threats at all costs. The publication centers on a Counter Improvised Explosive Device state but the methodology can be applied appropriately to situations centered on friendly networks as well. The AtN approach breaks down friendly networks into Blue (U.S. and Allied Capabilities) and Green Networks (Host Nation Capabilities) as illustrated in Figure 2.

Figure 2. Friendly networks[69]



[68] Joint Chiefs of Staff, Joint Publication 3–15.1, *Counter- Improvised Explosive Device Operations* (Washington, DC: Department of Defense, 9 January 9, 2012), xi.

[69] Joint Forces Command, *Commander's Handbook for Attack the Network*, II-12.

The Green Network, which is related to the dim network concept in this study, is a key factor to sustaining the Global Special Operations Network and within that network the host nation military, and security forces must be capable at eliminating threat networks they face. In addition, the PSF must be fully partnered with and engaged by the United States, and constantly understood by USSOF to transition from a dim network to light network.

D. CONCLUSION

Because the United States is currently undergoing changes to signal global stability, peacetime engagements will replace major combat operations in the Middle East; therefore, an update to the commander's handbook is necessary. This addition needs to capture how the United States can best engage the various networks across the global stage with a renewed interest in PSF networks. Different units should be analyzed differently depending on their makeup and composition. For example, a tier 1 surgical strike unit will be much smaller compared with a conventional infantry unit. In certain countries, specific host nation partners are chosen simply because of their preexisting mission type or other political reasons. Using metrics to uncover how units compare with each other can save time, manpower, resources, and enhance engagements. SNA tools can be used to differentiate variables determined by the analysts that give more importance to certain attributes over others. However, adding specific weights to different variables should always default back to the theater strategic interests of why that engagement is occurring.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE ANALYSIS OF SNA USE IN DARK AND LIGHT NETWORKS

Chapter II described what networks are, provided an overview of social networks, and outlined the military application of SNA. In Chapter III, we will present two examples of how SNA has been applied to a dark and a light network. By showing its utility in these two networks, we attempt to make the case that with all things being equal, SNA could have the same utility for dim networks. Both cases are unique in their composition. The selected dark network is actor-specific, whereas the selected light network is predominantly organizationally specific. Each network maintains certain characteristics that can be found in PSF networks, both overt and covert. This chapter will identify those characteristics and how they converge and diverge with those characteristics found in dim networks.

A. OVERVIEW

> *"Viewing the detailed structure of a community we see the concrete position of every individual in it, also, a nucleus of relations around every individual which is 'thicker' around some individuals, 'thinner' around others. This nucleus of relations is the small social structure in a community, a social atom."*[70]
>
> —Jacob L. Moreno

The previous chapter described how much of the defense-related research has focused on understanding and mapping terrorist organizations or dark networks. Recently, literature circulating within these communities indicates the importance of the utilization of networks, writ large, to benefit the U.S. government, especially in times of diminishing resources. Some of this literature explores the application of SNA on light networks that exist in an SC context. SNA can help develop an improved consistency in SC by collecting accurate data on friendly networks. Through the tools of this analysis, the influential actors and critical characteristics of organizations can become visible.

[70] Cukier, *Words From Jacob Levi Moreno*, 47–51.

Inside the spectrum of networks, the scale is bidirectional with limits of dark to light. Depending on the purpose of a certain network, it can be categorized anywhere in this spectrum. Dark networks are composed of elements that are both aware and unaware to the nature of the network. The elements that are witting take efforts to conceal their involvement in the network as well as seek to disguise the signature of the network to remain as clandestine or covert as possible. Without a certain degree of knowledge, a person cannot identify that a network exists nor infer that it exists. There are certain identifying features of a dark network that assist in identifying its existence and topographically mapping it.

Networks can be identified by their network topology and by the actions of those in the network, whether or not they are aware of their role within the network itself. Once actors are identified, investigation into their personal connections will further illuminate that network. The goal is to gather enough data to move that network from dim to the dark end of the spectrum or the light end. Until the network is light, it must go through the dim portion of the network. The dim portion characterizes a network that is known to exist but no data or not enough data have been gathered. Dim networks can be both malign and benign networks. This research focused on the friendly networks surrounding SC and labeled them dim networks because of the incompleteness of data on the PSF. From their inception, light networks can exist solely on the light end of the spectrum. Additionally, an overt network with elements that are not witting to the networks structure can exist as a dim network. Connections can be identified and solidified moving that network from a dim network to a light network. SNA principles and measures can progress a network from dark to light and dim to light. Furthermore, at any point in the spectrum, SNA measures can be used to both further illuminate the network and understand the dynamics within the networks topography. The following cases demonstrate this utility for both dark and light networks.

B. DARK NETWORKS

In *Dark Networks as Problems,* Raab and Milward define dark networks as covert and illegal networks.[71] This term can apply to a range of illicit networks, from drug trafficking and blood diamond networks to the terrorist group Al-Qaeda. Dark networks can also include the examples of resistance groups that formed in France during World War II and the Viet Cong. Analysis shows that the organizations are able to adapt and evolve their respective networks based on the external pressures applied to them within their environments. Milward contends that dark networks must be "hyper-flexible" to survive.[72] This characteristic makes the effective targeting of these networks very difficult; however, the advantage dark networks have enjoyed is being eroded through the application of SNA.

1. Noordin Top Terrorist Network

This case study provides a clear and understandable example of a typical dark network that took formed in Southeast Asia, specifically Indonesia. The Noordin Top Terrorist Network was a nebulous network that capitalized on decentralization to conduct numerous terrorist acts in Southeast Asia. Additionally, the application of SNA in this particular case provides a link to its capabilities in influencing the military decision and making process in regards to course of action selection.

Noordin Top, before his death in 2009, was considered the most wanted terrorist in Southeast Asia.[73] He was widely believed to be the self-proclaimed leader of the military wing of Jemaah Islamiya, while maintaining the roles of key financier and bomb maker.[74] In April 2005, Top reportedly claimed that he was the head of the working group for the Malay Archipelago of al-Qaeda.[75] Top has directly been linked to numerous bombings against "Western" targets, beginning with the October 2002 Bali

71 Raab and Milward, "Dark Networks as Organizational Problems: Elements of a Theory,," 334.

72 Ibid.

73 International Crisis Group, *Terrorism in Indonesia: Noordin's Networks*, Asia Report (2006).

76 Ibid.

75 Ibid., 1.

bombing and the Jakarta bombings of the Marriott and the Ritz-Carlton in July 2009.[76] The International Crisis Group (ICG), which states that it is an "independent, non-profit, non-governmental organization committed to preventing and resolving deadly conflict,"[77] published a report chronicling Noordin Top's activities and his use of networks to carry out his vision of global jihad. This report was titled, "Terrorism in Indonesia: Noordin's Networks."[78]

To map, visualize, and analyze Top's networks, students at the Naval Postgraduate School used SNA programs and coded the Noordin Top Terrorist Network Data.[79] These data were taken largely from the ICG report. Primarily, relational data were collected and coded. These data included the group's organizational ties with schools, businesses, religious institutions, and, of course, other terrorist groups. It also included person-to-person ties such as kinships friendships and shared affiliations, such as classmates or being members of the same organizations.

Everton and Nancy Roberts supervised the students that coded the Noordin Top data and have independently continued to research Top's networks. They display their knowledge of these networks as well as their expertise in applying SNA to the particular problem set of dark networks in their article, "Strategies for Combating Dark Networks."[80] In their article, the authors demonstrate how the application of SNA on dark networks can provide military leaders and planners with courses of actions based on a desire approach and kinetic or nonkinetic methods.[81] Additionally, their purpose for

---

76 For a listing of bombings and corresponding reports see http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia.aspx.

77 International Crisis Group, http://www.crisisgroup.org/en/about.aspx.

78 This report can be found at http://www.crisisgroup.org/~/media/Files/asia/south-east-asia/indonesia/114_terrorism_in_indonesia_noordin_s_networks.pdf.

79 Nancy Roberts and Sean F. Everton, Roberts and Everton Terrorist Data: Noordin Top Terrorist Network (Subset), 2011. [Machine-readable data file]. http://www.thearda.com/archive/files/codebooks/origCB/Noordin%20Subset%20Codebook.pdf.

80 Sean Everton and Nancy Roberts, "Strategies for Combating Dark Networks," *Journal of Social Structure* 12, no. 2 (2011): 1–32.

81 Everton and Roberts define the two approaches in their article as follows: "The kinetic approach involves aggressive and offensive measures to eliminate or capture network members and their supporters, while the non-kinetic approach involves the use of subtle, non-coercive means for combating dark networks."

writing the article was to highlight the need of alternate counterterrorism strategies that are "context-dependent rather than letting social network analysis metrics define and drive a particular strategy."[82]

a. Data Structuring

Everton and Roberts used one- and two-mode[83] relational and affiliation network data[84] from the ICG 2006 report. Relational ties consisted of friendship and kinship connections. Affiliation connections consisted of both religious and educational ties. They structured the data along operational ties, trust ties, and institutional-level ties.[85] It is important to note that because the Noordin Top network was labeled a dark network, the analysts assumed that a tie would likely form between two individuals who share a mutual acquaintance and subsequently did not know each other before becoming members of the network. This factor is important because it is necessary to outline specific assumptions before generating networks to limit the possibility of underestimating the number and category of the ties. This is necessary when a network is in the dim portion of the spectrum. Certain assumptions must be made to advance the network through the spectrum from dark to light. Everton and Roberts generated two one-mode networks (operational and trust) at the individual level (Figures 3 and 4) and two one-mode networks (organizational and educational) at the institutional level (Figures 5 and 6).[86]

When analyzing networks, it is necessary to establish a focus or purposes for the analysis. The process of SNA and the plethora of software available that allows this analysis to be conducted are all capable of providing extensive amounts of information.

---

82 Everton and Roberts, *Strategies for Combating Dark Networks*, 8–9.

86 In social network analysis, the term "mode" refers to a class of entities also known as actors, nodes, or vertices. A one-mode network consists of a single set of actors and direct contact. All actors are the same type (people, organizations, etc.). Two-mode networks consist of ties between two sets of actors from different classes, where the ties are across classes (affiliations or events).

84 Everton and Roberts, *Strategies for Combating Dark Networks*, 9.

85 For more detailed information about each type of relation used, please see Everton and Roberts, *Strategies for Combating Dark Networks*.

86 Everton and Roberts, *Strategies for Combating Dark Networks*, 9.

Focusing the analysis on aspects of the network that can drive a decision is important, especially with regard to a covert network that you seek to disrupt, destroy, or otherwise influence. Everton and Roberts provide examples of this focus by way of establishing possible courses of actions one might develop for attacking a dark network.

b. Data Analysis

Everton and Roberts present four different courses of action for the purposes of demonstrating the utility of SNA. The courses of action were broken down into two that focus on a kinetic approach and two on a nonkinetic approach. Within the kinetic and nonkinetic approaches, each was broken down further into a course of action for an individual network and an organizational network focus. For the purposes of this case study, the focus will be on the individual for both nonkinetic and kinetic courses of action. The strategies for the organizational networks are similar enough to the individual networks that the concepts used are virtually the same: identify the most influential nodes.

The first course of action was nonkinetic and focused on the individuals in the operational network. The purpose of this course of action was to implement a psychological operations strategy in order to influence the network toward some ends or disseminate a disinformation plan. Essential to any effort to pass information is the level of influence or interaction that a node—or person, in this case—has in the network. More specifically, a node with a high betweenness centrality score theoretically has the capability to reach the most nodes at the quickest rate because of the assumption that the information follows the shortest path length. As presented in Table 1, the names in bold represent the eight individuals that rank in the top ten of all four centrality measures. Using these data, a planner could conceptually develop a strategy to target these individuals and have a reasonable degree of certainty that they are targeting the most influential individuals. When visualized in Figure 7, the planner could also identify these individuals; however, it is recommend that the table and sociograms be used together to maximize the understanding of the network and its nodes within the context of the analysis.

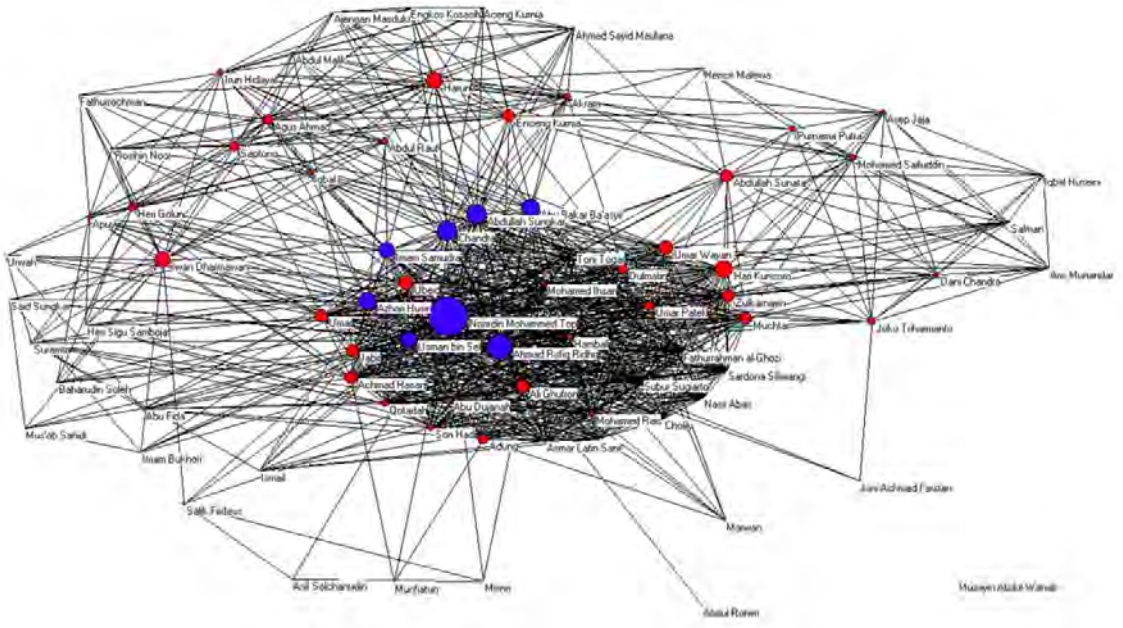
The next course of action is kinetic and focused on the individuals in the trust network shown in Figure 4. Typically with kinetic operations, the goal is to remove a node from the network, usually through force. Because of the finality of kinetic operations, it is important to understand and be aware of possible second- and third-order effects. Once these effects are taken into consideration, the target list can be prioritized.

Table 1. Top ten individuals in the operational network (by score)[87]

Degree	Closeness	Betweenness	Eigenvector
Noordin Top (74.36)	**Noordin Top** (.802)	**Noordin Top** (14.88)	**Noordin Top** (25.97)
Azhari Husin (58.97)	**Azhari Husin** (.713)	**Ahmad Rofiq Ridho** (5.70)	**Azhari Husin** (25.89)
Chandra (58.97)	**Chandra** (.713)	**Chandra** (3.68)	**Chandra** (24.63)
Abdullah Sungkar (57.69)	**Abdullah Sungkar** (.706)	**Abdullah Sungkar** (3.43)	Ubeid (24.39)
Abu Bakar Ba'asyir (56.41)	**Abu Bakar Ba'asyir** (.700)	Hari Kuncoro (3.12)	**Imam Samudra** (24.37)
Ahmad Rofiq Ridho (56.41)	**Ahmad Rofiq Ridho** (.700)	**Azhari Husin** (3.00)	**Abdullah Sungkar** (24.36)
Imam Samudra (55.13)	**Imam Samudra** (.694)	**Abu Bakar Ba'asyir** (2.86)	**Abu Bakar Ba'asyir** (24.27)
Ubeid (55.13)	Ubeid (.694)	Iwan Dharmawan (2.73)	**Usman bin Sef** (24.25)
Usman bin Sef (55.13)	**Usman bin Sef** (.694)	**Imam Samudra** (2.42)	**Ahmad Rofiq Ridho** (24.06)
Hari Kuncoro (53.85)	Hari Kuncoro (.688)	**Usman bin Sef** (2.41)	Umar Wayan (24.01)

[87] Ibid., 11.

Figure 3. Operational network (betweenness centrality) [88]



In this case, the target list is developed through processing the members of the trust network along the four-centrality measures (Table 1). The results are in stark contrast with the members in the operational network result. Three actors in this network are consistently in the top ten of each centrality measure. Interestingly, Noordin Top is not the most central. One would logically suspect that Noordin Top would be highly central in all the networks based on his position in the overall network. This is a strong example of the diversity of results SNA provides. When this network is visualized (Figure 4) and the three most central actors are highlighted (blue icons circled in black), it becomes apparent that their position is important because of how they connect the core of the network to the periphery.[89] When presented with this information, a planner or targeting officer would have reasonable certainty that eliminating the three most central actors would temporarily disconnect the core from the periphery. This action could limit the core network's ability to be effective in conducting terrorist activities.[90]

[88] Ibid., 13.

[89] Ibid., 17.

[90] Ibid., 17.

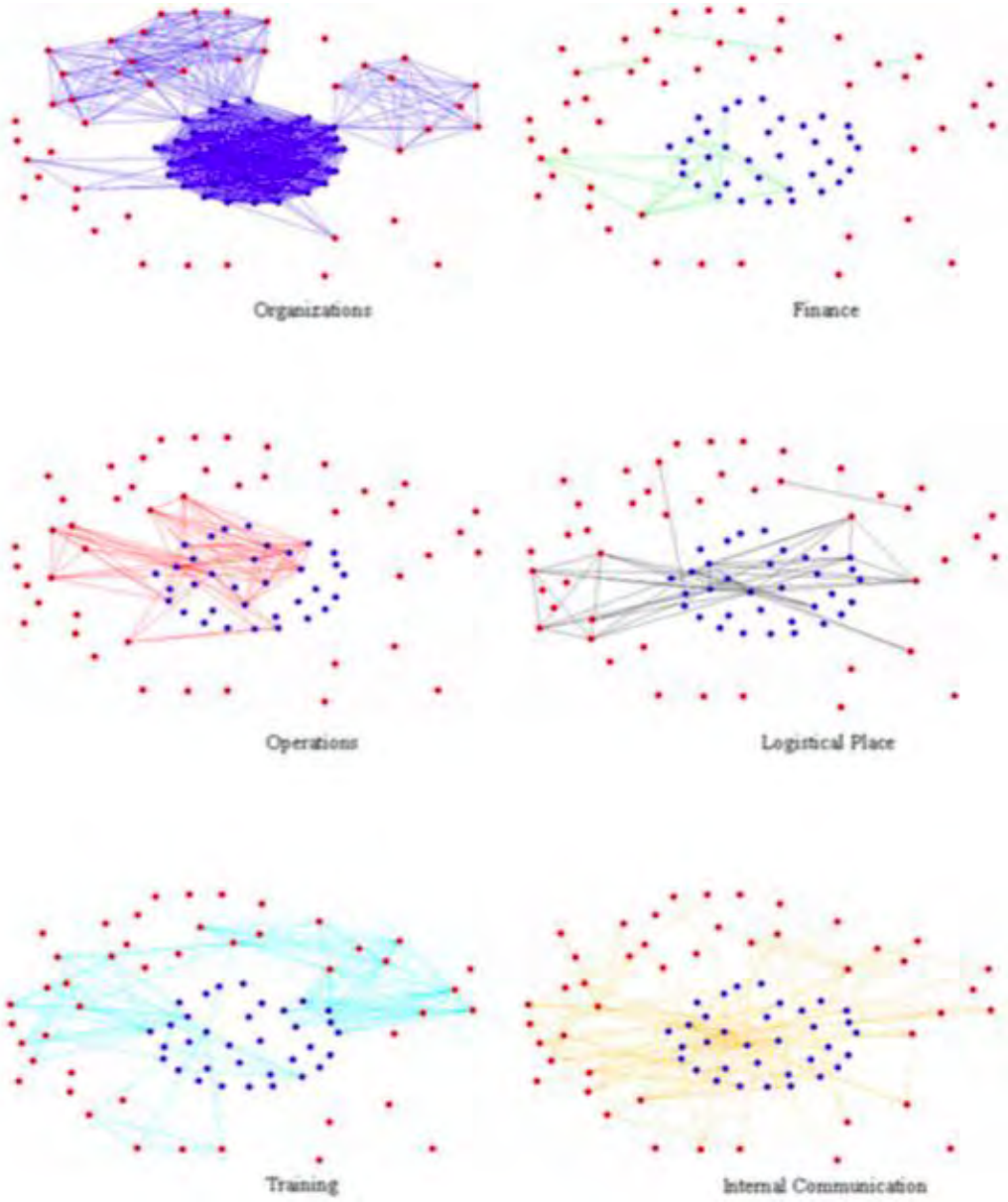
Table 2. Top ten individuals in the trust network (scores in parentheses)

Degree	Closeness	Betweenness	Eigenvector
Ahmad Rofiq Ridho (29.49)	**Ahmad Rofiq Ridho** (53.60)	**Ahmad Rofiq Ridho** (19.41)	Mohamed Rais (35.64)
Adung (28.21)	**Ubeid** (50.76)	Iwan Dharmawan (17.25)	Tohir (35.64)
Jabir (28.21)	Adung (48.91)	Abdullah Sunata (10.87)	Jabir (34.70)
Mohamed Rais (28.21)	Mohamed Rais (48.55)	**Ubeid** (8.46)	Adung (34.30)
Tohir (28.21)	Tohir (48.55)	Noordin Top (8.13)	Asmar Latin Sani (34.22)
Son Hadi (26.92)	**Son Hadi** (47.86)	Adung (7.15)	**Son Hadi** (33.83)
Ubeid (26.92)	Jabir (47.52)	Usman bin Sef (6.27)	**Ubeid** (33.54)
Asmar Latin Sani (24.36)	Asmar Latin Sani (46.53)	**Son Hadi** (4.59)	**Ahmad Rofiq Ridho** (33.42)
Suramto (24.36)	Suramto (46.53)	Akram (4.58)	Suramto (33.25)
Zulkarnaen (23.08)	Zulkarnaen (45.58)	Zulkarnaen (4.33)	Fathurrahman al-Ghozi (32.50)
	Noordin Top (45.58)	Agus Ahmad (4.33)	Toni Togar (32.50)

Figure 4. Trust network (core in blue; periphery in red)[91]

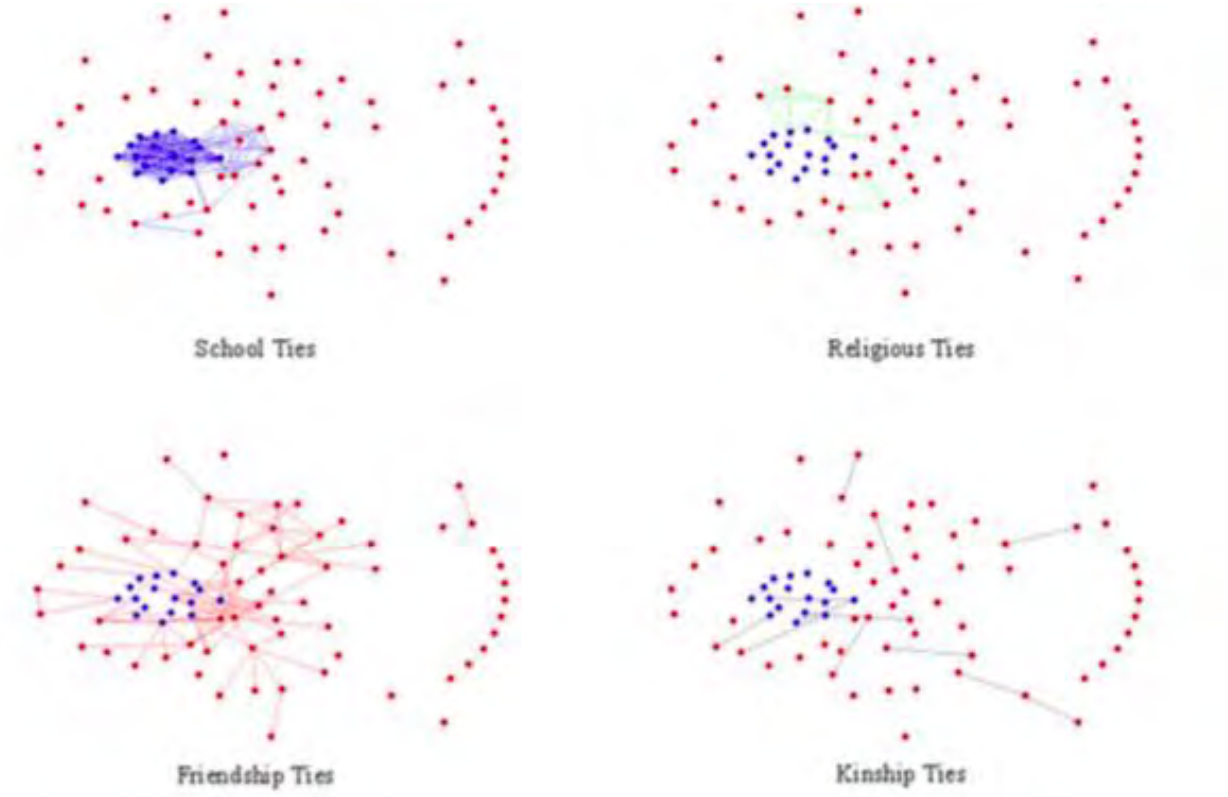
[91] Ibid., 17.

Figure 5. Noordin Top's operational network[92]



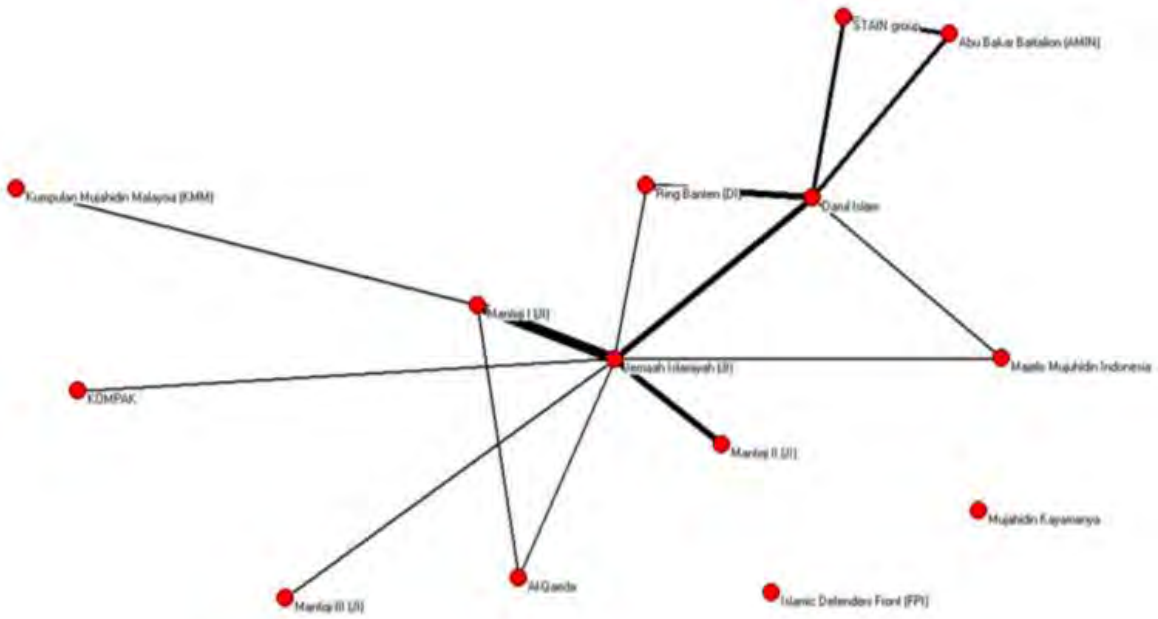
92 Ibid., 15.

Figure 6. Trust network[93]



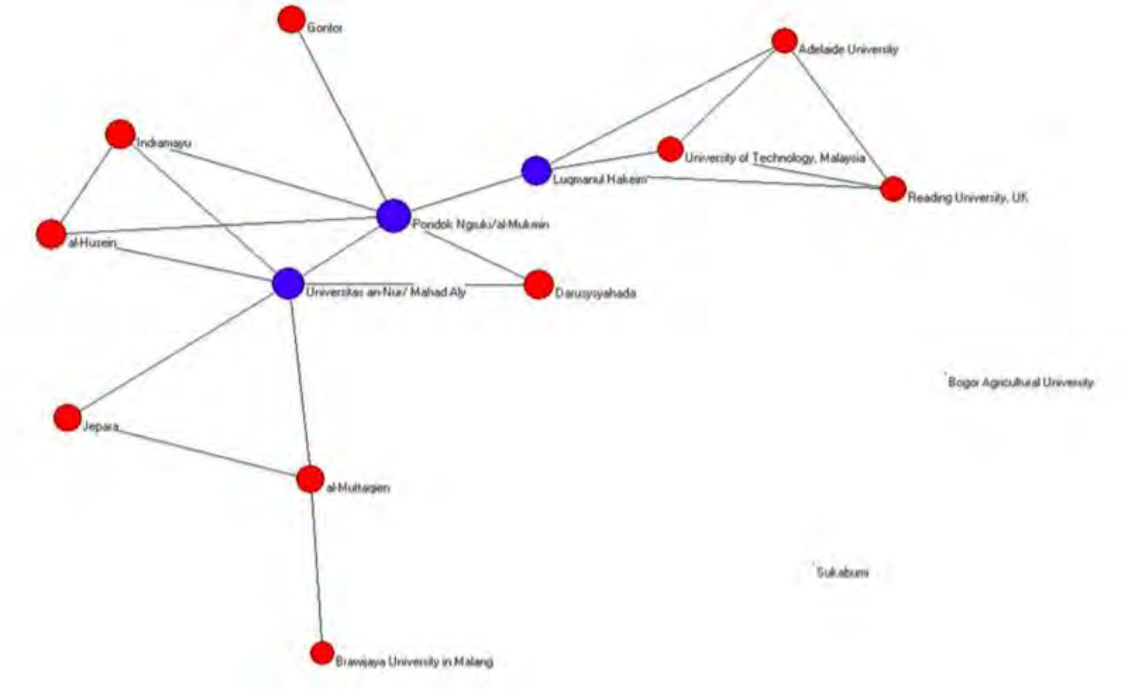
93 Ibid., 19.

Figure 7. Terrorist organizational network[94]



[94] Ibid., 16.

Figure 8. Terrorist education network[95]



[95] Ibid., 21.

2. Summary

The study of Noordin Top's terrorist network provides a clear example of the utility of SNA in illuminating a dark network. Everton and Roberts' article provides excellent examples of the characteristics of dark networks and how SNA tools can turn scattered data points, such as kinship ties, into focused results. Connecting these results to defined courses of action shows how understanding the network through the context of centrality provides a planner with insight necessary to craft a kinetic or nonkinetic targeting strategy.

A central theme within dark networks is information needed to illuminate their networks are hidden and covert. There is no single strategy that can eliminate dark networks because of their ability to adapt and evolve past the point of extinction. However, methodologies do exist that allow strategists to increase their chances of designing efficient and effective ways to eliminate the threats posed by these groups. In the case of Noordin Top's network, the uncovered data created insight into their network structure and network characteristics. Centrality is salient in this example; however, other aspects of network analysis assisted in the development of courses of action. One such aspect is the measurement of the network's density. Network density describes the number of potential connections that exist a network that are actual connections. The aggregated density score of the operational network was 0.307. Compared with the trust network (0.84), the operational network is more dense. Identifying the density of networks further allows the planner to determine where to invest more effort and resources, depending on the desired outcome. In this case, the planner could assume that effects could be achieved faster by targeting the operational network because of its higher number of actual connects. More identified connections could mean more opportunities for exploitation and a higher threshold for the risk of failure.

C. LIGHT NETWORKS

This section will focus on a light network, its characteristics, and the utility of SNA in developing a strategy for that network. Literature surrounding the SNA field is filled with examples of the benefits of understanding overt networks. As such, "Bright

networks, that is, a legal and overt governance form that is supposed to create advantages for the participating actors and to advance the common good and does not—at least intentionally—harm people,"[96] are open and accessible. The reason these organizations are easy to study is due to their openness in society, which allows them to be successful and/or survive. Light networks, such as the United Nations, consist of actors or organizations that seek out connections and understand their importance for the overall success of the network. Light networks can also exist without the actors within them knowing they are connected or actively seeking to leverage that connection. Fans of a professional sports team openly advertise their affiliation with that team. The fans are all mutually connected through this affiliation, but do not necessarily operate as a cohesive network outside of this shared allegiance to the team.

Concepts surrounding this discipline continue to reflect that relational ties and network characteristics can indicate significant meanings within that network, as Raab and Milward state: "If covert networks, like overt networks, are also characterized by a need to integrate functionally or geographically differentiated elements, then the most likely way to disrupt them is to attempt to find the link that joins as many of these differentiated elements as possible."[97] A fundamental approach to forming concrete military alliances around the world is to determine how these alliances are held together and what is potentially missing within these military partnerships. Consequently, because of the military and security applications of SNA being mostly dedicated to dark networks, approaches to light networks are lacking. However, this trend is beginning to change.

The next case demonstrates how understanding light networks is increasingly important in environments where all actors are linked in one-way or another. In addition, this case identified a shortcoming in the military study of light networks. The study of the humanitarian assistance networks in Tajikistan provides a great example of a dim network that progresses to a light network. What sets the network apart from a dark network and is that the organizations in this network are overt and advertise their relationships so collection methods must be developed for it differently. Actors do not

96 Raab and Milward, 419.

97 Ibid., 435.

always realize they are in a light network, so data necessary to map these networks out can be collected relatively easy through normal interactions during engagements.

1. Humanitarian Assistance Networks in Tajikistan

This case provides a clear and understandable example of a dim network that existed in Central Asia that was illuminated into a light network. Tajikistan was the poorest state in the former Soviet Union. Consequently, after the fall of the Soviet Union, Tajikistan has remained one of the poorest countries in world.[98] Being a second-world developing country, numerous organizations operate in Tajikistan to provide aid and assistance due to widespread poverty.

Two U.S. Army Civil Affair officers, Majors Jeff Han and Ryan Schloesser, identified the humanitarian assistance network in Tajikistan. These officers wanted to improve Civil Military Support Elements (CMSE) capabilities in meeting Civil Military Engagement objectives in Tajikistan. CMSEs "build partner capacity in a preventive, population-centric, and indirect approach to enhance the capability, capacity, and legitimacy of partnered indigenous governments."[99] CMSEs typically collaborate with numerous humanitarian organizations both international and local to address population grievances that exist in the host nation. Han and Schloesser recognized that for CMSEs in Tajikistan to be effect, they must identify the most relevant actors in the humanitarian assistance network. The network that they mapped had numerous different forms of nodes. This included NGOs, intergovernmental organizations, domestic governmental organizations, religious charities, and financial and commercial organizations. Han and Schloesser understood that a network existed that CMSEs could leverage to optimize their engagement strategies. This network is a good example of our dim network concept.

The purpose for Han and Schloesser's research was not only to develop the humanitarian assistance network, but also to use the results of SNA to help develop different strategies for advancing the capabilities, capacity, and legitimacy of partnered

[98] *Global Finance* lists Tajikistan as the thirty-third poorest country in the world in 2015. https://www.gfmag.com/global-data/economic-data/the-poorest-countries-in-the-world?page=12.

[99] U.S. Army. *ATP 3–57.80: Civil Military Engagement* (Washington, DC: Department of the Army, 2013), 4–1.

indigenous governments. Through the use of SNA-produced metrics, they were able identify the most influential actors in the network and leverage those actors to suit a specific strategy.

a. Data Structuring

The research set out to identify the most influential organizations within the unmapped humanitarian assistance network of Tajikistan. Second, it seeks to answer what strategy can USSOF units, specifically Civil Affairs teams, implement to sustain long-term stability in Tajikistan? To accomplish this, researchers Han and Schloesser began by conducting open source research to list the organizations that fit this category, and then categorized any relevant connections the listed organizations displayed on their websites. It is important to note that their approach used relational ties that were overt and openly disclosed. This is a key characteristic of a light network; however, before these ties are analyzed and mapped, the network remains dim.

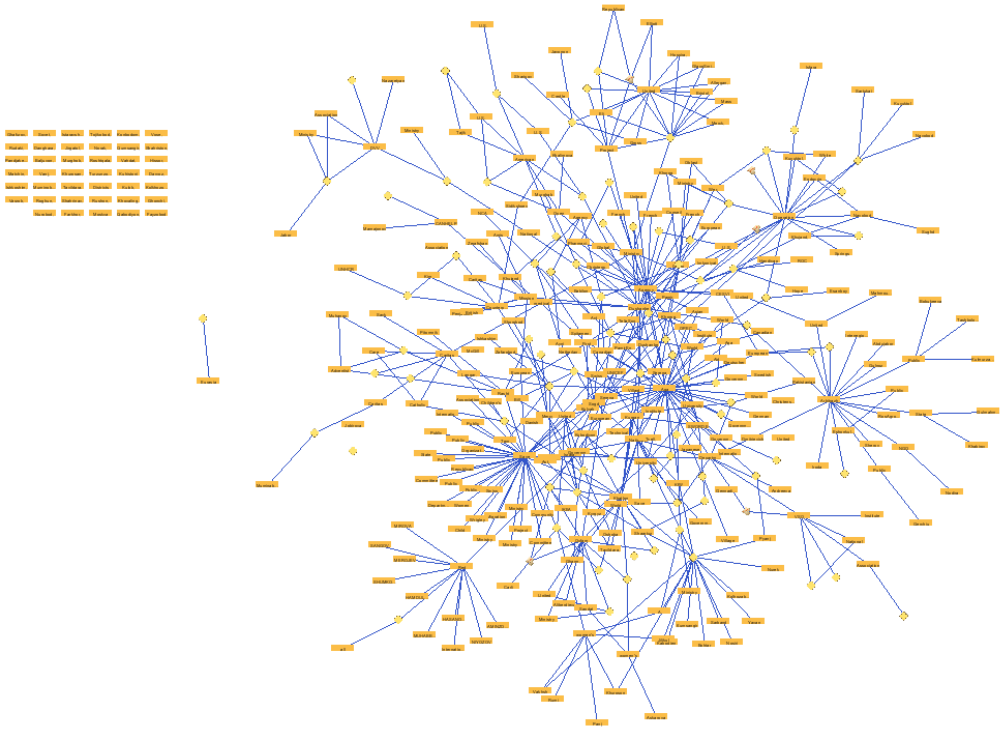
Moving the network from dim to light required searching the Internet for any missing information they could not obtain from the organizations websites. They used Palantir-developed software that takes data from multiple sources and fuses the data into human centric models. Palantir data analysis software was used to "tag" or highlight the relevant information from the open-source research that amounted to: "308 entities, 97 of which are location types, 166 are organization types, 42 are individuals, and 169 are event types."[100] Figure 9 illustrates the complex humanitarian network formed after the relational ties were input into Palantir. The blue lines indicate relational ties between two nodes, and the orange icons represent the nodes, or an individual humanitarian organization, individual, event, or location. This link analysis graph indicates that several nodes have significantly more connections as compared to other nodes. There are also isolates, or nodes, that share no observed ties to any other node in the network.

[100] Jeffrey Han and Ryan Schloesser, "Joining the Helping Hand: Understanding the Humanitarian Assistance Network in Tajikistan" (unpublished paper Naval Postgraduate School, 2014), 5.

b. Data Analysis

To answer the research question pertaining to the humanitarian network, the researchers were required to only focus on the social network with the same class that included only organizations. They isolated the other nodes (events, locations, and individuals) and the present network included 168 organizations or nodes.[101] This was to determine which organization within this network was the most influential based on its network characteristics and its scores across various SNA metrics.

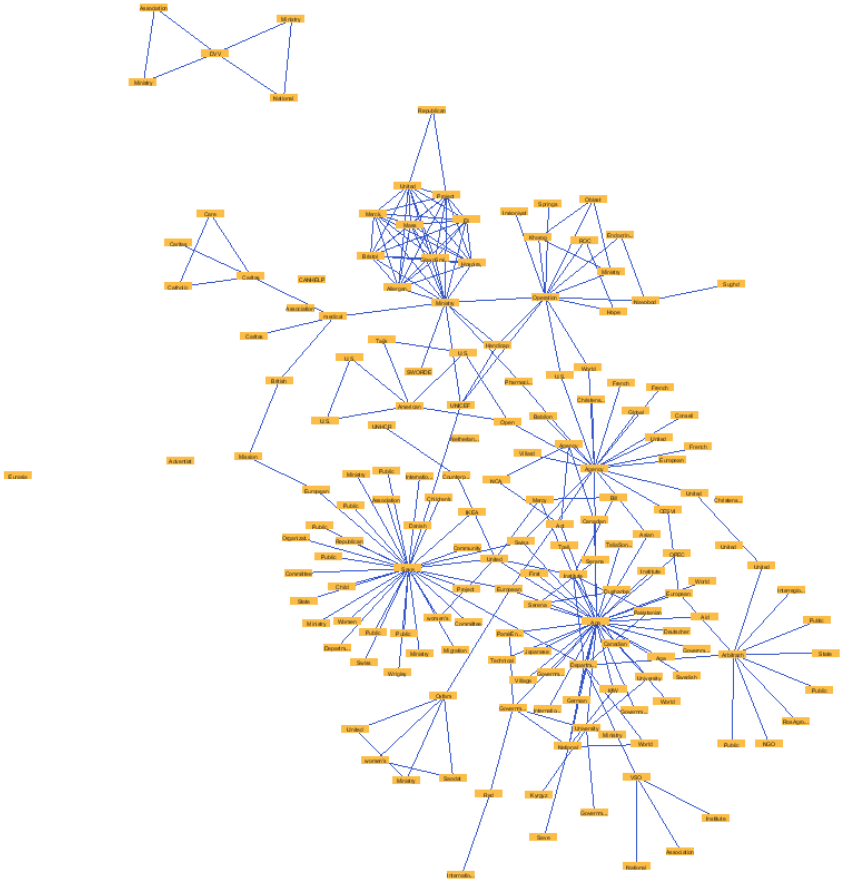
Figure 9. Tajikistan humanization assistance link diagram[102]



[101] Ibid., 8–9.

[102] Ibid., 7.

Figure 10. Sociogram of humanitarian assistance organizational social network[103]



First, by observing the sociograms illustration, they were able to identify the most central organizations within the network. Those central organizations can be extremely influential and powerful based on their structural location. Second, they ran metrics to see if the scores corresponded to the initial observations using the four-centrality measures: Degree, Betweenness Centrality, Eigenvector Centrality, and Closeness Centrality.[104] Both the sociogram and the SNA metrics indicated the most influential humanitarian networks within Tajikistan.

[103] Ibid., 11.

[104] Ibid., 12.

Table 3. Humanitarian assistance network centrality measures

Degree Centrality

Rank	Organization Name	Deg Raw	Deg Scale
1	Aga Khan Development Network (AKDN)	39	1.00
2	Save the Children	35	0.89
3	Agency for Technical Cooperation and Development (ACTED)	20	0.50
4	United States State Department	19	0.47
5	Ministry of Health, Tajikistan	17	0.42
6	Operation Mercy	14	0.34
7	Project HOPE	13	0.32
8	Department for International Development (DFID)	11	0.26
9	Arbitrazh	10	0.24
10	Bristol-Myers Squibb, Pharmaceutical Company	10	0.24

Closeness Centrality

Rank	Organization Name	Close Raw	Close Scale
1	DVV International	1	1
2	Ministry of Labour and Social Protection, Tajikistan	0.67	0.60
3	National Adult Education Centre	0.67	0.60
4	Ministry of Labor, Tajikistan	0.67	0.60
5	Association for Scientific Technical Intelligence (ASTI)	0.67	0.60
6	Aga Khan Development Network (AKDN)	0.39	0.27
7	Agency for Technical Cooperation and Development (ACTED)	0.38	0.26
8	Save the Children	0.38	0.26
9	Department for International Development (DFID)	0.37	0.24
10	European Community Humanitarian Office (ECHO)	0.36	0.24

Betweenness Centrality

Rank	Organization Name	B/W Raw	B/W Scale
1	Aga Khan Development Network (AKDN)	5269.19	1.00
2	Save the Children	4833.25	0.92
3	Agency for Technical Cooperation and Development (ACTED)	4131.88	0.78
4	Ministry of Health, Tajikistan	2455.86	0.47
5	Department for International Development (DFID)	2167.76	0.41
6	UNICEF	1647.86	0.31
7	Operation Mercy	1544.04	0.29
8	European Community Humanitarian Office (ECHO)	1209.77	0.23
9	Pharmaciens Sans Frontières Comité International (PSFCI)	1207.96	0.23
10	Arbitrazh	1120.36	0.21

Eigenvector Centrality

Rank	Organization Name	Eig Raw	Eig Scale
1	Aga Khan Development Network (AKDN)	0.08	1
2	Save the Children	0.07	0.88
3	Agency for Technical Cooperation and Development (ACTED)	0.04	0.48
4	United States State Department	0.03	0.40
5	Ministry of Health, Tajikistan	0.03	0.36
6	Operation Mercy	0.02	0.31
7	Project HOPE	0.02	0.27
8	Department for International Development (DFID)	0.02	0.27
9	Arbitrazh	0.02	0.24
10	National Social Investment Fund of Tajikistan (NSIFT)	0.02	0.21

Highlighted in yellow is the Aga Khan Development Network. It consistently ranked at the top of each centrality measure. Han and Schloesser identified that the top five actors in closeness centrality were all members of the Institute for International Cooperation of the Deutscher Volkshochschul-Verband e.V. sub-network listed as DVV

International (indicated by the red outline). Therefore, the actual position of the Aga Khan Development Network could be assumed to be higher than its listed position as sixth in closeness centralization. Save the Children and Agency for Technical Cooperation and Development are also dominant in their centrality. These organizations are prominent NGOs that are chartered to provide certain services to address grievances and shortcomings of the host nation. The results produced through SNA provide CMSEs with the necessary focus to develop a strategy that leverages the influence these organizations maintain in the humanitarian assistance network.

2. Summary

The analysis of the humanitarian network in Tajikistan provides a concise example of how to transition a dim network to a light network as well as the utility of SNA when applied to a light network. In addition to providing insight into the level of influence certain NGOs have within the network, the study showed how mapping the network could lead to additional understanding of a complex environment through the identification of other substantial actors previously thought to be non-influential. These include domestic and international governmental organizations. Han and Schloesser showed that the belief that NGOs and charities were the sole agencies conducting humanitarian efforts to be untrue in this case. Similarly, many PSF units are believed to have a certain level of influence in security matters and are therefore targeted for continued partnership.[105]

This research demonstrated that mapping out the human domain in steady-state operations is essential to future USSOF operations. They drew on an existing model for adapting social movement theory into USSOF operations as a requirement to be able to effectively analyze existing networks, which in turn will effectively build USSOF networks.[106] As a sample network, they analyzed indigenous organizations. Within

105 In some instances, that perception is perpetuated by the host nation despite the truth that the unit in question is mostly ceremonial. This is ironically the case with certain Tajik military units. One such unit is the Tajik National Guard. Despite the unit's title, it is the private guard of the president of Tajikistan.

106 Han and Schloesser, "Quantifying the Indirect Approach: Understanding and Applying Network Development in Special Operations" (Thesis: Naval Postgraduate School, March 2015).

indigenous organizations, there are members, established structure of solidary incentives, communication, and leaders. By looking at these organizations from a network theory perspective, analysts could determine motivations of its members. For example, when participants believe the system they were part of was unjust and open for change, they are likely to mobilize and join some of the anti-state establishments.[107] This represented an advanced position to use network characteristics to achieve stable USSOF networks that have the ability to manipulate their environment when needed.

3. Relevance to Research

Although both studies analyze different networks, the techniques and tools can be used to examine all type of networks. The benefit of studying friendly networks is that information about the organizations is usually open, not hidden, and can be routinely collected during engagements. The dark and light network cases indicate that the more reliable information one has, the more one will understand about that network and the entirety of the operating environment. These networks begin as dim networks. Identifying the actors through their actions or events they are involved in is critical to moving the network from dim to light or dim to dark.

Gathering the data necessary to map a dark network differs from gathering the data for a light network. The covertness of the dark network limits the available sources for mapping this network through noninvasive means. Certain intelligence and information-gathering techniques may have to be used to gather the necessary information to map a dark network. However, once certain actors or events are identified, open-source research becomes more effective. Consequently, because of most intelligence requirements being focused on dark networks, data collection though intensive labor is less difficult. Open-source information on light networks tends to be more available through most mediums such as the Internet and publications. The openness of light networks allows for greater availability of information. Additionally, because of the openness of light networks, overt information-gathering techniques can be

107 Doug McAdam, *Political Process and the Development of Black Insurgency*, *1930–1970* (Chicago, IL: University of Chicago Press, 1982), 32.

used to obtain more detailed information on operational and relational ties. However, because of the emphasis placed on dark network–related information and intelligence, reporting these ties about light network actors is not a priority.

Once a network is believed to exist and at least two or more actors are identified, the network should be considered dim. Additional significant properties that characterize dim networks will be discussed in the proceeding chapters. Based on the actions of the actors, a determination can be made as to which side of the spectrum the network will move toward; bad to dark, good to light. With this being the case, when a dim network is identified, the analyst must initially fuse data gathering techniques from both dark and light networks to begin to map the identified network.

Networks largely consist of people, relationships, and boundaries but can also be other things as well. To understand how these elements relate to one another for the creation of a network, certain steps must be completed. When SNA is applied to network development, it illustrates how particular dynamics within a network represent opportunities to leverage and influence based on connections, fractions within the network, and or the networks structural location. However, correct data about the organization under study must be obtained to prevent improper analysis from occurring.

IV. PSF DIM NETWORK CASE

> *"You can't attack a network with a field army. Instead, it takes a willingness to field a nimble, networked force of your own."*[108]
>
> —Dr. John Arquilla

Chapter III presented two case studies to illustrate how dark and light network characteristics can be applied to SNA of dim networks. The techniques identified in the previous chapter's case studies will be used to understand organizational networks involved during a crisis surrounding a specific incident in the Philippines involving U.S. PSFs. This case will indicate what steps will need to be implemented to effectively integrate a SNA methodology into security cooperation events. This chapter will analyze the crisis to identify how understanding the dim networks of the partner security force could have aided the efforts of the Government of the Philippines (GPH). Additionally, this chapter will present themes identified from current reporting requirements that should be refocused toward peacetime operations.

An overview of the 2013 Zamboanga City Crisis and precipitating events will be presented as a case study, followed by a description of how SNA could strengthen the understanding of dim networks surrounding this incident. A significant amount of SC events have been executed in the Philippines. This chapter will discuss what information would be needed to map and understand friendly networks using SNA by examining USSOF data collection methods. Additionally, the case study will be further analyzed to illustrate missed opportunities and how an understanding of the friendly dim network could be leveraged to shape better outcomes.

Dim is a description of the state a network is in based on the data available. This neutral state is the transitional position of both dark and light networks. The identification of a dim network is similar to that of a dark network. In the context of an overt or friendly network, dim is the state in which a perceived network exists if that network is not known

108 Arquilla, "How to Win," *Foreign Policy.*

to its actors but only to the outsider looking in. PSF networks exist in this portion of the spectrum. An SC planner knows that the PSF units in a certain country such as the Philippines work together for numerous purposes. These purposes can be security enforcement missions, humanitarian assistance, disaster relief, or training. The planner can identify these events, and they can then begin to build a network outlining the connections each PSF unit has to one another as well as outside organizations. Incrementally, the planner, through mapping the network, moves it through the spectrum from dim to light.

A. PSF IN THE PHILIPPINES

The DOD, and most recently U.S. Special Operations Command, has maintained a long history of cooperation with the Armed Forces of the Philippines (AFP). The contextual background of this relationship is by far too extensive to detail in this chapter; however, the recent relationship will be discussed as it pertains to the methodology forging the proposed framework. USSOF has advised and assisted the AFP's counterterrorism campaign. This relationship extends far beyond the extensive training programs created and developed for the AFP but spreads to operational support. Recently, USSOF advisors have been embedded with AFP USSOF units to ensure this support shapes the progress of the Philippine Internal Peace and Security Plan where the AFP transition to external border security and the PNP focus on internal security of the country. During this transition, USSOF have also been working with PNP Special Action Forces as they increase their respective security role, while developing partnerships with governmental and NGO agencies in the Southern Philippines to ensure the reasons that lead to the insurgency problem are appropriately addressed.

In theory, understanding and leveraging networks in a foreign country are cornerstones of USSOF missions. However, more often than not USSOF teams have high turnover rates of personnel and over time, specific missions can shift to other teams or even to different companies, battalions, or groups. When this occurs, the personal knowledge and understanding pertaining to specific networks can be lost and/or buried in outdated and obsolete reporting that could potentially never resurface again. What is

needed is a tangible output that transcends all types of reporting and remains important from the value of its analysis. SNA can be used to bridge the gap needed to understand environments in which USSOF operators are embedded to overcome the problems created from the current reporting mechanisms and swapping of the unit personnel. As the United States invests considerably more resources in foreign partnerships, peacetime engagements will undoubtedly increase as cost-effective ways to increase these partnerships and maintain stability in the area.

Recent military relations between the countries include both enduring engagements from the combat advisory mission of the Joint Special Operations Task Force – Philippines (JSOTF-P) to episodic engagements underneath a theater security cooperation program. According to David Rothkopf in his article in *Foreign Policy*, "Does America Need New 'Special Relationships'?" forming new and influential relationships has to begin by looking at existing alliances and revitalizing them to meet current times.[109] Capacity building is used to project U.S. influence in particular areas and deter acts from malevolent actors. The United States can create these special relationships using focused military capacity-building efforts. Additional by-products of military advising and assisting are an enhanced understanding of the operating environment. To develop long-term and sustained influence after the departure of U.S. Forces, a comprehensive understanding of the environment is necessary. PACOM via JSOTF-P has been successful working with the GPH primarily through the PSF to improve its capacity to combat terrorism throughout Mindanao while attempting to establish USSOF networks. However, what was missing was a comprehensive understanding of how the partner forces are interconnected with each other. Malevolent actors have far less freedom to maneuver compared with what was available before 2001; nonetheless, they persistently operate throughout the Philippines challenging the national government.

109 David Rothkopf, "Does America Need New 'Special Relationships?' "*Foreign Policy*, August 4, 2015.

B. ZAMBOANGA CITY CRISIS BACKGROUND

The GPH has been involved in a long peace process with the Moro National Liberation Front (MNLF) in Southern Mindanao, the Philippines. In 1996, an agreement between both parties created the Automatous Region in Muslim Mindanao. Nur Musari, then-chairman of the MNLF, became the Automatous Region in Muslim Mindanao's first governor in 1996, serving through 2002.[110] Most recently, the GPH has been involved with peace talks with the Moro Islamic Liberation Front, a splinter group of the MNLF. Factions within the MNLF have viewed the Moro Islamic Liberation Front-GPH peace talks negatively over concerns of derailment of the 1996 agreement. On September 9, 2013, rogue MNLF Elements (Rogue Moro National Liberation Front Element [RME]) led by commander Ustadz Habier Malik staged an attack in Zamboanga over this dissatisfaction.[111] The crisis provides an example of a joint operation that the local and national government, security forces, and NGOs worked together to end. The question remains whether this situation provides opportunity to study network structure and network characteristics of the friendly forces surrounding the incident to create the framework needed to fully integrate this approach into future SC events.

C. OBSERVATIONS FROM ZAMBOANGA CITY

The Zamboanga City Crisis was a unique situation because it occurred during a time when JSOTF-P's mission was ending due to the Philippine military gains in combating terrorism across Southern Mindanao. This incident represents the evolution of the AFP's capabilities while demonstrating to the United States the importance of truly understanding military networks. The devastation caused by the RME and the complicated bureaucratic operations resulted in a 3-week siege.[112] Several things can be observed about communication and relational ties during the crisis that reveal something that can be done better. Primarily, a well-synchronized and collaborative effort at the

110 Carmela Fonbuena, "Zamboanga Siege: Tales from the Combat Zone, September 13, 2014. http://www.rappler.com/newsbreak/68885-zamboanga-siege-light-reaction-battalion.

111 Ibid.

112 The author was assigned to JSOTF-P during this incident and provides first-hand information to cover any gaps that the research was unable to fill.

individual and organizational level is needed for an effective response to a crisis situation. Unfortunately, both the GPH and JSOTF-P did not have the information necessary to illuminate the dim networks involved.[113]

The presence of these dim networks directly validates the counterterrorism focus of both the host nation and JSOTF-P from 2001 to the present. There was a lack of information available to government and U.S. forces to illustrate how the recovery and security organizations on the ground were networked, both independently and collectively. Significant planning delays resulted because of the time it took to gather information about who was involved, what their capabilities were, and what their specific roles would be. Equally important, there was no mechanism to foster collaboration amongst agencies. This lack caused several days of inaction where the RME were able to strengthen their fighting positions and the AFP and PNP awaited a political solution. If the past SC events executed in the Philippines had collected this information, the typical Filipino response network could have been mapped out using SNA software. This analysis would supplement the decision making of the host nation to prevent delays in their response to the crisis.

The lack of knowledge about the PSFs' networks was mitigated by JSOTF-P's presence in Zamboanga. The Light Reaction Companies (LRC)[114] was instrumental in the success of the operation. Through persistent engagement and training by USSOF, the LRC's developed the capability and capacity to conduct hostage rescue operations, close quarter combat, and precision marksmanship. These capabilities answer the question about the ability of the partner force to successfully respond to a crisis situation but failed to account for how this happened from a network perspective.

113 This is strictly limited to an SNA context. There was a lack of sufficient information to make the connections of the security forces to external organizations. Additionally, little information about individual and organizational network characteristics was known.

114 The LRC are a Philippine special operations unit created and trained by USSOF.

Figure 11. Sample network of organizations involved during Zamboanga City crisis created in Palantir[115]

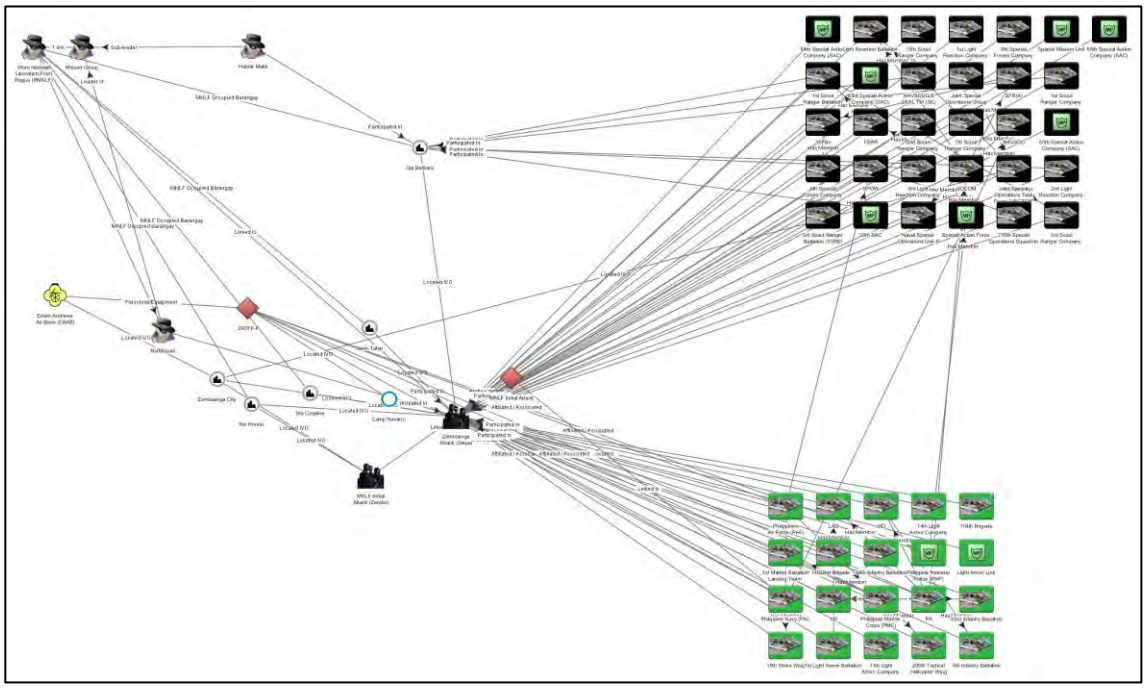
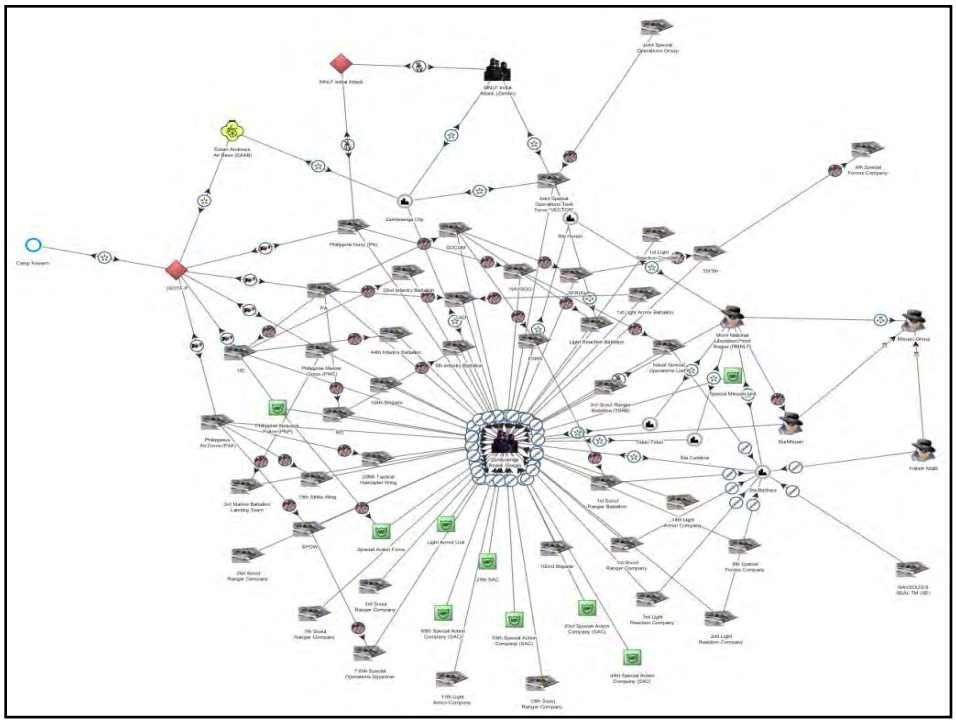


Figure 11 is a network of the PSFs involved during the crisis. This information was obtained from the AFP after action reporting and Filipino open-source reporting from the Internet. The black icons on the top right of the graph illustrate the AFP USSOF units involved during the crisis. The green icons directly below show the superimposed conventional AFP units involved. JSOTF-P was able to use the connections it had within the leadership of the Philippine special operations units to help shape the outcome. This was due in part to USSOF advisors being co-located with their host nation counterparts and contributing to collaborative efforts on the ground in time-effective ways. USSOF does not always have this luxury to assist allies in this way during a time of crisis. The lack of knowledge about the networks was thereby mitigated by direct intervention and support from JSOTF-P.

[115] Data for this study originate from open-source research and unclassified portions from the Special Operations Command Pacific that are available from the special operations command Pacific (SOCAC) portal.

The next finding observed on the ground was that a weak communication network existed in the early stages of the crisis. There were times that the organizations involved questioned who was in charge of operations (i.e., whether the local or national government). Figure 12 shows how the security forces were connected to each other and how they were linked with the RME, but fails to account for external connections to any nonsecurity agencies.

Figure 12. Sample network of organizations involved during the Zamboanga City crisis in the Philippines[116]



Understanding crisis communication networks would eliminate unnecessary time being dedicated to nonessential tasks. Initially there were several organizations working to understand how to communicate effectively during the crisis, which delayed necessary actions taking place. Unfortunately, no JSOTF-P personnel were permitted to attend the host nation synchronized planning meetings that subsequently took place during the latter

116 The data from which these sociograms derived originated from open-source Internet searches of the 2014 Zamboanga crisis and unpublished reports obtained from the Armed Forces of the Philippines.

part of the incident. This prevented the collection of information necessary to map out how the communication network looked from a SNA perspective.

The security forces, governmental and nongovernmental offices, and international organizations each maintained headquarters elements and separate field teams that composed organic subgroups within their organizations. These subgroups were the action arms of the agencies and early interagency synchronization would have allowed for more effective cooperation.[117] Many of these subgroups maintained their own networks and additional opportunities were present to seek additional connections and/or strengthen the preexisting relations. There were indications on the ground that subgroups lacked sufficient ties to subgroups of other agencies. This barrier impacted communication by creating bottlenecks, which led to a duplication of effort with minimal initial collaboration.

Resources sent by the GPH and U.S. government were disproportionately distributed and were being sent to organizations that, in large part, maintained direct ties to the government. JSOTF-P elements helped to coordinate developmental agency efforts to mitigate the communication issues with organizations that were not receiving resources from an inherent lack of relational ties to influential personnel within the local or national governments. Pfeffer, in *Managing with Power,* states, "Social networks are, then, structures that can be built deliberately, and our place in the network of communication is something that is under our own control."[118] A lack of understanding of the existing communication network during the crisis led to more time and resources directed toward alleviating some of the initial redundant problems. By mapping out the organizations involved, their relationships, and network characteristics, early identification of key areas and/or gaps would have been known from the start. In addition, resources would have been distributed more rapidly, which would have significantly decreased the demands of the security force personnel throughout the crisis.

---

[117] The coordination clusters executed by the LGU corrected these early synchronization issues. These clusters identified responsibilities of each agency during the recovery to foster collaboration.

118 Pfeffer, *Managing with Power: Politics and Influence in Organizations*, 125.

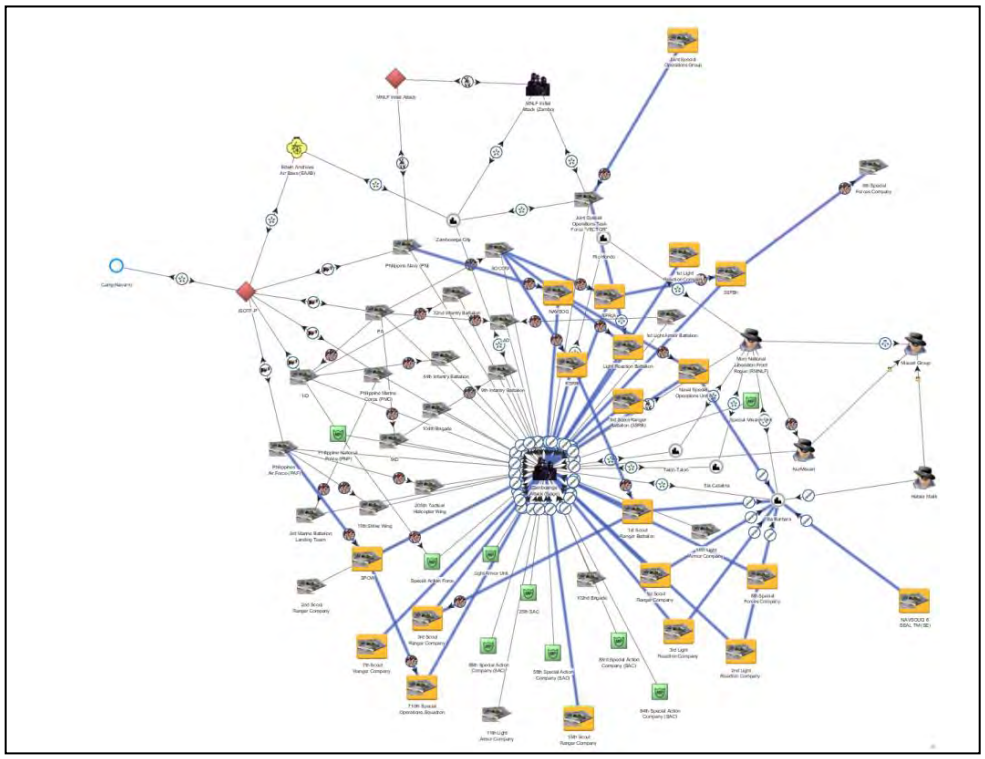
D. SNA AND PSF SELECTION

The principles and tools used to study covert organizations can be applied to develop a comprehensive approach to the study of friendly networks. This section will pull in theories presented earlier to support the Zamboanga application. Now that the mission has concluded, it is important to derive lessons learned to improve future strategies and highlight how understanding networks can be beneficial writ large. This section will show how SNA illumination of dim networks can solve the problems identified during this crisis as well as offer added benefits.

The networks available during a crisis situation are important to analyze to determine how organizations can be expected to behave in similar situations. Figure 13 shows the military units involved during the Zamboanga City Crisis. This diagram highlights the AFP USSOF units on which USSOF focuses its engagement strategy within the Philippines. The focus on SOF-specific units is telling for multiple reasons. The first is that this signifies that the GCC engagement strategy for the Philippines is successful as the units being engaged directly respond to national crisis and, although dimly lit, have connections to other agencies involved during national crisis. At this time, it remains to be seen if these units are the optimal units located in the Philippines. Relationships and networks will continue to change as the Philippines progress through the Philippine Internal Peace and Security Plan. There must be a system in place to collect the necessary data to measure these connections.

The next finding is that the USSOF within the AFP must work alongside the conventional military units and PNP units during security threats. This amounts to unexploited opportunities to engage other partner units that operate in the environment that could possibly have more substantial influential relationships, which could have been efficiently leveraged during the crisis.

Figure 13. Network of SOF units (highlighted) involved during the Zamboanga City crisis[119]



The network presented represents additional opportunities to influence the environment by determining key and influential actors within the network to see how they are connected and whom they are connected to. This would allow for the creation of more focused engagements while allowing the PSF opportunities to see the strengths and weaknesses in their network organization. Unfortunately, information about the connections to the local government units, national government agencies, intergovernmental organization, and NGOs is missing. Without these important relational ties illustrated, the friendly forces that share several annual SC events with the United States will remain dim networks.

[119] Data for this study originate from open-source research and unclassified portions from Special Operations Command Pacific that are available from the special operations command Pacific (SOCAC) portal.

E. SNA IN THE AFTERMATH

If SNA is to be used to transition dim networks to light networks across the dark-light spectrum, we see by looking at the Zamboanga City Crisis that the correct data to do this are not being collected. The foundation for this analysis is network relational data. This includes data collection from engagements, exercises and open-source research, and proper data structuring. The analysts may use different formats for reporting (i.e., Word or Excel documents), but whatever instrument chosen, it must be compatible with SNA software. This section will describe techniques to incorporate data collection into engagements to ensure the necessary data to profile dim networks are collected. The steps presented can be used in any situation and are not limited to a crisis.

The first step is to identify all the relevant organizations, or nodes, which are required to mobilize in a time of crisis. This could simply be all security force elements, all relevant intergovernmental organizations and NGOs, and other influential agencies within the government. JSOTF-P knew that the LRC and other AFP USSOF units would be involved, but was unaware of the involvement of other organizations. Information about the organization necessarily includes but is not limited to: size; resources; authorities; internal associations; external associations (criminal organizations, governmental organizations, police and military organizations, international organizations, media; NGOs, political, religious, and terrorists); and executed events (date/location).[120] What was known about the units JSOTF-P engaged with was focused on internal characteristics of that organization (i.e., composition, leadership, and organizational capabilities). Information about relational connections to external organizations was missing; this information is important to know when organizations work together. Figure 14 represents the network composed of the AFP and PNP units the United States engages with during the multitude of annual SC events that take place in the country. On the surface, this limited network identifies collective relations with units based on the shared events but does not account for relational ties outside of the exercises; nor does this limited network account for other attributes that could contribute

120 Data fields within these steps are taken from the SOCOM Code Book. A codebook ensures the data being collected are consistent and structured properly to ensure accurate analysis occurs.

to a better understanding of these units, their network characteristics, or network structure.

The information needed to conduct the analysis is somewhat contained within various sections of existing reporting, yet it is not identified as being important information to collect. SNA will produce outputs and analysis that illustrate the significance of this information to all stakeholders involved. This will help prevent complacency, demonstrated by the reuse of old information as seen in chronological operational reporting from the repeated exercises conducted with the same PSF. Historically JSOTF-P personnel have had enough experience in the country to capture this information over time to illuminate these dim networks but solely focused on capturing the type of data necessary to understand dark networks. The outcome of this step is to determine if the node is in fact realistically structured and capable of mobilization in the time of a crisis.

The next step is to determine the ties between nodes within the network. These ties can be multi-relational to include: kinship; relationship; business/operational; shared membership; or acquaintance. This can include historical or present connections. For example, during the Zamboanga City crisis, an analyst could link PSFs that conducted joint operations together or all agencies listed in the same recovery clusters. Unfortunately, these ties were not observed until days into the crisis. It is necessary to define what constitutes a tie to eliminate inconsistencies in relational patterns within the network. This is usually done with a codebook to ensure relational definitions are objective, can be easily duplicated for further analysis, and not misunderstood. Capturing various types of relational data is important. The goal here is to determine how nodes interact collectively within this network.

The final step is to determine how nodes are connected to specific events. These types of relations can include: associated with; participated in; and victim of.[121] A majority of the NGOs involved during the crisis response maintained relationships with military commanders or government officials that correlated to the support they received

121 For a detailed description of other relational ties reference the SOCOM codebook used to construct this methodology for friendly networks.

during the crisis. The observed interactional patterns will identify subgroups and illustrate the network composition and how it functions. At the completion of this step, the information will have to be uploaded into SNA software to produce visualizations and view the network's metrics. Higher echelons of command would ideally be responsible for conducting additional analysis and serve as a clearinghouse for continuity purposes to ensure the information is collected, analyzed, disseminated, and passed on appropriately.

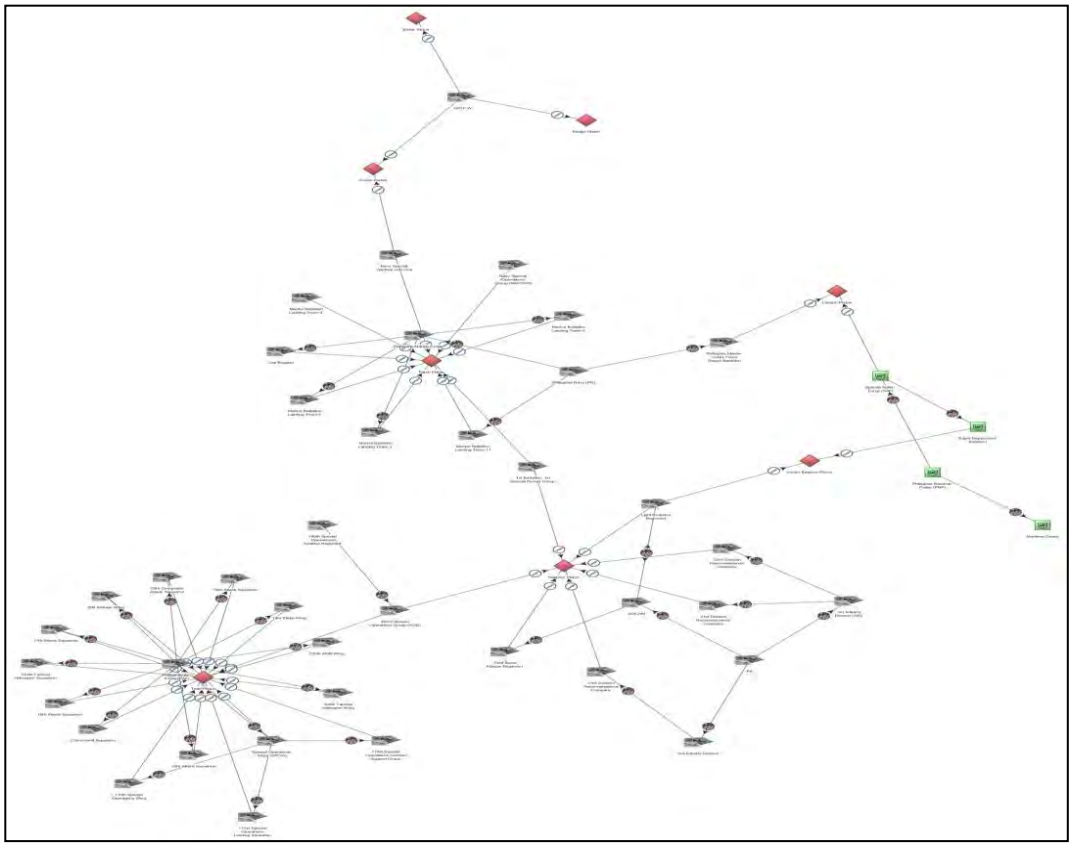
F. THE UNSTRUCTURED DATA PROBLEM

The present state of research on peacetime engagement indicates information necessary to illuminate dim networks is not a substantial segment within current reporting requirements around the DOD.[122] For the analysis to occur, a systematic collection method must be developed aimed at capturing relational data. Raab and Milward state, "The network concept is useful as an analytical tool because it calls for a systematic collection of information about the relations among the social units, be they individuals, groups, parts of organizations, or whole organizations." Bits and pieces of this information are located throughout reports produced to meet various reporting requirements, but the majority of the data needed to properly illustrate a network is missing. For this methodology to be effectively employed to support peacetime engagements, a desire to collect and prioritize this information is needed.

The Special Operations Debrief and Retrieval System reporting format can be used, as a tool to enable USSOF to integrate SNA within SC. SODARS is the reporting mechanism to capture and distribute information passively acquired by USSOF during operational missions. SODARS could be the method to obtain, analyze, and disseminate data on the dim networks surrounding host nation–friendly forces. Simple modifications to the current structure within these reports would be relatively easy as this is currently an existing reporting format used by USSOF. This modification of an existing system would eliminate certain bias found in these reports because the information is based on observations that would later be analyzed mathematically by SNA software.

122 Raab and Milward, 435.

Figure 14. Network formed from U.S. SOF JCETs (2001–2014)[123]



The only limitation of using SODARS as the repository of this information is the storage of these reports. SODARS are classified by some of the information contained within the report itself, so the ability to share this information with host nation forces would be problematic. However, the unclassified information used to illustrate these networks would be able to be shared with the host nation for them to benefit from this analytical tool. Commands must ensure data are collected and structured properly and confirm correct analysis is conducted to eliminate error in analysis. SNA tools are becoming widely available throughout SOCOM; it will just take guidance from higher commands to require the integration of this analysis into peacetime operations.

[123] Data for this study originate from open-source research and unclassified portions of the Special Operations Command Pacific that are available from the special operations command Pacific (SOCAC) portal.

G. FINAL THOUGHTS

The approach described in this chapter can lead to an optimization of SOCPAC's engagement strategy using SNA to identify the networks of the PSF being engaged and how influential the network is within the assortment of networks in that country. This development will benefit the teams on the ground conducting the exercise in that they will begin to understand how the PSF is nested with strategic interests for the United States and the host nation and be able to tailor that engagement appropriately. This chapter discussed the 2013 Zamboanga City Crisis in an attempt to illustrate the importance of how a dim network can be used to interdict threats. This event illustrated that any and all PSF relational ties with external organizations is necessary to collect during peacetime engagements in order to illuminate any networks prior to the start of crisis events. This analysis established an initial framework that enables a commander's engagement plan to be used as a platform to understand and leverage light networks.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SIMULATED NETWORK

Chapter IV presented a theory development case used to unpack the application of SNA to examine the dim networks surrounding security cooperation. The Zamboanga case uncovered several gaps in inability to illuminate dim networks that was linked to reporting that focused on dark networks. The reporting collection requirements of present security cooperation events are not suited to illuminate any networks that are not dark. This chapter will focus on how to correct and fill those gaps by presenting a simulated network to demonstrate the technique to collect data on security cooperation events to build a policy recommendation to allow for better analysis of security cooperation events.

A. DILEMMA

> "*Our vision is a globally networked force of Special Operations Forces, Interagency, Allies and Partners able to rapidly and persistently address regional contingencies and threats to stability."*[124]
>
> —Retired Admiral William H. McRaven

The Philippines is host to an average of fifteen annual JCETs that have a price tag of $4-5 million per year.[125] This does not include the regular non-SOF engagements conducted in addition to the JCETs. Analysis of the USSOF SC events reveals several apparent themes. A good assumption based on the amount and frequency of these engagements would be that enough information has been collected over the years to illustrate the network of host nation security forces.[126] However, upon analyzing the reports submitted after each event, the information necessary to map these PSF networks was not present. This is due to the fact that the data to illuminate these dim networks is not part of the current reporting requirements. The SODARS, although detailed in many

124 William McRaven, Posture Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command Before the 113th Congress House Armed Services Committee (2013).

125 Liebreich, "JCET Program Overview for PNP MG," 2014.

126 The total amounts of host nation personnel trained were 910 in 2014 and 1020 in 2013. Data obtained from JUSMAG Philippines reports sent to Naval Postgraduate school for research.

aspects, currently lacks the data fields necessary to illuminate friendly networks. The following example of a dim network using simulated data provides a comprehensive look of what information is essential and what different networks will look like once analyzed.

B. SIMULATED CASE OVERVIEW

At the onset of developing this thesis, it was identified that there was a shortfall in necessary data that would allow for the coding and mapping of the Philippine PSF network that is believed to exist. Despite SODARS reporting including specific information on the partnered units trained by USSOF, it did not include necessary relational data to begin to develop a network. Furthermore, despite the increasing access to open-source information, it was discovered that the data needed were not present online. It was necessary to create a simulated dim network that USSOF could encounter during SC events to justify this approach. To accomplish this, the network is simulated to ensure no analytical bias existed within the nodes or data used.

C. GENERATING AND VISUALIZING THE NETWORK

Because actors and the connections among them define networks, it is useful to begin the description of the simulated dim networks by examining these very simple properties. The actors presented in this simulated network are typical of those that can be found in a standard PSF network. Organizational connections are used to demonstrate how different dim networks can be developed through the mapping of these connections. As discussed in Chapter III, PSF networks that have not been mapped share characteristics of a dark network, in that the network is not known and could be considered somewhat clandestine. It is understood that a network exists because certain events may indicate this, such as a natural disaster or domestic crisis, where these forces can be seen cooperating with other agencies or organizations. Observing this places the network in a dim status within the spectrum of dark to light. This simulated network represents a dim network that progressed to the light end of the spectrum through the gathering of relational data between certain organizations and PSFs. Through the lens of SNA, each network is analyzed and centrality measures are calculated. The application of analysis is discussed and presented through the lens of an SC planner.

There are a host of different SNA tools available. One of the more useful benefits of SNA is its ability to visually represent data in network form. These visualizations are referred to as sociograms and show relational ties between nodes using a line connecting nodes that share a tie with each other. For this research, Organization Risk Analyzer (ORA) is used to simulate, visualize, and analyze the notional light network.[127] In addition to ORA, the open-source statistical environment called R was used. We used RStudio[128] software, a graphical user interface–based platform that provided us the ability to randomly generate values for X variables critical to the development of our hypothetical dim network. This statistical randomization allows for the mitigation of selection bias.

PSF networks vary widely depending on their political connections, threats they face, and resources available to them; therefore, it was necessary to control for these variances and generalize the simulated network based on personal experiences, and an assumption that the network would replicate the average PSF network that USSOF will encounter. This process began by generating a scale-free randomized network within ORA. Scale-free[129] was chosen because it more accurately represents existing networks. PSF networks typically consist of numerous well-connected units and some that are not connected to any entity outside their organic unit. This is typical of many former Soviet Bloc countries such as Tajikistan and Kyrgyzstan.

This simulated network was generated with 20 nodes. The first 10 nodes were labeled as GPF[130] 1–10 and SOF 11–20. This network is labeled as the MIL_MIL

---

127 ORA is defined as "a network analysis tool that detects risks or vulnerabilities of an organization's design structure. The design structure of an organization is the relationship among its personnel, knowledge, resources, and task entities. These entities and relationships are represented by a collection of networks called the Meta-Matrix. ORA analyzes the Meta-Matrix using measures, and reads and writes network data in multiple formats to make it interoperable with existing network analysis software." Kathleen M. Carley and Jeff Reminga, "ORA: Organization Risk Analyzer," Carnegie Mellon University, Center for Computational Analysis of Social and Organizational Systems, Pittsburgh, PA, 2004, 1.

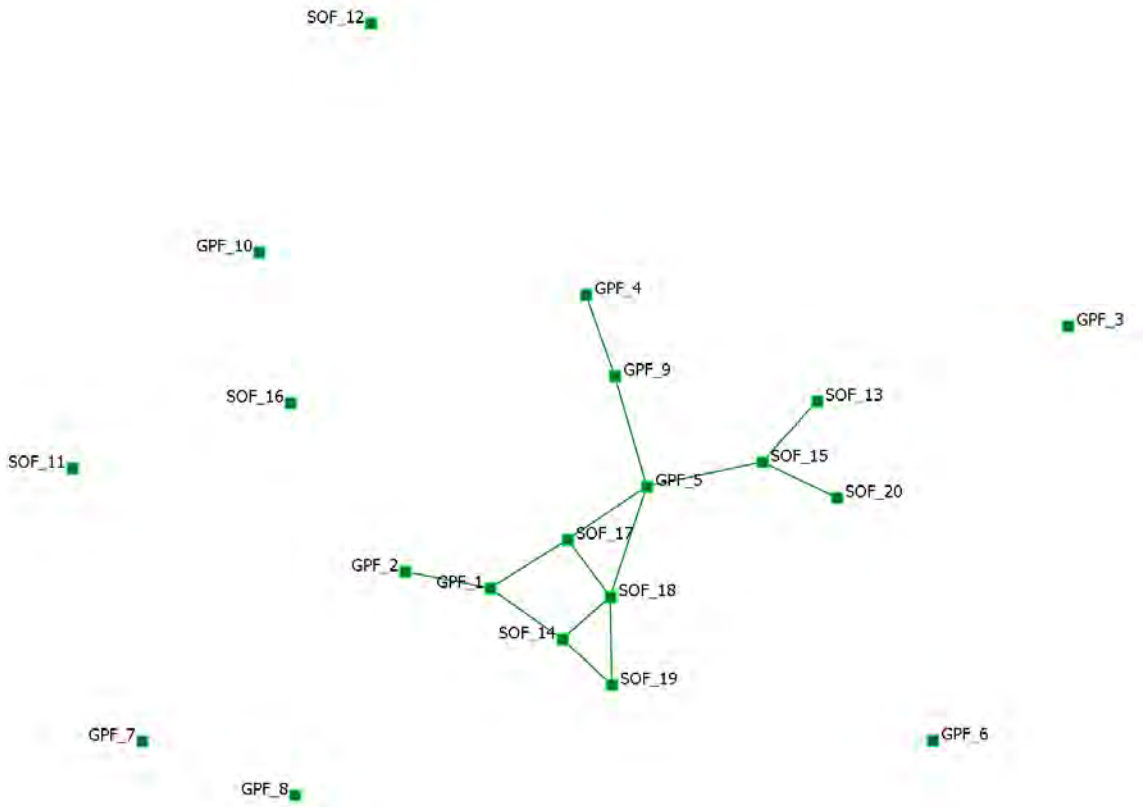
128 For more information on RStudio please visit https://www.rstudio.com/products/rstudio/. For more information on R, please visit https://www.r-project.org/.

129 For more detailed information on scale-free networks, see the Barabasi and Bonabeau article, "Scale-Free Networks," *Scientific American*, 2003.

130 GPF stands for general-purpose force, also known as conventional or regular forces.

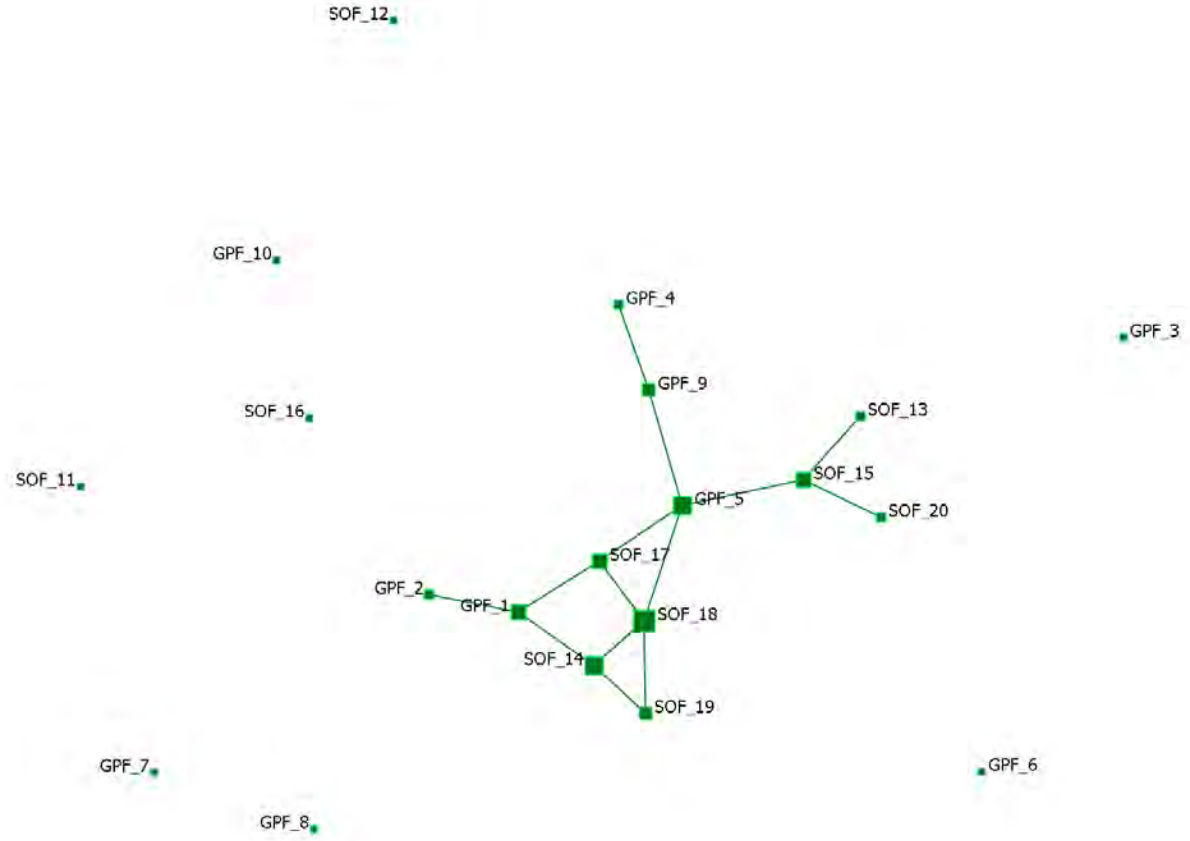
Network. This network consists of an equal distribution of a host nation's GPF and SOF for the purposes of negating any precondition of numerical advantage.

Figure 15. ORA MIL_MIL network (simulated)



The use of the scale-free function produced a network with a core group of connected nodes and eight isolates (Figure 15). Though not the most illuminating, the calculation of certain centrality measures can be done to determine the basic level of influence a unit might have based on their connections to other military units. Figure 16 shows the network with node sizes based on their total degree of centrality.

Figure 16. ORA MIL_MIL network nodes sized by total degree of centrality



This initial analysis, though not conclusive, does provide an SC planner with a simulated assessment of which units within this network are the most connected. By ranking the connections, a planner could then infer a unit with the most connections could also have the most influence in a friendly light network that could be in turn influenced through continued engagement.

The next step was to generate additional dim networks that are assumed to exist in the PSF network. This step begins with the assumption that connections and cooperation exist between the PSF and local government units (LGU).[131] For the purposes of simplicity, 10 LGUs were incorporated into the already established MIL_MIL network.

131 LGU refers to governmental entities below the national level government, such as provinces, districts, and so on. This could range from local law enforcement, local enterprises, correctional facilities, to public works, etc.

Using RStudio, a random number generator was created to provide the number of ties each military unit would have. Once the number was generated, a randomly generated set of numbers was created based on the previous random number. This process provides a truly random set of relational ties for each node.

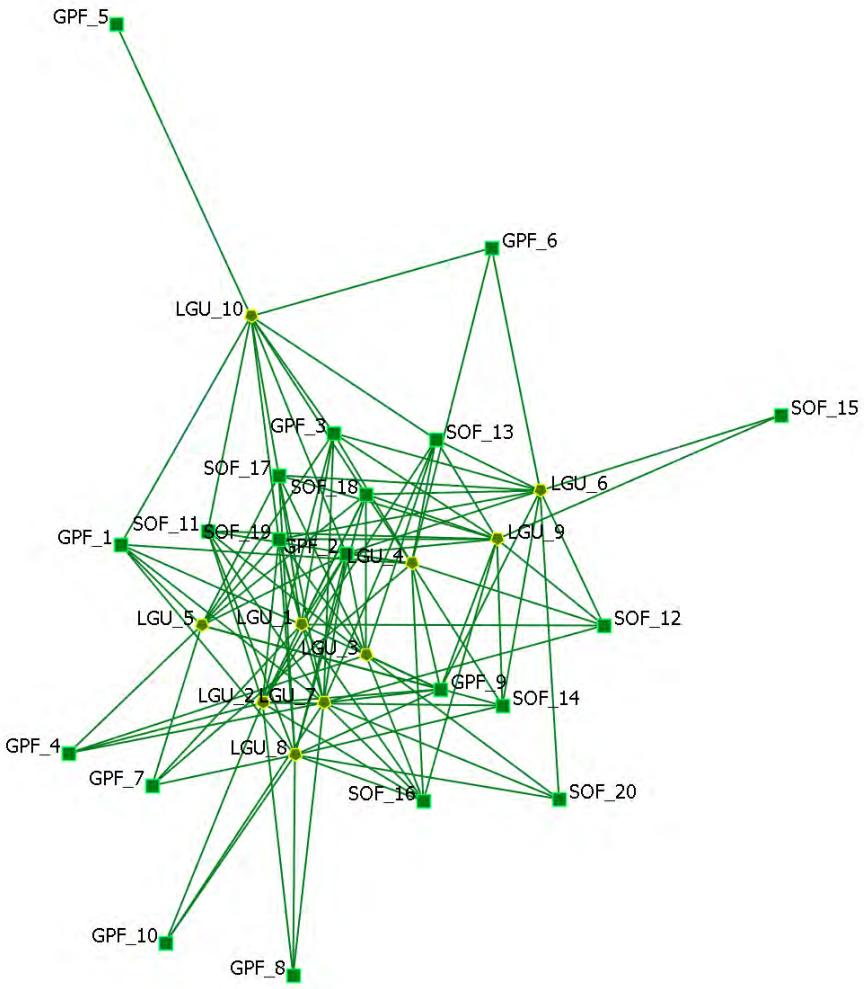
Table 4. ORA total degree centrality score for top ten nodes in the MIL_MIL network

Rank	Nodes	Value
1	SOF_18	0.128
2	GPF_5	0.103
3	SOF_14	0.103
4	GPF_1	0.077
5	SOF_15	0.077
6	SOF_17	0.077
7	GPF_9	0.051
8	SOF_19	0.051
9	GPF_2	0.026
10	GPF_4	0.026

The first code would provide a single number; for example, 4. The number 4 would then be inserted into the second code and that code would provide 4 random numbers between 1 and 10.[132] Each number would correspond to an LGU (1–10). Within the editor function in ORA, all the ties for the MIL_LGU network were randomized in this fashion. This network is depicted in Figure 17.

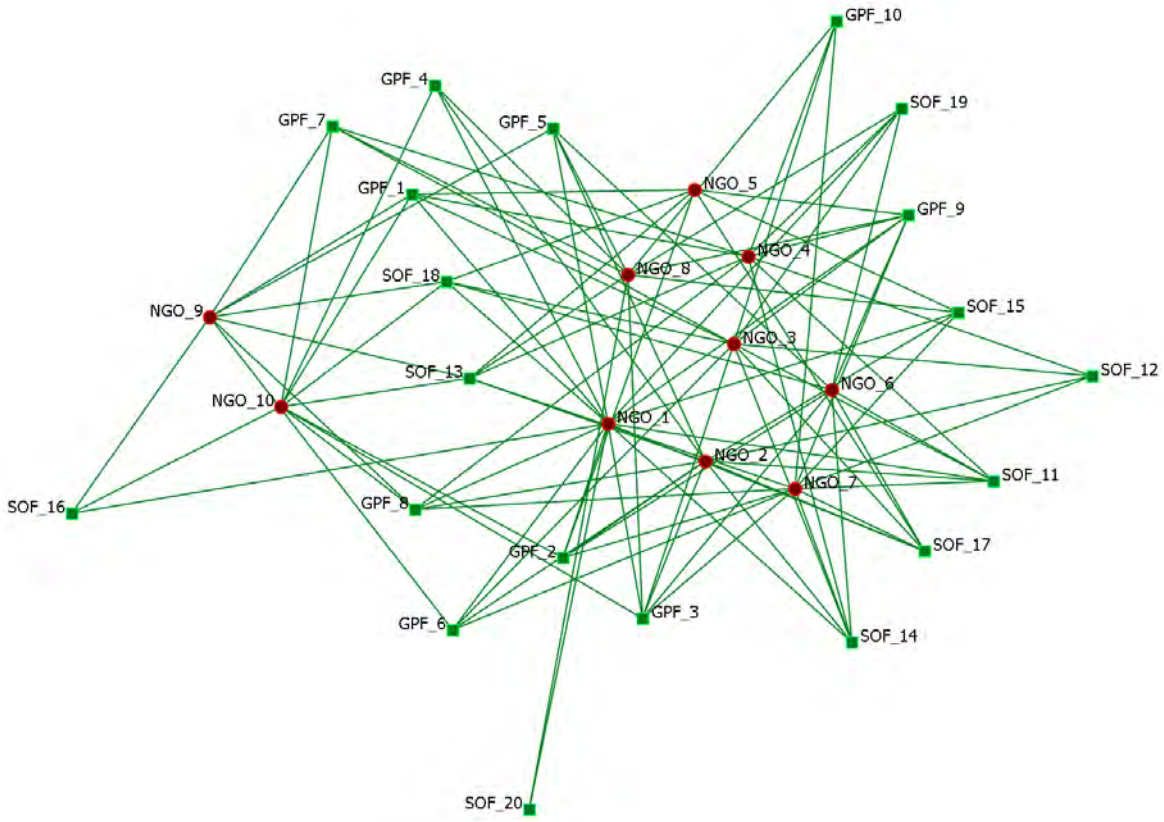
[132] The R code used can be found in the Appendix.

Figure 17. MIL_LGU network



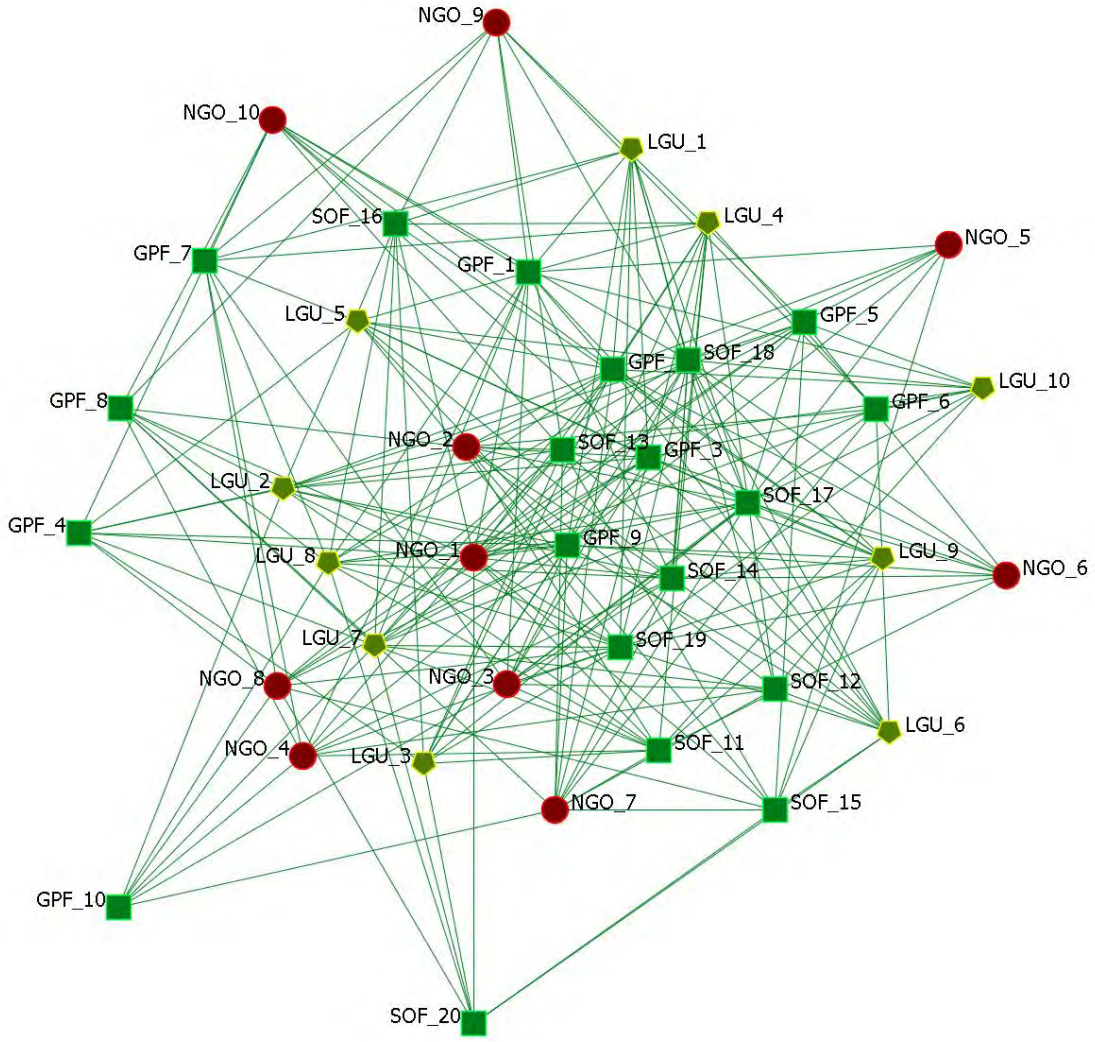
The next step was to create an NGO network. The widespread involvement of NGOs in all aspects of global interaction cannot be ignored. As described in the earlier case study, NGOs can have significant strategic effects on the military operating environment. Therefore, recording and understanding the ties PSFs have with NGOs is important for the overall analysis of these networks and determination of PSFs' influence within the environment. The previous process for LGUs was replicated, to develop the MIL_NGO network consisting of ten NGO nodes.

Figure 18. ORA simulated MIL_NGO network



Each separate network can provide certain insights in the potential level of influence that the PSF units maintains; however, it is not until each network is compiled into one cohesive network that we can assume some level of accuracy on the true level of influence based on their overall connectedness.

Figure 19. ORA simulated combination of all three separate networks



Once all the simulated networks have been created and compiled into one network, then ORA can be used to analyze the network. This chapter will apply and focus on four centrality measures, although there are many more that can be analyzed and provide different insights into understanding the network. The measures that we have selected all have specific utility in determining the connectedness of each node. These measures can provide an SC planner with the initial analysis to determine which units may have the most influence through their ties and thus begin to craft an engagement strategy that meets the commander's intent, expected outcomes, and desired end state. Though each measure is not specific to dim networks, their utility as the vehicle that can

advance a dim network to a light network is central to their selection. Centrality is a determinant factor of the level of influence a network has. Influence, along with capability and capacity, should be regarded as important characteristics of PSF units.

D. ANALYZING THE NETWORK

ORA allows the user to process specific reports that provide a listing of all measurable data. We employed this capability to produce a report that displayed the node-level measures of our combined network. We narrowed the results to the top ten nodes in each measure. Table 5 provides the top ten nodes ranked by their total degree centrality scores. Total degree centrality is a normalized sum of the nodes ties.[133] Nodes that have a higher score indicate that they have a higher degree of connectivity in the network, or they essentially have the most connections. It is assumed that nodes that have a higher score have more access within the network or access to the information within the network. This is very beneficial to the idea of shaping the operational environment and maximizing SC efforts across all security entities in a particular region. Identifying a PSF unit that is well-connected allows a planner or commander to prioritize manpower and resources toward SC engagements with that unit. Even if the unit is well-connected but not necessarily leveraging any influence within the network, U.S. forces could identify this and begin to manipulate this situation to benefit the host nation and American national interests. In this particular instance, an SC planner could cross-reference the units in the network with historical reporting on the units that U.S. forces have persistently engaged. In doing so, the planner can assist in providing the commander with a better picture of where each PSF ranks within the network. Depending on the lines of effort for that command, the commander and staff can adjust their engagement strategy to capitalize on the connectedness of the PSF in their region.

This idea can be carried through each of the centrality measures presented or applied to the totality of analysis of all four combined. This will provide a more complex understanding of the network as well as each specific node in the network. Table 5 identifies the top nine scores in betweenness centrality. The nodes that rank the highest

[133] Everton, *Disrupting Dark Networks*, 399.

have the shortest path across all node pairs for connectivity. Nodes that rank high in betweenness centrality have a greater potential to broker connections between other groups because of their position along the shortest path of connectivity. This brokering capability could be used to influence one group to apply influence on another. As mentioned previously, this analysis can provide SC planners with insight that could prove to be extremely valuable and directly impact the effectiveness of the engagement strategy in a particular region.

Table 5. Total degree centrality (ORA)

Rank	Nodes	Value
1	SOF_18	0.253
2	GPF_9	0.228
3	GPF_2	0.215
4	SOF_17	0.215
5	SOF_14	0.203
6	SOF_19	0.203
7	NGO_1	0.203
8	GPF_1	0.190
9	GPF_3	0.190
10	SOF_13	0.190

Table 6. Betweenness centrality[134] (ORA)

Rank	Nodes	Value
1	SOF_18	0.018
2	SOF_14	0.011
3	GPF_5	0.009
4	GPF_1	0.007
5	SOF_15	0.006
6	SOF_17	0.006
7	GPF_2	0.003
8	SOF_19	0.002
9	GPF_4	0.001

Table 7 lists the top ten nodes for closeness. Closeness is most easily described as how many connections it takes for a node to have a connection with all other nodes. This distance can be described as steps. The lower the average number of steps a node is from all others in the network can indicate its respective position in the network as well as an increased ability to influence the network in certain situations.

Table 8 lists the top ten nodes for Eigenvector centrality. This measurement determines a nodes weighted centrality based on the magnitude of its ties centrality. This measurement focuses on the power of cliques and the importance of who the perceived leader of that clique is. In certain instances, the security forces of a country are separated by a delineation of responsibility such as internal or external security, maritime security, or counterterrorism. Understanding this dynamic would greatly increase the SC planner's insight into the unwritten hierarchy of a particular country's security apparatus. Concentrating efforts to either cultivate this leadership or reduce or reassign its influence

134 This table lists only the top nine because of all the other nodes being tied for tenth with a score of 0.000.

for U.S. interests via USSOF objectives can be determined through the use of this centrality measure.

Across the four measures, certain nodes maintain high rankings. SOF_18, SOF_17, SOF_14 are consistently in the top five in three of the four measures. GPF_1 and GPF_2 are in the top five in two of the four measures. Many of these nodes are within a degree of each other or are tied with the same score. Though not conclusive, this basic analysis of the network shows that even with minimal detail the application and utility in applying SNA to exiting PSF networks can provide an SC planner with evidence to make informed recommendations. These recommendations could range from continuing to maintain the current strategy, identify new units to engage to improve or expand their influence in the network or reduce the influence of a unit through the reduction of U.S. influence and support.

Table 7. ORA-generated closeness centrality

Rank	Nodes	Value
1	SOF_14	0.075
2	SOF_18	0.075
3	SOF_17	0.075
4	GPF_1	0.074
5	SOF_19	0.074
6	GPF_9	0.058
7	GPF_2	0.042
8	SOF_13	0.042
9	GPF_3	0.040
10	SOF_11	0.037

Table 8. ORA-generated Eigenvector centrality

Rank	Nodes	Value
1	SOF_18	0.344
2	SOF_17	0.314
3	GPF_9	0.309
4	GPF_2	0.303
5	SOF_19	0.300
6	NGO_1	0.300
7	SOF_14	0.293
8	GPF_1	0.274
9	GPF_3	0.265
10	LGU_7	0.251

For this particular instance, it appears that the SOF units are the most connected. This could be due to U.S. involvement that, when substantiated, could indicate a certain measure of progress or success. The inclusion of the GPF forces in the top five could identify a shortfall in engagement for the TSOC because the typical force of choice to engage with is SOF. Identifying units outside of the traditional forces that the TSOC engages with could allow the planners to expand their level of influence to these units that appear to have a high level of centrality in the overall security network.

Through the use of SNA software, such as ORA, a planner can incorporate additional variables or attributes as they become available or as a part of a concerted collection effort, whether overt or covert. The incorporation of these variables and attributes will continue to illuminate these dim networks, rendering them more and more complete. As these networks are mapped and the understanding of the networks advances, SC planners will have the tools necessary to optimize peacetime engagement

efforts. This begins with the selection of the most appropriate unit based on the commander's lines of effort and intent.

E. FINAL THOUGHTS

The DOD will need to reexamine and possibly update its engagement strategy to determine if it is structured in a manner to have optimal results forging necessary and long-lasting SC networks. SNA can be used to develop a model to assist the commander and staff in developing an engagement strategy by determining which forces will provide the best opportunity for advancing both national and regional security efforts. Networks can be examined based on the amount and type of influential ties either created and/or maintained by the PSF to determine an optimum level of influence and network performance. However, in certain countries, PSF selection is centered on national politics over anything else. This type of selection cannot be avoided in these situations but, in the absence of such political constraints, a robust and influential network is an ideal attribute for a PSF unit to have.

The engagement plan has multiple options available when approaching a PSF with inadequate or a less than optimum influential network. The first is to continue to engage with the unit but prioritize an expansion and/or adjustment in network connections and capability as part of the engagement strategy. This can include an increase in ties to other organizations or possibly decreasing connections based on the type and need for specific ties to exist. This can be accomplished by conducting joint training or joint operations during the engagement. Because networks are constantly changing, there is no specific methodology prescribed here. General methods to accomplish this option have been identified in earlier sections of this thesis, but information that maps light networks must be continuously sought and recorded. The next best option is to partner with the PSF with the most optimal network available that can be leveraged in a time of crisis. This option is preferred if there is limited episodic engagements planned and/or restricted training opportunities available. Nonetheless, before these options are available, the information that indicates how these units compare with one another again has to become a priority within existing reporting.

This approach is not limited to information collected from the field. SNA can be conducted on previous historical terrorist incidents in specific countries to illustrate the evolution of the friendly units involved and their connectivity to other units and agencies over a specific timeline. The focus of this analysis will not be on the dark networks or terrorist organizations that caused the event, but on the host nation security forces that responded. This will give an indication of how USSOF engagements have shaped the operational environment and if USSOF are currently partnered with the ideal security force in that country. Similar approaches can be used in other countries independent of their exposure to USSOF engagements. This will allow for planners to analyze how host nation organizations are used in a time of crisis and how security forces are connected to help determine ideal units to engage with.

VI. CONCLUSION

> *"But it is an unfortunate fact that we can secure peace only by preparing for war*."[135]
>
> —President John F. Kennedy

Social network theorists have used the term "light network," which has a generally understood meaning of cooperative networks not attempting to conceal themselves.[136] Light networks are vital for USSOF to understand in order to build effective networks throughout the world. Barabàsi and Bonabeau, in *Scale-Free Networks*, express the notion that networks are everywhere and "Societies, too, are networks of people linked by friendships, familial relationships and professional ties."[137] One way to accomplish an enhanced level of understanding of the environment is through analysis of the people who live and operate there.

A. VALIDITY FOR IMPLEMENTATION

Today's unknown groups throughout the world can cause the problems and challenges that have plague the United States in the twenty-first century. The key to solving these unknowns is to have existing mechanisms capable of responding to threats. One focus area is to know, understand, and influence the networks in strategic areas around the world. The study of light networks within host nation militaries across the world has largely been ignored; yet, these networks can be instrumental by being used in ways to avoid large-scale U.S. military intervention. From a networking perspective, theater security cooperation events can be improved to better contribute to long-term U.S. government objectives using SNA. One method to ensure the pendulum shifts in this direction is to invest in SNA tools and resources and apply them to all engagement strategies within SC.

---

135 Kennedy. "Speech of Senator John F. Kennedy, Civic Auditorium, Seattle, WA" September 6, 1960.

136 Everton, *Disrupting Dark Networks, 6*.

137 Barabási and Bonabeau, *Scale-Free Networks*, 62.

Understanding dim and light networks can have tremendous advantages for both the U.S. and the host nation involved. Information about light networks will allow the U.S. to observe how partner forces are connected domestically and regionally. This will allow USSOF units to have a better sense of how their engagement can realistically shape the operational environment, thus advancing the TSCP. Additionally, this understanding will allow the host nation to graphically represent the extent of its security forces' influence from a network perspective.

This research has developed a three-phase approach to integrate SNA into SC. This is a long-term initiative and this research is attempting to initiate the conversations with the policy makers in order to uncover advantages that were not previously known about. The first phase is investment. This phase starts with the GCC implementing standard operating procedures to incorporate this approach into current peacetime engagements. The next phase is development. During phase 2, select cases will be used to advance this approach across the different combatant commands. Within these cases, historical examples can be used to indicate the connections units had before USSOF engagements and the connections they presently have. If a unit does not fit in with what the TSOC commander wants in that region, a new unit can be selected that is more suited to accomplish long-term strategic interests in the area. The following phases (investment and development) were developed along with this research as a way to institutionalize this approach.

1. Execution

a. Phase 1 Investment

This phase starts with Combatant Command agreeing with this approach and each command enforcing the type of data collection necessary to illuminate the dim networks across the region.

Essential tasks during this phase:

1. Standardization across current security cooperation reporting requirements that highlight a dim network SNA focus.
2. SNA implementation at tactical, operational, and strategic levels.

3. This must become a joint venture with designed cross-service SNA education.

b. Phase 2 Development

This phase starts with the formulation of a strategy to implement in key states. Data and analysis must be continuously updated to show any differences and/or evolution of the light networks overtime. This phase must demonstrate the utility for this approach to the U.S. Country Team and host nation. By using SNA to move the spectrum of dim networks toward light networks, the optimal partner force can be selected that bests meets the strategic goals of the United States.

2. Study Purpose

This thesis proposes ways to use SNA to select the ideal partner force in noncombat environments. Updated reporting requirements and engagement strategies focused toward understanding complex strategic environments is necessary. Although this advancement cannot occur overnight, this research is aimed at slowly moving the methodology forward to gain interests across the DOD. If the shift toward prioritizing the illumination of these types of networks does not occur, it will be difficult to learn whether the units being engaged have the political connectivity and resources necessary to be called on by the national government to successfully interdict a crisis. Consequently, this could demand increases in the mobilization of U.S. forces, which will soon be a significant challenge for the U.S. administration.

B. FURTHER RESEARCH

Current operations in the Middle East present ideal conditions to test this method of analysis further with U.S.-partnered forces in the region. Syria has been the location of failed attempts to build a partner force that have similar objectives of the United States and are capable of defeating adversaries. SNA can be a means to visualize how the existing forces operating within this region are actually situated around the chaos in the area as opposed to creating a capable force from little to nothing. This approach can be used to illustrate relational structures within current military organizations, identify fracture points toward the Syrian Regime, or identify allegiance toward ISIS. However,

was this type of information collected during previous military engagements conducted in the region? In addition, was the interpretation of PSF networks in this area a top priority for commanders during these engagements? If not, and the data to illuminate the security forces in this area are not available, the best time to start is the present. This will give the United States and a coalition against current threats a means to understand how local moderate forces are positioned and what ties need to be eliminated and/or strengthen to increase chances of launching successful future operations.

Additional research is needed to determine what, if any, correlation exists between the capabilities of a unit and the amount of external network connections. In other words, once a unit is highly specialized and reaches a certain level of proficiency, is there a point where external ties become less relevant or the relational ties change as the political environment changes? This would be important to consider in the decision-making process concerning network manipulation and future engagement strategy. Although the available data to understand these dim networks are limited, this research employs the methods used to study dark and light networks to improve future efforts to lighten the formerly dim networks. This illumination will help objectively determine the type of SC event to execute as well as the most optimal partner to engage with.

C. FINAL THOUGHTS

The short-term success from the kill-and-capture missions executed during the course of the wars in Iraq and Afghanistan, including the famous raid on Osama bin Laden, has overshadowed any other long-term strategy from materializing. A long-term strategy will require a long-term investment that favors accurate data collection, data structuring, and data analysis to be successful. New forms of warfare carried out against the United States and its allies will require new strategies. New groups are emerging that challenge the ability of the state to govern while simultaneously creating opportunities to benefit financially from the warfare and the chaos they inflict. These criminal and terrorist groups are becoming more adept at evolving in response to government actions against them. This increases the incentives from a cost-based analysis standpoint for the rise of dark networks conducting illegal activities. To defeat an organization that has

developed advanced network characteristics will require more information and analysis than current operations and reporting requirements command. The new strategies must include the ability to leverage the light networks to its full capacity against the dark networks. Understanding the full depth of our PSF networks, how U.S. forces can best influence those networks, and then leveraging them in a time of crisis may be the first step in developing these new strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

The R Code listed here will allow for the replication of the random number generators used for the simulated network in Chapter V.

##Random selection of NGO ties

RSNGOT <- sample (1:10, 1)

RSNGOT

The number generated with the previous code is inserted into the following code indicated by the #.

##Random selection of which NGO(s) the MIL is tied to

NMT <- sample (1:10, #, replace=F)

NMT

Each number corresponds to a different NGO (1–10).

##Random selection of LGU ties

RSLGUT <- sample (1:10, 1)

RSLGUT

The number generated with the previous code is inserted into the following code indicated by the #.

##Random selection of which LGU(s) the MIL is tied to

LMT <- sample (1:10, #, replace=F)

LMT

Each number corresponds to a different LGU (1–10).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albert, Reka. Hawoong Jeong, and Albert-László Barabási, "Internet: The Diameter of the World Wide Web." *Nature* 401 (1999), 130–131.

Army Capabilities Integration Center. *Strategic Landpower: Winning the Clash of Wills*, May 6, 2013. http://www.arcic.army.mil/app_Documents/Strategic-Landpower-White-Paper-28OCT2013.pdf.

Arquilla, John. "How to Win." *Foreign Policy*. October 12, 2009. Accessed 19 September 2015. http://foreignpolicy.com/2009/10/12/how-to-win/.

Barabási, Albert-László. *Introduction and Keynote to a Networked Self*, ed. Zizi Papacharissi. New York, NY: Routledge, 2011.

_____. *Linked: How Everything Is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. New York, NY: Plume, 2009.

Barabási, Albert-László and Eric Bonabeau. "Scale-Free Networks." *Scientific American* (2003), 50–59.

Carley, Kathleen M. and Jeff Reminga. "ORA: Organization Risk Analyzer." Carnegie Mellon University, Center for Computational Analysis of Social and Organizational Systems, Pittsburgh, PA, 2004. Accessed December 7, 2015. http://www.casos.cs.cmu.edu/publications/papers/carley_2004_oraorganizationrisk.pdf.

Clinton, Hillary. "America's Pacific Century." *Foreign Policy*. October 11, 2011. Accessed September 30, 2015 . http://foreignpolicy.com/2011/10/11/americas-pacific-century/.

Cross, R. and Thomas, R. *Driving Results Through Social Networks: How Top Organizations Leverage Networks for Performance and Growth*. New York, NY: Jossey-Bass, 2009.

Cukier, Rosa. *Words From Jacob Levi Moreno*. N.p.: Rose Cukier, 2007.

Defense Security Cooperation Agency. *Security Assistance Management Manual*, C1.1.1 (Washington, DC: Defense Security Cooperation Agency). Accessed December 7, 2015. http://www.samm.dsca.mil/chapter/chapter-1.

Department of Defense. *Defense Strategic Guidance*. Washington, DC: U.S. Department of Defense, 2014.

_____. *Quadrennial Defense Review*. Washington, DC: U.S. Department of Defense, 2014.

Everton, Sean F. *Disrupting Dark Networks*. Cambridge, U.K.: Cambridge University Press, 2012.

Everton, Sean F., and Nancy Roberts. "Strategies for Combating Dark Networks." *Carnegie Mellon Journal of Social Structure* 12, no. 2 (2009), 1–32.

Fonbuena, Carmela. "Zamboanga Siege: Tales from the Combat Zone." September 13, 2014. Accessed December 7, 2015. http://www.rappler.com/newsbreak/68885-zamboanga-siege-light-reaction-battalion.

Freeman, Linton C. *The Development of Social Network Analysis: A Study in the Sociology of Science*. Vancouver, B.C., Canada: Empirical Press, 2004.

Granovetter, Mark. "The Strength of Weak Ties." *American Journal of Sociology* 78, no. 6 (1973): 1360–1380.

Han, Jeffery S. and Ryan Schloesser. "Joining the Helping Hands: Understanding the Humanitarian Assistance Network in Tajikistan" (Unpublished paper, Naval Postgraduate School, March 27, 2014).

International Crisis Group. *Terrorism in Indonesia: Noordin's Networks*. Asia Report, May 5, 2006. Accessed December 7, 2015. http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/114-terrorism-in-indonesia-noordins-networks.aspx.

Joint Chiefs of Staff. "National Military Strategy of the United States of America, 2015. The United States Military's Contribution to National Security." Washington, DC: U.S. Joint Chiefs of Staff, 2015.

_____. Joint Publication 3–15.1. *Counter-Improvised Explosive Device Operations*. Washington, DC: Department of Defense, 9 January 9, 2012.

Joint Special Operations University (JSOU). *Special Operations Forces Reference Manual*, 4th edition. Tampa, FL: JSOU Press, 2015.

Kadushin, Charles. *Understanding Social Networks: Theories, Concepts, and Findings*. Oxford, U.K.: Oxford University Press, 2012.

Kautz, Henry, Bart Selman, and Mehul Shah. "Referral Web: Combining Social Networks and Collaborative Filtering." *Communications of the ACM*, 40, no. 3 (1997).

Kennedy, John F. "Speech of Senator John F. Kennedy, Civic Auditorium, Seattle, WA," September 6, 1960. Accessed December 7, 2015. http://www.presidency.ucsb.edu/ws/?pid=25654.

Kleiner, Art. "Karen Stephenson's Quantum Theory of Trust." *Strategy + Business* 29, Fourth Quarter (2002). Accessed July 20, 2015. http://www.strategy-business.com/article/20964?gko=8942e.

Koschade, Stuart. "A Social Network Analysis of Jemaah Islamiyah: The Application to Counterterrorism and Intelligence." *Studies in Conflict & Terrorism* 29, no. 6 (2006), 559–575.

Liebreich, Theodore T. "JCET Program Overview for PNP MG" (Joint United States Military Advisory Group reporting, Philippines, 2014).

MacCalman, Molly, Alexander MacCalman, and Greg Wilson. "Visualizing Social Networks to Inform Tactical Engagement Strategies That Will Influence the Human Domain." *Small Wars Journal.* Accessed October 28, 2015. http://smallwarsjournal.com/print/14428.

McAdam, Doug. *Political Process and the Development of Black Insurgency*, *1930–1970.* Chicago: University of Chicago Press, 1982.

McRaven, William. Posture Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command Before the 113th Congress House Armed Services Committee. Accessed December 7, 2015. http://docs.house.gov/meetings/AS/AS00/20130306/100394/HHRG-113-AS00-Wstate-McRavenUSNA-20130306.pdf.

Obama, Barack. *National Security Strategy of the United States of America* (Washington, DC: White House, 2015.) Accessed September 15, 2015. www.whitehouse.gov /sites/default/files/docs/2015_national_security_strategy.pdf.

Pescosolido, Bernice. "The Sociology of Social Networks," in *21st Century Sociology*, ed. C. Bryant and D. Peck (Thousand Oaks, CA: SAGE Publications, Inc., 2007).

Pfeffer, Jeffrey. *Managing with Power: Politics and Influence in Organizations.* Cambridge, MA: Harvard Business Press, 1992.

Prell, Christina. *Social Network Analysis: History, Theory & Methodology*. London: SAGE, 2011.

Raab, Jörg. "Dark Networks as Organizational Problems: Elements of a Theory." *International Public Management Journal* 9, no. 3 (2006): 333–360.

Raab, Jörg and H. Brinton Milward. "Dark Networks as Problems." *Journal of Public Administration Research and Theory, J-Part* 13, no. 4 (2003): 413–439. doi: 10.1093/jpart/mug029.

Roberts, Nancy and Sean F. Everton. "Strategies for Combating Dark Networks." *Journal of Social Structure* 12, no. 2 (2011): 1–32.

Roosevelt, Franklin D. “Undelivered Address Prepared for Jefferson Day,” April 13, 1945. Accessed December 7, 2015. www.presidency.ucsb.eduws/?id=16602.

Rothkopf, David. “Does America Need New ‘Special Relationships?’” *Foreign Policy*, August 4, 2015./

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

Special Forces Association. “The Origin of Special Forces.” Accessed December 7, 2015. http://www.specialforcesassociation.org/about/sf-history/.

Szayna, Thomas S, and William Welser IV. *Developing and Assessing Options for the Global SOF Network*. Santa Monica, CA: RAND, 2011.

White House, The. *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2015). Accessed December 7, 2015. www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

U.S. Army. ATP 3–57.80: Civil Military Engagement. Washington, DC: Department of the Army, 2013.

U.S. Joint Forces Command. *Commander’s Handbook for Attack the Network* Washington, DC: U.S. Government Printing Office, 2011.

U.S. Special Operations Forces. *Operating Concept*. MacDill Air Force Base, FL: United States Special Operations Command, 2013.

Votel, Joseph L. Statement to The House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, March 18, 2015. Accessed December 7, 2015. http://fas.org/irp/congress/2015_hr/031815votel.pdf

Ziemke, Earl F. *The U.S. Army in the Occupation of Germany 1944–1946*. Washington, DC: U.S. Government Printing Office, 1975. http://www.history.army.mil/books/wwii/Occ-Gy/index.htm.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California