Theses and Dissertations   1. Thesis and Dissertation Collection, all items

2018-12

Improving nonlethal targeting: a social network analysis method for military planners

Brown, Jason C.

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/27800

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVING NONLETHAL TARGETING: A SOCIAL NETWORK ANALYSIS METHOD FOR MILITARY PLANNERS

by

Jason C. Brown

December 2012

Thesis Advisor:	Nancy Roberts
Thesis Co-Advisor:	Sean Everton

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE IMPROVING NONLETHAL TARGETING: A SOCIAL NETWORK ANALYSIS METHOD FOR MILITARY PLANNERS		**5. FUNDING NUMBERS**
6. AUTHOR(S) Jason C. Brown		
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)

Nonlethal strategies are an essential part in the military targeting process to defeat and disrupt terrorist and insurgent networks. The majority of nonlethal options of military power come through Information Operations, including the use of deception. This thesis explores how a deception plan against a terrorist network can be informed and prepared using social network analysis methods. Selecting targets that fragment the network becomes the object of the deception, whereas the actual targets of deception are individuals who are connected to these fragmentation nodes. A simulation of how information diffuses through the network helps identify how rapidly and how far a misinformation message might spread. Social network analysis also shows where intelligence collection might be incorporated to provide feedback about the success of message dissemination and the deception effort.

14. SUBJECT TERMS Information Operations, deception, nonlethal strategies, simulation, network, fragmentation, information diffusion, intelligence, targeting, social network analysis, influence			**15. NUMBER OF PAGES** 83
			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

IMPROVING NONLETHAL TARGETING: A SOCIAL NETWORK ANALYSIS METHOD FOR MILITARY PLANNERS

Jason C. Brown
Major, United States Army
B.S., United States Military Academy, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2012

Author: Jason C. Brown

Approved by: Nancy Roberts
Thesis Advisor

Sean Everton
Thesis Co-Advisor

John Arquilla
Chair, Department of Defense Analysis

iii

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Nonlethal strategies are an essential part in the military targeting process to defeat and disrupt terrorist and insurgent networks. The majority of nonlethal options of military power come through Information Operations, including the use of deception. This thesis explores how a deception plan against a terrorist network can be informed and prepared using social network analysis methods. Selecting targets that fragment the network becomes the object of the deception, whereas the actual targets of deception are individuals who are connected to these fragmentation nodes. A simulation of how information diffuses through the network helps identify how rapidly and how far a misinformation message might spread. Social network analysis also shows where intelligence collection might be incorporated to provide feedback about the success of message dissemination and the deception effort.

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

D3A—Decide-Detect-Deliver-Assess targeting methodology

HPTL—High Payoff Target List

ICG—International Crisis Group

IIA—Inform and Influence Activities

IO—Information Operations

ISR—Intelligence, Surveillance, and Reconnaissance

KLE—Key Leader Engagement

KPP-NEG—Key Player Problem/Negative

KPP-POS—Key Player Problem/Positive

MILDEC—Military Deception

MISO—Military Information Support Operations

ORA—Organization Risk Analyzer (software)

PA—Public Affairs

SNA—Social Network Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Nancy Roberts and Dr. Sean Everton, for helping me keep this project manageable and applicable to the real world. I would also like to thank LTC Ian McCulloh for his contribution and assistance with social network analysis; LTC Keith Jarolimek for his ideas and mentorship in IO planning; the CORE Lab and especially Dan Cunningham for getting through the mechanics of SNA; and Doowan Lee for help with social movements and scoping the problem of social influence. Finally, I want to give special thanks to my family for their loving support and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND PROBLEM

A. BACKGROUND

Since 9/11, the U.S. military has been working hard at attacking terrorist networks in order to disrupt them or bring them down. Some strategies to attack the network have focused on lethal action, defined as combat operations that "close with and destroy or seize enemy facilities, equipment, or personnel... as a means to end [the enemy's] will to resist."[1] Some examples of lethal strategies include drone strikes on suspected training camps or against suspected high value individuals such as Anwar al-Awlaki, and the Special Operations Forces mission that killed Osama bin Laden. Other successful lethal targeting missions include the deaths of top al-Qa'ida in Iraq leaders, heavily disrupting this organization's efforts in Iraq.[2]

The pursuit of lethal strategies has had its downsides, such as increasing, rather than reducing, the number of insurgents. It is counterintuitive to think that removing leaders and organizers of insurgencies may actually increase the resolve of the people in whom the insurgency resides. For instance, Major General Michael Flynn points out that the brutal tactics of the Soviet counterinsurgency campaign in Afghanistan only served to broaden the size of the insurgency.[3] Admiral Eric Olson, former commander of U.S. Special Operations Command said that a direct action mission is "urgent and necessary, but not decisive. It is a holding action that buys time for the indirect approach to have its decisive effect."[4]

---

1 Charles Faint and Michael Harris, "F3EAD: Ops/Intel Fusion 'Feeds' the SOF Targeting Process," *Small Wars Journal* (January 31, 2012). Accessed November 13, 2012. http://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-"feeds"-the-sof-targeting-process.

2 JD, "Lethal Targeting in Iraq; Success on an Unprecedented Scale," *al Sahwa* (April 22, 2010). Accessed November 13, 2012. http://al-sahwa.blogspot.com/2010/04/lethal-targeting-in-iraq-success-on.html.

3 Michael T. Flynn, Matt Pottinger, Paul T. Batchelor, "Fixing Intel: A Blueprint for Intelligence Relevant in Afghanistan," *Voices from the Field* (Center for a New American Security, January 2010), 8.

4 Eric T. Olson, "Q&A: Admiral Eric T. Olson," *Special Operations Technology* 6 no. 4 (2008). Accessed November 13, 2012. http://www.special-operations-technology.com/sotech-home/56-sotech-2008-volume-6-issue-4/423-qaa-admiral-eric-t-olson.pdf.

One of the key challenges in current counterterrorism efforts is to find nonlethal strategies that may avoid the downsides of lethal targeting and offer a greater advantage in terms of the risks undertaken or the resources employed to execute the strategies. The search is on for strategies that maximize adversarial disruption while minimizing costs to those pursuing them.

Nonlethal strategies are defined here as "those instruments aimed at modifying or disrupting an adversary's ability to operate effectively while also changing his behavior using nonlethal means. Nonlethal fires change perceptions while shaping conditions that are favorable to our own goals and objectives."[5] Nonlethal strategies include stability and civil support operations such as reconstruction and cleanup in humanitarian and disaster relief, rebuilding infrastructure damage after combat operations, medical and veterinarian services, and "other nonlethal, constructive actions by Soldiers working among noncombatants."[6] Alternately, "nonlethal, constructive actions can persuade the local populace to withhold support from the enemy and provide information to friendly forces."[7] Many of these actions are coordinated through Civil Affairs programs.

In addition to the stability and civil support operations conducted through Civil Affairs, many of the nonlethal strategies fall under the umbrella of Information Operations (IO). Many commanders have come to realize that IO is not just a conglomeration of information related tasks and capabilities, but a decisive and critical component to military campaigns. COL Ralph Baker, a former brigade commander in Baghdad during Operation Iraqi Freedom said, "I quickly discovered that IO was going to be one of the two most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency (COIN) campaign."[8]

---

[5] Dewey A. Granger, "Integration of Lethal and Nonlethal Fires: The Future of the Joint Fires Cell," monograph, Fort Leavenworth, KS: U.S. Army Command and General Staff College (2009), 19.

[6] United States Army, *Field Manual 3.0: Operations,* Washington, DC: Department of Defense (Feb. 2011), 3–26.

[7] *FM 3.0: Operations*, 3–27.

[8] Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13.

IO support and complement a full range of nonlethal strategies through the military targeting process—the forum in which a friendly commander's objectives are operationalized against the adversary. The goal in the process is to spot points of vulnerability within the network that are susceptible to influence activities (i.e., psychological warfare and deception), points for informational diffusion (related to both Military Information Support and Public Affairs activities), and both formal and informal influence nodes whom key U.S. leaders can approach to shape opinions and actions.[9]

B.   PURPOSE AND OBJECTIVES

The purpose of this thesis is to demonstrate how to craft nonlethal IO strategies to disrupt networks. In particular, this thesis develops recommendations, informed by IO techniques, to take to the targeting and planning processes. Ultimately, the intention is to prompt the network to implode from within or to modify normal operating procedures by sowing seeds of mistrust through a deception plan rather than require lethal interventions from the outside. The goal of such a plan would be to expel, remove, or otherwise limit the relationships and impacts of key nodes.

C.   RESEARCH QUESTION

This thesis addresses the question: How can the IO planner make more appropriate recommendations for nonlethal targeting? Answers to this question will reveal methods for creating a list of nodes whose removal will highly fragment the network as well as reveal methods for quickly diffusing a message through the network.

D.   THESIS SCOPE AND METHODOLOGY

The framework of this thesis is a simulation study of how the IO method of deception produces disruption effects through fragmentation. The first step is to collect data on which to test a deception strategy. Data for this exercise is drawn from a network of terrorists in Indonesia associated with Noordin Top, who was formerly a member of

---

[9] Army FM 3–0 uses "inform and influence activities" to provide scope and guidance on the informational domain of warfighting. Military Information Support Operations (MISO), public affairs, military deception, and soldier/leader engagements are examples of the activities required to dominate the information domain. *FM 3.0: Operations,* 6–16.

Jemaah Islamiyah. These terrorists were directly involved with the 2003 Marriott Hotel bombing and the 2004 Australian Embassy bombing in Jakarta, Indonesia, as well as the 2005 Bali bombings, among others.

The second step is to analyze the network. Social network analysis (SNA) has been utilized to analyze terror networks, regardless of the strategy being pursued and will be employed in this research as well. The use of SNA methodologies such as transforming link diagrams to one-mode networks, running centrality measures to describe network positions, and deducing sub-groups provide insight into how a network is potentially vulnerable to lethal targeting operations.[10] While SNA methods have been applied to understand social influence and messaging, they have not been operationalized for IO practitioners. The IO planner should use all available techniques (including SNA) to develop the best IO strategies against the network.

The identification of starting nodes for a target list comes from Borgatti's Key Player 1 analysis tool.[11] This software uses social network algorithms to generate lists of individuals who, if removed or expelled, would optimally fragment the network. Key Player 1 also generates lists of people who, if given a piece of information, will rapidly diffuse that information across the network. These are separate algorithms that generate separate lists, but I will demonstrate how a deception plan can make use of both.

The third step is to simulate how far across the network misinformation can travel given a certain set of starting points. For this exercise, I use ORA's Micro Simulation tool. This simulation takes the starting nodes identified as points for optimal diffusion by the Key Player tool and graphically shows, over time, what part of the network has received the message and what part has not.

Visualizing the reach of misinformation is important as it shows which nodes have yet to receive the new information during a particular time period. If the analyst realizes that nodes directly connected to our target node will not receive the

---

[10] Kathleen M. Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Networks," *Connections* 24, no. 3 (2002): 7992.

[11] Stephen P. Borgatti, "Identifying Sets of Key Players in a Social Network," *Computational, Mathematical and Organizational Theory* 12 (2006): 21–34.

misinformation in a timely manner, then we should adjust the number and selection of starting nodes to ensure we reach the "right" individuals. In this case, the "right" individuals are those directly connected to our node, who, if they believe the misinformation, will attempt to isolate or expel the untrusted target. Alternately, organizational leadership may use their influence to remove the targeted individual from his position in the network, causing the fragmentation effect we desire, but they must also have the opportunity to receive the misinformation before they can act.

Finally, analysts can use the information diffusion simulation to assist in creating an intelligence collection plan. There will be locations within the network that would make good places to use human intelligence (HUMINT), signals intelligence (SIGINT), and other intelligence resources to create a feedback mechanism that monitors the information environment for indicators that our misinformation is spreading correctly and that our deception plan is having an effect. This feedback must be in place before implementing the plan or we risk losing some of these indicators.

Although some factors of planning a thorough deception scheme are referenced herein, this thesis will only focus on the mechanism for choosing initial targets, the theoretical information diffusion that will occur by inserting messages at selected entry points, and possible locations for intelligence, surveillance, and reconnaissance (ISR) needed to observe and collect on the effectiveness of fragmentation and information diffusion. This mechanism applies to IO strategies as a whole, not only to deception. The manner in which our misinformation is inserted into the network is not within the scope of this thesis, but may include information enablers such as Military Information Support Operations (MISO), Public Affairs, leader engagement, military cyber capabilities and so forth, to covertly and overtly insert and reinforce communications, messages, misinformation and truthful information.

E. CHAPTER REVIEW

I introduce the problem and research question in Chapter I. Chapter II is a review of literature relevant to nonlethal strategies. It begins with an overview of Information Operations doctrine and methods, as IO strategies tend to focus on nonlethal methods.

Next, it reviews influence theory, social movement theory, as well as network destabilization techniques. Chapter III describes the data set and the research design that culminates in a simulation to explore the theoretical reach of misinformation across our network. Social network analysis methods applicable to this research are also discussed. Chapter IV summarizes the results of the simulation that measure the level of disruption in a network using fragmentation, the extent of information diffusion, as well as potential places in the network for further intelligence collection. Chapter V discusses this analysis and how it applies to the creation of a deception scheme. Limitations of the research design and methods are also discussed. Chapter VI contains recommendations for IO planners and military commands on the pursuit of deception strategies. Follow-on research is also suggested.

II. LITERATURE REVIEW

A. INTRODUCTION

The importance of IO in military operations begins in doctrine, yet understanding the viability of IO input into the creation of nonlethal strategies for network disruption must begin with an understanding of the broad categories of *influence theory*, *social movement theory*, and a growing corpus of *network destabilization* techniques. In order to influence a target group, whether an individual or a massive foreign audience, we must understand what motivates people to make decisions and join organizations, how social factors heavily impact human reactions to messages and ideas, and how to engineer these social factors to work in the favor of U.S. forces. Only by understanding the forces that work to bind people together can deception strategy begin to formulate plans on how to unbind them. Although this thesis uses a deception plan as the vehicle for a nonlethal IO strategy, other elements of IO are served by the literature review that follows.

B. IO DOCTRINE AND METHODS

There is much confusion and misunderstanding about information operations, both in doctrine and in practice. Constantly changing doctrine, terms, staff functions, and a variety of best practices have not made it easy for the IO practitioner to establish legitimacy in the targeting process.[12] The most recent and definitive definition of IO comes from a 2011 memorandum from Secretary of Defense Roberts Gates, in which he

---

[12] Joseph L Cox, "Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?" monograph, Fort Leavenworth, KS: United States Army Command and General Staff College (2006).

defines IO as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[13]

Joseph Cox, a student at the U.S. Army's School of Advanced Military Studies wrote, "Perhaps it would be better if commanders thought of IO as a combination of four functions: influence, inform, attack and protect, whose coordinated use produces an effect on the battlefield greater than merely adding the results of the individual functions together."[14] Since influencing the enemy commander is the primary objective of deception,[15] this thesis narrows the review of IO methods down to the essentials of influence with little consideration to the inform, attack, and protect aspects.

Although not an exhaustive list, the commander generally has three primary influence arms available for his IO influence strategy, not including the use of military force as a deterrent or coercive measure. The first method is key leader engagements (KLE), the second is Military Information Support Operations (MISO) and the third is military deception operations (MILDEC). A related capability is Public Affairs operations, which provide information to audiences but do not primarily seek to influence behaviors.

1. Leader Engagement

In some circumstances, the commander may conduct leader engagements personally with so-called "influential" members of the target audience. In others, he may direct meetings with subordinate leaders or request assistance from higher echelons when the appropriate community or network leader falls outside his sphere of influence. These

---

[13] In 2011, Secretary of Defense Robert Gates approved a definition of IO as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." Robert Gates, "Strategic Communication and Information Operations in the DoD," memorandum (January 25, 2011).

[14] Cox, "Information Operations," 3.

[15] For instance, Latimer argues that "in battle it is not sufficient for a commander to avoid error; he needs actively to cause his enemy to make mistakes." Jon Latimer, *Deception in War* (Woodstock, NY: Overlook Press, 2001), 1.

leader engagements are normally designed to influence behaviors by building trust and confidence in the other party.[16] It may be the case that an individual occupies a leadership position, but the real influence may lie in a subordinate who controls monetary contracts or someone outside the leadership circle who knows the "scoop" on everyone. Who the "influential" members are is a matter of debate and properly identifying them is the aim of the research techniques presented in Chapter III.

2. Military Information Support Operations (MISO)

Military Information Support Operations (MISO), otherwise known as psychological operations, or PSYOP, provides the commander a vector into the psychological needs and susceptibilities of a target audience. The purpose of PSYOP is "to induce or reinforce foreign attitudes and behavior favorable to U.S. national objectives. PSYOP are characteristically delivered as information for effect, used during peacetime and conflict, to inform and influence."[17] IO strategies using MISO often are wide reaching, but may look at influencing individual behaviors in addition to masses of people.

MISO are "employed to counter adversary propaganda and to sow disaffection and dissidence among adversaries to reduce their will to fight and ultimately to induce their surrender."[18] Since the mission of MISO is to "influence the behavior of foreign target audiences to support U.S. national objectives," it is possible to use the skills and assets of MISO operatives to change behavior at the individual and organization level.[19] One behavior change is defection from the organization, mentioned above. Others may include reconciliation, surrender, or movement to areas less conducive to the network's growth and sustainment.

---

[16] Jimmy A. Gomez, "The Assessments Process in Contemporary Operating Environment," Small Wars Journal, June 22, 2011. http://smallwarsjournal.com/jrnl/art/the-assessments-process-in-contemporary-operating-environment.

[17] United States Army, *Field Manual 3–05.30: Psychological Operations*, Washington, DC: Department of Defense (Apr 2005): 1–1.

[18] Nancy Roberts and Sean F. Everton, "Strategies for Combating Dark Networks," *Journal of Social Structure* 12, no. 2 (2011): 6.

[19] *FM 3–05:30: Psychological Operations*, 1–2.

Understanding message diffusion is important to the MISO plan. Everton asserts that a powerful use of information diffusion is to convince members of a network to defect. Studies have shown that a defection is much more disruptive to an insurgency than the death of a member.[20] This is because of the leaders of the insurgency are uncertain what the defector has told the authorities, so generally, the organization must change procedures, reevaluate operational plans, and lie low.[21]

3. Military Deception Operations

Deception operations often are aimed at the cognitive processes of an adversarial force by influencing the opposing commander to make decisions based on what he *thinks* he sees or knows rather than what is *actually* going on. The Army defines military deception as "those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[22]

One way to execute a deception is to send messages crafted in a way to cast doubt on the integrity or trustworthiness of a particularly important individual. Several principles of good deception make this possible. First, the deception must reach those actors who have the authority and ability to cause the target to be rejected from the network.[23] These decision makers are likely to be within the core of the network and may be isolated from receiving messaging efforts directly from military-controlled assets. Second, the timing and delivery of any misinformation efforts must ensure a consistent and credible narrative.[24] Third, the effectiveness of the deception hinges on causing the decision maker to believe what he already expects.[25] Finally, creativity and imagination

---

[20] Sean Everton, *Disrupting Dark Networks*, (New York and Cambridge: Cambridge University Press, 2012), 36–37.

[21] Everton, *Disrupting Dark Networks*, 37.

[22] *FM 3.0: Operations*, 6–108.

[23] Latimer, *Deception*, 60.

[24] Latimer, *Deception*, 67–69.

[25] Charles A. Fowler and Robert F. Nesbit, "Tactical Deception in Air-Land Warfare," *Journal of Electronic Defense* (June 1995): 42–42.

are necessary to navigate through the factors of social influence that are the primary resistors to an effective deception operation.[26] Only when these factors of deception are planned for should the IO strategist attempt to execute the program with any reasonable expectation that the intended outcome will come to pass.

Another important factor to consider is whether the recipients of our information can actually piece together the same picture we had intended to send. *Type-M* deceptions ("misleading") attempt to reduce ambiguity and point to a very clear, attractive picture in the wrong direction.[27] If the misleading information is about the trustworthiness of a network member, then all hints and injected messages must help the decision makers come to the conclusion that our target must not be trusted. The opposite type of deception, *Type-A*, or ambiguity increasing, actually obscures the truth and makes it more difficult for a decision maker to make any conclusions about our intentions. This is counter-productive to network fragmentation effects in this context.

C.   INFLUENCE THEORY

The first broad category of influence concerns influence and social networks, and begins with an understanding of social psychology. The broad field of social psychology attempts to study individual-to-individual interaction, individual-to-group interaction, and group-to-group interaction. Major divisions within this field include *social influence*, *group dynamics*, and *interpersonal relations*. Important topics within social influence are conformity, compliance, and obedience.[28] These topics set the foundation for engineering influence operations.

1.   Social Influence

Two motives drive social influence: normative and information influence. *Normative influence* describes how people conform in order to be socially accepted. Peer

---

[26] Fowler and Nesbit, "Tactical Deception," 76.

[27] Donald Daniel and Katherine Herbig, *Strategic Military Deception* (New York: Pergamon, 1982): 6.

[28] "Social Psychology," *Wikipedia*. Accessed September 5, 2012. http://en.wikipedia.org/wiki/Social_psychology.

11

pressure is a form of normative influence.[29] Reciprocation is another. Cialdini describes the powerful effect of reciprocation, or that feeling that one should try and repay what another has done for him.[30] Even when a person would not normally be inclined to act, reciprocity creates an obligation for repayment of what was provided. A free sample of a product or a flower handed out by a solicitor is another method of creating this feeling of reciprocation. *Information influence* describes how people will seek information to create a correct or acceptable response. Cialdini says this method of conformity lies in the principle of social proof. When one is uncertain about how to act in a scenario, the normal response is to see how others act. For instance, in 1964, thirty-eight neighbors allegedly witnessed a murder in Queens and not one of them called the police, obviously anticipating someone else would do it.[31] In emergency situations where someone takes a leadership role and directs perfect strangers to do tasks, such as phone the police or divert traffic, response is immediate.[32] This is the result of social proof. Research within social influence includes famous studies like Milgrim's electric shock experiment[33] and Asch's line estimation experiment.[34]

2.   Rules of Social Influence

Included in influence theory are factors of our social network that guide our actions, attitudes, and beliefs. Christakis and Fowler describe five rules that illustrate the power of the interconnection of people and relationships.[35]

---

[29] Cialdini and his associates have found that information programs that emphasize injunctive normative influences (what one *ought* to do) are much more influential than those that focus on descriptive norms (what normally is done) or when no focus is made on norms at all. See Robert B. Cialdini and Linda J. Demaine, et al., "Managing social norms for persuasive impact," *Social Influence* 1 no. 1 (2006): 4–5.

[30] Robert B. Cialdini, *Influence: The Psychology of Persuasion*, New York: Harper Collins (2007), 17.

[31] Cialdini, *Influence*, 129–130.

[32] Cialdini, *Influence*, 139–140.

[33] Stanley Milgram, "Behavioral Study of Obedience," *Journal of Abnormal and Social Psychology* 67 (October 1963): 371–378.

[34] Solomon E. Asch, "Opinions and Social Pressure," *Scientific American* 193, vol 5 (November 1955): 31–35. Asch's experiments have been found to confirm the strength of normative influence and also show that uncertainty can be created when social proof and actual observations differ. See John C. Turner, *Social Influence,* Bristol, PA: Open University Press, 1991.

[35] Nicholas A. Christakis and James H. Fowler, *Connected* (New York: Little, Brown and Company, 2009): 17–26.

Rule 1: We shape our network. We each decide the structure of our network by choosing how many people we are connected to and the strength of those connections. Our natural tendency is to associate with people who are like us. This is called homophily, or literally "love of being alike."[36] We join clubs based on our interests and belong to churches where others believe as we do. The inclusion or exclusion of people from our networks is often by choice, but sometimes circumstances such as geography, family make-up, and societal factors determine to whom we are connected.

Rule 2: Our network shapes us. The number of friends and connections within our network has a significant influence on how we see the world. Christakis and Fowler argue that "having an extra friend may create all kinds of benefits for your health, even if this other person doesn't actually do anything in particular for you."[37] Being in a tight-knit military unit where each person has close connections to everyone else is different than being in a job where the only interaction is reporting results to a supervisor. The networks we belong to provide us meaning and constrain our behavior more than we realize.[38]

Rule 3: Our friends affect us. The shape of our networks is not the only thing that matters. Information and resources that flow across connections matter as well. In addition to advice and the comfort of friendship, the influence of friends can alter our behavior and attitudes. Christakis and Fowler argue that we often mimic and influence those around us. For instance, they found that students performed better with roommates who were studious or that homeowners kept up their own lawns when they had a neighbor who was an avid gardener.[39]

Rule 4: Our friends' friends' friends affect us. Christakis and Fowler also studied the effect of overweight friends on each other. Their conclusion? An obese person "was more likely to have friends, friends of friends, and friends of friends of friends who were

---

[36] Christakis and Fowler, *Connected*, 17.

[37] Christakis and Fowler, *Connected*, 20.

[38] Sean Everton, *Disrupting Dark Networks*, 5.

[39] Christakis and Fowler, *Connected*, 22.

obese than would be expected due to chance alone."[40] Beyond this, though, there was no evidence of influence. This is the "Three Degrees of Separation" rule, which posits that we both influence and are influenced by those three steps away from us. The amount of influence may wane the further someone is from us, but there is still some measurable effect until that third step.[41]

Rule 5: The network has a life of its own. The simplest method of ascertaining a person's connections is to ask him; however, there are attributes and functions of a network "that are neither controlled nor even perceived by the people within them. These properties can be understood only by studying the whole group and structure, not by studying isolated individuals."[42] Traffic jams, stampedes, and the wave at sporting events are examples of networks that cannot be studied by querying the individual.[43] Although closely linked to the same principles, the life a network has on its own is not quite the same as the field of group dynamics.

3.   Group Dynamics

Group dynamics researchers study the roles, relationships, norms, and interaction of individuals within a group. To a large extent, the social identity of humans depends upon group membership. Those within a group share a social identity, which influences behavior and perception towards members of the same group and towards other groups.[44] Those in the same group are viewed favorably and those external to the group receive some measure of negative perception or perhaps discrimination. The sum total of group membership and the behaviors and perceptions that each group imparts on the individual ultimately define the identity of the individual himself.[45] Other categories within group

---

[40] Christakis and Fowler, *Connected*, 108.

[41] Christakis and Fowler, *Connected*, 27–28. The premise of three-degrees of influence has been challenged on mathematical and statistical grounds. See Everton, *Disrupting Dark Networks*, 247.

[42] Christakis and Fowler, *Connected*, 24–25.

[43] Ibid.

[44] Henri Tajfel and John C. Turner, (1986). "The Social Identity Theory of Intergroup Behavior," in S. Worchel and W. G. Austin (Eds.), *Psychology of Intergroup Relations* (Chicago, IL: Nelson-Hall, 1986): 7–24.

[45] Tajfel and Turner, "Social Identity Theory," 7–24.

dynamics include group decision-making, which includes polarization and groupthink, social identity, and task efficiency or productivity.[46]

4.   Interpersonal Relations

Interpersonal relations are closely related to social exchange theory. This theory posits that all human interactions and relationships use a subjective cost-benefit analysis to find a point of stability. This stability is when the interests of both parties are considered. Michael Roloff said, "The guiding force of interpersonal relationships is the advancement of both parties' self-interest."[47] The particular worth of a relationship is calculated by the rewards minus the costs.[48] This is salient for influence operations as increasing the costs of maintaining the relationship or breaking a relationship is one objective of coercive influence that might be used in a deception operation or via a series of leader engagements. Additionally, leader engagement strategies depend entirely upon the quality of relationship that can be established with a target audience. The trust created in a relationship between a senior U.S. leader and a tribal sheikh, for instance, can influence the reaction an entire tribal area has towards U.S. forces.

5.   Influence Operations

Last, influence theory continues with definitions of *influence operations*, in particular, how military organizations can use influence to achieve objectives within the social domain. Influence operations are those that aim to "induce desired changes in the attitudes and behaviours of enemies."[49] U.S. Joint doctrine defines influence as operations that "cause others to behave in a manner favorable to U.S. forces."[50] The U.S. Army defines influence as a line of effort that "effectively changes attitudes, beliefs, and

---

[46] "Social Psychology," *Wikipedia*. Accessed September 5, 2012. http://en.wikipedia.org/wiki/Social_psychology.

[47] Michael Roloff, *Interpersonal Communication: The Social Exchange Approach* (Beverly Hills: Sage Publications, 1981).

[48] P.R., Monge; N., Contractor (2003). *Theories of Communication Networks*. Oxford University Press, as quoted in http://en.wikipedia.org/wiki/Social_exchange_theory.

[49] Barbara D. Adams, Jessica Sartori, and Sonya Waldherr, "Military Influence Operations: Review of Relevant Scientific Literature," Toronto: Human Systems, Inc. (November 2007), 8.

[50] JP 3–13, "Information Operations," (13 February 2006), p. I-10.

ultimately behavior of foreign friendly, neutral, adversary, and enemy populations to support operations. Influence guides actors to make decisions that support the commander's objectives."[51]

There are two major methods of influence. The first is compliance and the second is persuasion. *Compliance* attempts to simplify change behavior in a manner favorable for the practitioner. It does not attempt to have the target internalize the reasons for the change in behavior. Sometimes, this behavior change is coerced through military might or force of law. Consider the sight of a patrolman with a radar gun on the side of a freeway. Invariably, the average speed of commuters goes down and drivers begin complying with posted speed limits. *Persuasion*, on the other hand, attempts to change the attitudes and beliefs of an individual. Persuasion targets the internal motivations for behavior change and usually sees a longer-lasting effect because of the internal advocacy towards the behavior change.[52] Traffic accident footage on the nightly news and safe-driver training programs may help a driver internalize the potentially dangerous effects of non-compliance with posted speed limits.

D. SOCIAL MOVEMENT THEORY

Related to influence and social networks is social movement theory. It provides insight into what types of ideas and norms actually constitute influence. This theory relies heavily on framing, which is a psychological device that offers a perspective and allows the person to adopt certain features but ignore others in order to influence subsequent judgment.[53] *Positive frames* and *negative frames* are opposite sides of the same coin. Using a positive frame to aid decision-making tends to reinforce less-risky choices, while examining the same decision with a negative frame tends to reinforce choices with more risk.[54] Research indicates that the human tendency to avoid loss is an even more powerful

---

[51] FM 3–0, C1, "Operations," (22 February 2011), p. 6–17.

[52] Kelton Rhoads, "Working Psychology," (2004), Accessed 5 September 2012, http://www.workingpsychology.com/definit.html.

[53] Rhoads, "Working Psychology," http://www.workingpsychology.com/whatfram.html.

[54] Amos Tversky and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science* 211 no. 4481 (1981): 453–458.

motivator for affecting choices. Negative frames tend to emphasize the prospect of a loss more than positive frames do. "Prospect theory… give[s] us an invaluable insight into human nature. We know that a human's first priority is not to lose--gains are secondary to the "no loss" rule. Thus, framing a decision in terms of possible loss should motivate a person more than framing the same decision in terms of possible gain."[55]

Kelton Rhoads, a Senior Mentor at the John F. Kennedy Special Warfare Center, explains the balance of positive and negative information. "Psychologists have long known of the existence of the "positivity bias," which states that humans overwhelmingly expect good things (as opposed to neutral or bad things) to occur. If perceivers construct a world in which primarily positive elements are expected, then negative information becomes perceptually salient as a jolting disconfirmation of those expectations. We also know that people stop to examine disconfirmations to a much higher degree than confirmations. Negative information is often highly informative and thus may be assigned extra weight in the decision-making."[56]

1.   Motivations of a Social Movement

Social movement theory argues that the motivations behind a movement are to forward the ideas and beliefs of some group, whether the ideas or beliefs are religious, environmentally based, or grounded on some other grievance or social cause. Meaning is created in the movement itself. "Movements function as carriers and transmitters of mobilizing beliefs and ideas, to be sure; but they are also actively engaged in the production of meaning for participants, antagonists, and observers."[57] If the meaning of a movement frames the beliefs and actions of a participant then in order to change the frame of a participant, one must change the meaning associated with the movement. There must be found a greater mobilizing belief or idea outside of the organization's frame for a participant to change his involvement in that organization.

---

[55] Rhoads, "Working Psychology," http://www.workingpsychology.com/riskybeh.html.

[56] Rhoads, "Working Psychology," http://www.workingpsychology.com/lossaver.html.

[57] David Snow and Robert Benford, "Ideology, Frame Reference, and Participant Mobilization," *International Social Movement Research* 1 (1988): 198.

If the beliefs and aims of the movement are motivation enough to join, participate, and enlarge the movement, then the IO practitioner must find a way to connect that person with a different movement or idea in order to change his involvement in the first movement. For instance, strategic framing can heavily affect how recruits are drawn into an organization, how these groups stay together, and what causes them to break apart.[58] *Frame analysis* is a method of understanding how people understand the world around them. Modifying frames through *alignment processes* is a contributing factor to changes in behavior. This is possible when new frames resonate stronger than current frames.[59] Using frame alignment processes, any IO strategy can attempt to influence individuals and clusters of individuals within a network. Put differently, influence can be enhanced by understanding structural traits of networks while frame analysis can help us understand how to put together influential narratives to plant in target networks.

2.   Frame Alignment Processes

Snow and Benford argue that there are four frame possible frame alignment processes, each of which are applicable to IO strategies. *Frame bridging* connects "ideologically congruent but structurally unconnected frames" regarding a specific problem set.[60] Frame bridging seeks out unmobilized pools of individuals who have similar sentiments opinions. These data are often found from public opinion polls or rosters of group membership.[61]

---

[58] David A. Snow, E. Burke Rochford, Jr., Steven K. Worden and Robert D. Benford, "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review* 51, no. 4 (Aug., 1986): 464.

[59] Snow and Benford argue that three framing tasks that motivate people for behavior change (mobilization, in the case of social movements). These tasks are: "a) diagnostic framing for the identification of a problem and assignment of blame, b) prognostic framing to suggest solutions, strategies, and tactics to a problem, and c) motivational framing that serves as a call to arms or rationale for action." See David A. Snow and Robert D. Benford, "Ideology, Frame Resonance, and Participant Mobilization," *International Social Movement Research* 1 (1988): 197–217 as quoted in http://en.wikipedia.org/wiki/Frame_analysis.

[60] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 467.

[61] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 467–468.

Frame amplification clarifies and invigorates "an interpretive frame that bears on a particular issue, problem, or set of events."[62] Amplification of particularly poignant values and beliefs in the target audience is a strong mobilizing tactic, especially when amplification convinces a moral obligation to act.[63]

Frame extension expands the boundaries of a "movement's primary framework so as to encompass interests in points of view that are incidental to its primary objectives but of considerable salience to potential adherents."[64] Sometimes the values of the movement are not readily inherent in the target population so it is the obligation of the movement to expand its framework to include points of view with which the target more readily identifies.[65] This does not mean that the movement must compromise its values or original framework by adopting counterproductive points of view, rather, finding common points of interest to discuss in a leader engagement rather than press just the U.S. agenda is an example of frame extension.

Last, *frame transformation* is a "systematic alteration" of extant frames that do not resonate with the movement's frames.[66] The goal of frame transformation is to make an issue that was originally taken for granted into a problem that is in need of repair.[67] For instance, impoverishment may be internalized as a part of life meant to be endured, but through frame transformation, a person may see that the problem lies externally and is the fault of food-hoarding warlords. An extension of this type of transformation is a change of global interpretive frames, or when an individual has a thorough conversion to a new "universe of discourse."[68] This means that future decisions and interpretations of life are seen through a lens that was previously non-existent. Religious conversion (and not even in an extremist way) may take on this global transformation. The final

---

[62] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 469.

[63] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 470–471.

[64] Snow, Rochford, Worden, Benford, "Frame Alignment Processes,"472.

[65] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 472.

[66] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 474.

[67] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 474.

[68] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 475.

consideration is that the initial frame of a target is varied and cannot be assumed. Factors such as influence received from membership in other groups might not be visible to the IO analyst and might skew the understanding of the initial frame. Similarly, once a frame alignment has taken place, this new perspective cannot be taken for granted as conditions change and alignment may shift.[69]

When the movement is violent, dangerous, or targeted by security forces, it makes sense to convince a participant that remaining in the movement is a negative frame that leads to risky behavior. Even within risky organizations such as a dark network or terrorist group, individuals hope for a good outcome or that their efforts are necessary to furthering the cause. Reframing this hope to something like despair or futility is one way to change the mobilizing belief behind an individual's commitment to the movement.

Studies on trust and social change have shown that people join networks based on pre-existing ties rather than on ideology alone.[70] This is insightful for IO targeting because it would identify nodes, relationships, preexisting conditions, and environmental factors taken into the context of the network's setting. These conditions and factors can be easily correlated with social movement frame analysis methods mentioned above. While the structural approach of social network analysis primarily identifies specific traits of nodes and ties, the second category sheds light on what makes networks emerge and stay cohesive over time. This distinction is not trivial. Where SNA might identify a particular broker of information or resources, without understanding how and for what motivations that individual actually controls the flow of a resource, an IO strategy may not be effective.

E.   NETWORK DESTABILIZATION

With influence and frame analysis, the goal is arguably to disrupt and destabilize target networks. And this is the main contribution of the third broad category. It focuses on specific techniques to destabilize networks, especially dark networks trying to remain

---

[69] Snow, Rochford, Worden, Benford, "Frame Alignment Processes," 476.

[70] Rodney Stark and William S. Bainbridge, "Networks of Faith: Interpersonal Bonds and Recruitment to Cults and Sects," *American Journal of Sociology* 85, no. 6 (1980): 1376–1395.

hidden, and the potential dynamic consequences of network destabilization. Applied to IO, *deception operations* are one method of disrupting dark networks.[71] Successful *counterinsurgency techniques* (to include IO) have been applied to counter-gang operations.[72] Other methods are found in Davis (1992),[73] Moon (2008),[74] Carley, Lee and Krackhardt (2002),[75] and Tsevetovat and Carley (2005).[76]

In sum, it is evident that the above three categories of relevant knowledge are appropriate to selecting IO as an option for the military commander, however it is not clear how to operationalize these categories when applying IO methods. It is precisely the intent of this thesis to fill the identified gap in the literature. In short, IO should be less concerned with creating "themes and messages" and more focused on mobilizing target audiences through inform and influence activities with the result being a frame realignment that favors U.S. interests and the U.S. perspective.

F.   CONCLUSION

In summary, the purpose of studying social science and theories related to information operations is to develop accurate and consistent understanding of the motivations, structures, and properties of social interaction. The fields of social psychology, social influence, social movement theory, and frame alignment provides the IO strategist a starting point for identifying features of a target individual or target

---

[71] Anonymous, "Deception 2.0: Deceiving in the Netwar Age," unpublished paper (Task Force Iron, Iraq, 2009).

[72] Michael Freeman and Hy Rothstein, eds, "Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism," (Monterey, CA: Naval Postgraduate School, 2007).

[73] James Kirkpatrick Davis, "Spying on America: The FBI's Domestic Counterintelligence Program" (New York: Praeger, 1992): 73–95.

[74] Il-Chul Moon, "Destabilization of Adversarial Organizations with Strategic Interventions," Unpublished Doctoral Thesis (Pittsburgh, PA: Carnegie Mellon University, 2008).

[75] Kathleen M. Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Networks," *Connections* 24, no. 3 (2002): 79–92.

[76] Maksim Tsvetovat and Kathleen M. Carley, "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence," *Journal of Social Structure* 6, no. 2 (2005).

network that might be susceptible to military influence operations. They also provide insight into how to help disrupt target organizations. This understanding also provides methods for measuring success as IO strategies are applied; if a behavior change is perceived because of military influence activities, then perhaps the behavior change can be documented, shared, and replicated across other military units.

III. METHODOLOGY

A. INTRODUCTION

Social network theories and methods identify various ways for analyzing network structure. Some of the more important ones included looking at networks in terms of critical nodes by measuring centrality scores,[77] while others look at tie strength[78] and critical relationships.[79] Analyzing a network in terms of its social structure is different than other analytic frameworks in the behavioral and social sciences.[80] Wasserman and Faust state that network analysis "provides a collection of descriptive procedures to determine how the system behaves, and statistical methods to test the appropriateness of the propositions. In contrast, approaches that do not include network measurements are unable to study and / or test such theories about structural properties."[81] The purpose of this thesis is to explore certain aspects of the structure of networks and describe how and why this is important to crafting a deceptive IO strategy.[82]

In this chapter, I introduce the data, SNA methods used, and the importance of the metrics chosen for analysis. I then introduce the software packages and the analytical steps used to illustrate recommendations for deception.

---

[77] Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, (Cambridge, UK: Cambridge University Press, 1994): 178–192.

[78] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, 78 (May 1973): 1360–1380.

[79] Wasserman and Faust, *Social Network Analysis*, 20.

[80] Wasserman and Faust, *Social Network Analysis*, 21.

[81] Wasserman and Faust, *Social Network Analysis*, 22.

[82] I do not cover every aspect of social network analysis in this thesis. There are many good introductory books and websites on SNA that can be used as a primer. For example, see Robert A. Hanneman and Mark Riddle, *Introduction to Social Network Methods*, Riverside: University of California, Riverside, 2005 (accessed November 5, 2012. http://faculty.ucr.edu/~hanneman/).

B. DATA

This chapter uses the Noordin Top terrorist cell data set (N=237) as derived from the 2006 and 2009 studies by the International Crisis Group.[83] These data have over 23 explicit and implied networks available for layering and aggregation studies as well as a substantial set of attributes discovered in several semesters of student projects.[84] I use the Noordin Top "operational" network as the basis for analysis, which is a multiplex, stacked network aggregated from the communications, logistical place, operations, financing, organizational, and training networks.[85] Below are the definitions for what constitute a tie in each of the various networks:

- "Internal communications: Defined as ties based on the relaying of messages between individuals and/or groups inside the network through some sort of medium.

- Logistical place: Defined as key places where logistical activity— providing materials, weapons, transportation and safehouses—occurred.

- Operations: Includes terrorists who were directly involved with the Australian Embassy bombing, the Bali I Bombing, the Bali II bombing and/or the Marriott Hotel bombing, either at the scene (e.g., suicide bombers, commanders) or as a direct support to those at the scene (e.g., driver or lookout). It does not include ties formed through communications, logistics, or organizations related to the operations

- Terrorist financing: Defined as the for-profit and not-for-profit businesses and foundations that employ members of the network.

- Terrorist organizational membership: Defined as an administrative and functional system, whose primary common goal is the operational conduct of terrorist/insurgent activities, consisting of willingly affiliated claimant members. Factions, affiliates and offshoots are considered separate from their parent organization.

- Training: Defined as participation in any specifically designated activity that teaches the knowledge, skills, and competencies of terrorism. It does

---

[83] International Crisis Group, *Terrorism in Indonesia: Noordin's Network,* (Brussels, Belgium: International Crisis Group, 2006); International Crisis Group, *Indonesia: Noordin Top's Support Base*, (Brussels, Belgium: International Crisis Group, 2009).

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

[85] Roberts and Everton, "Strategies for Combating Dark Networks," 8–9. Everton and Cunningham use a slightly different aggregation of this data set in a longitudinal analysis of Noordin Top's network. See Sean F. Everton and Dan Cunningham, "Detecting Significant Changes in Dark Networks," *Behavioral Sciences of Terrorism and Political Aggression*, (2012): 1–21.

not include participation in a terrorist sponsored act or mujahedeen activity in places such as Afghanistan, Bosnia, Chechnya or Iraq unless the individuals' presence was to participate in a specifically designated training camp or base in one of these areas."[86]

There are many combinations of subnetworks that could be used for analysis, each of which give a different view of network factors and social influences. An "appropriate" set of actors that have the ability to disconnect a targeted node greatly depends on which type of network or aggregated view of sub networks are being used for analysis. Providing misinformation that discredits a targeted node and ultimately disconnects that node from a logistical network may not disconnect him from the ties he has within the training or the communication network. Analyzing the ease or difficulty of severing ties within each type of sub network provides a more complete picture as to which nodes must be convinced that our target is untrustworthy and should be removed from the organization.

In this data set, individuals are coded as being dead, in jail, or free. I have removed individuals who are dead to demonstrate the current state of the network, but I include individuals who are currently in jail (as of the publication of IGC source documents). While arresting people has a disruptive effect on the network, it is likely that relationships remain intact and network fragmentation only truly occurs when a person is killed. Ties that may be dormant due to incarceration could be rekindled upon release or may still be valid methods of information diffusion strategies, as communication to others within the network may not be entirely cut off in most cases. Should an individual become free at some point, this analysis remains valid.

C.   ANALYTICAL APPROACH

1.   Overview of Analysis

In this thesis, I generate two lists of individuals using Borgatti's Key Player 1 tool. The first list identifies those individuals who, when removed, will optimally fragment the terrorist network. These become the high payoff target list (HPTL), and the object of our deception scheme. The second list identifies nodes that will rapidly diffuse

---

[86] Roberts and Everton, "Strategies for Combating Dark Networks," 25.

any information they receive. These nodes are starting points for a dissemination plan and will ideally carry the misinformation about our targets. I create a third list from social network and intelligence analysis. This third list of individuals is actually the focus of our deception. These are the decision makers and personally connected nodes of those on the HPTL. Recall that the focus of deception is the mind of the adversarial commander, or in our case, those individuals who have the ability to degrade relationships and expel our targeted nodes.

Examining how far and how fast our misinformation travels is the purpose of simulation. ORA's Micro Simulation tool provides a graphical picture of which nodes have received the information and which nodes have not. When the simulation shows that decision maker nodes have had ample opportunity to receive and digest the misinformation about our targets, then the analyst knows when sufficient starting nodes and resources have been used. This simulated diffusion also identifies nodes that are candidates for further intelligence collection, thereby creating a feedback loop that can determine success or failure of the deception. It makes little sense to approach a source or install a phone tap on an individual who does not have the opportunity to receive the misinformation and pass it along.

There is a complementary relationship between fragmentation analysis and information diffusion in terms of IO strategies. When network fragmentation is the operational goal and nonlethal IO methods are the means (versus a kinetic capture/kill option), using KPP-NEG will identify which nodes should be removed, but KPP-POS can be used to seed incriminating information that will hopefully cause the network to isolate and expel our target. Micro Simulation can validate and map the smallest target set required to use as seed nodes that reach essential decision makers in the shortest time possible.

2. Social Network Analysis Fundamentals

Social network analysis methods generate lists of individuals that can be considered as starting points for IO strategies. Analysts using SNA will sometimes use centrality measures to recommend individuals that are more central in the network.

Betweenness, degree, closeness, and eigenvector centrality are common measures and often used in the formulation of network disruption strategies.[87] Betweenness centrality measures the frequency with which a particular node lies on the shortest path between other nodes. An individual with high betweenness may be considered a broker. Degree centrality is a measure of the number of ties a node has. Someone with high degree knows a lot of people. Closeness centrality measures the number of steps individuals are from each other. This captures the "Six-degrees of Kevin Bacon" and other small world phenomena. Those with a high closeness score may have faster access to information. Eigenvector centrality is the measure of a node that is connected to those who themselves are more central to the network. In this thesis, I explore fragmentation based on high betweenness, degree, and closeness centrality.

Other measures of network structure may include identifying cohesive subgroups that highlight parts of the network with similar goals or who have a higher tendency to stick together.[88] IO influence targeting might assume that the diffusion of a behavior-changing idea should spread much faster in a network that has similar goals or values. Additionally, stacking techniques and aggregating several one-mode networks should also lead to insights in the ability to propagate influential messages throughout a network.[89] Finally, inefficiencies in the network appear at the extreme edges of centralization (either too hierarchical or too decentralized) or at the extreme edges of density (either too sparse or too dense).[90] IO strategies that disrupt efficiencies would likely see the network move towards one of these extremes. This becomes useful in measuring a strategy's effectiveness.

In crafting IO strategies, an analysis of the network's nodes and relationships is required prior to creating messages, recommending a MISO dissemination plan, or scheduling key leader engagement meetings. One approach is to craft strategies based on a ranking of nodes in terms of one or more centrality score, but because highly central

---

[87] Anonymous, "Deception 2.0," 7.

[88] Wasserman and Faust, *Social Network Analysis*.

[89] Everton, *Disrupting Dark Networks*, 50.

[90] Sean Everton, *Disrupting Dark Networks*, 136.

nodes are sometimes located close to one another, it is not always optimal to target all of them for removal or diffusion. Consequently, I turn to Borgatti's key player algorithms, which, as I discuss in more detail below, identify the optimal sets of nodes that most efficiently fragment the network or diffuse information.[91] Borgatti argues that network fragmentation and information dissemination using Key Player methods is superior to targeting actors based on centrality scores alone.[92]

Individuals who are expelled from the network or who sever association voluntarily may have residual ties that are difficult to map or predict, so I simplify the fragmentation model by assuming that the network has received sufficient information that the remainder of the actors in the network expel the targeted node and cut all ties.

There are two factors that heavily influence the ability to predict a fragmentation of this type. The first is that the appropriate actors in the network receive enough information to doubt the trustworthiness of the targeted node and the second is that they act on that information in a manner that will effectively make the target socially "dead."

3.   Simulating Reach of Information Diffusion

Doubting the trustworthiness of an individual requires the judge to overcome existing biases that caused a degree of trust in the first place. The idea of cognitive biases helps humans make decisions when presented with new information. One important bias is that of anchoring, which is that new information is judged against a previous starting point or anchor.[93] Adjustment is made from the anchor point rather than from "scratch." Injecting misinformation about a target's trustworthiness will almost certainly cause an evaluation starting from the anchoring point of what the recipient already knows or the reasons why he trusts the target to begin with. If the judge feels that acting on the new

---

[91] Stephen P. Borgatti, "Identifying Sets of Key Players in a Social Network," *Computational, Mathematical and Organizational Theory* 12 (2006): 21–34.

[92] Specifically, Borgatti identifies betweenness centrality as the measure most closely related to the effect of his KPP-NEG algorithm. Borgatti, "Key Players," 23.

[93] Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Tel Aviv: Tel-Aviv University, Jaffe Center for Strategic Studies, 1988), 111.

information is less costly than the risk of keeping an untrusted agent in the network, then he will adjust his cognitive assessment (and ultimately his actions) towards removing the untrusted agent.

Unfortunately, simulating a change in cognitive biases (the inner workings of the human brain) is extremely difficult and is beyond the scope of my study. However, simulating the ability for information to diffuse through a network may indicate which actors have had the *opportunity* to see incriminating information about our target and who may reevaluate their perception of the target. Simulating diffusion of information may also be useful for evaluating the effectiveness of propaganda programs, marketing, or mass media reach.

Simulation is not as simple as selecting starting nodes and letting the computer predict the reach of the message, though. Even with the ability to factor in the resistance of message adoption (as ORA's Micro Simulation tool allows), it is far more complicated to know which individuals will be receptive to a message and which will not. Studies have shown that social influences more than three steps from each other are negligible.[94] If an IO plan requires that a particular message gets delivered to a specific individual (for instance, the misinformation that a supplier is stealing supplies and should not be trusted), then it may be useful to start that rumor at a source less than three steps from the intended recipient. The ability to access a node within this targeted reach is something to consider when choosing message delivery methods and sources.

Another consideration of simulations is the assumption that the network will remain constant between time slices. In actuality, networks constantly evolve over time as actors enter and exit the network or ties between actors change. It may also be the case that the content of a message may influence the network to adapt. Conversely, the network can change the content of the message long before it reaches the simulated reach, thereby altering the amount of resistance or paths of propagation originally simulated. Christakis and Fowler identify instability in both the network and the message beyond three degrees that could affect the accuracy of the simulation. *Intrinsic-decay* is

---

[94] Christakis and Fowler, *Connected*, 28–30.

related to the message changing as it passes from point to point, akin to the childhood game of "telephone." *Network-instability* relates to the instability of ties due to the changing nature of the network that makes ties beyond three steps unstable.[95]

The second factor focuses on the whether those with the ability to kick out our target will choose to do so. Since the messages about the target node are most certainly to be deceptive in nature, it is also important to apply some principles of good military deception in crafting a misinformation plan that will end in a fragmented network.

Finding the appropriate actors who have the authority and ability to expel a targeted node requires significant insight into the network itself. It is not enough to see a simple sociogram (i.e., network map) and run network analysis metrics in a vacuum. The human factors outlined in Chapter II include social movement theory, interpersonal relations, and other factors of social influence. The depth of knowledge required to incorporate social factors into a deception strategy is not trivial. Understanding the particular reasons that caused the network to form the way it has or operate in its own particular manner is critical to the IO planner in choosing how, where, and more importantly, why to send particular bits of information to certain individuals.

D.   ANALYTICAL SOFTWARE USED

1.   Key Player

When developing IO methods to fragment a network, nodes identified using Borgatti's key player algorithms become targets for deception operations or social influence plans, such that the rest of the network expels them or their effects are marginalized. Insertion of the deception message or affecting the social influence framework can be done via MISO, key leader engagement, or other means through general broadcast or through specific diffusion nodes as described next. When message diffusion is the operational requirement, Borgatti's algorithms identify a message's insertion points, which can be done by key leader engagement, MISO, or through private messages like e-mails and texts.

---

[95] Christakis and Fowler, *Connected*, 28–29.

I operationalize the effects of fragmentation by using Borgatti's Key Player algorithm and ORA to identify the optimal nodes for deception targeting and show the fragmentation effect when these nodes are removed. Borgatti's software program, "Keyplayer 1," seeks to identify the optimal set of actors whose removal either disconnects or significantly fragments the network. These algorithms are also available in the software package, UCINET.[96] Two variations of the algorithm exist. One (KPP-NEG regular) uses the standard measure of fragmentation to gauge how much various sets of actors fragment the network when they are removed from the network. That is, a fragmentation score is calculated both prior to and after the removal of each of the sets, and the set that increases the level of fragmentation the most is considered optimal. The other (KPP-NEG distance weighted) is similar to the first except that rather than using the standard fragmentation measure, it uses a distance-weighted measure that identifies the optimal set of actors whose removal lengthens the average distance (in terms of path length) between all pairs of actors in the network.[97]

To identify nodes for targeting I run both the regular and distance-weighted KPP-NEG algorithms in order to identify the key players for sets of size one through twenty. I then plot the regular and distance weighted fragmentation score against the size of each set in order to determine when adding additional nodes to the target list becomes less efficient. I also create a sociograms before and after each subsequent node removal to visualize the fragmentation effect.

Borgatti, recognizing that the removal of actors may not always be the best or desired strategy, developed an additional algorithm designed to find the optimal set of actors that can pass along information that reaches the highest number of other actors. Here again, he developed two variations on this diffusion algorithm. One (KPP-POS regular) simply counts the proportion of distinct actors reached by the set of key actors;

[96] For an explanation of the steps to identify key players in UCINET, see Everton, *Disrupting Dark Networks*, 271–277.

[97] Borgatti, "Key Player," 23.

the other (KPP-POS distance weighted) weights this calculation by the path distance between the set of key actors and all other actors in the network.[98]

2. Micro Simulation

To operationalize the effects of information diffusion, I use both the regular and distance-weighted KPP-POS measures to identify optimal nodes for information diffusion and ORA's Micro Simulation tool to show the extent of this diffusion.[99] From "Key Player 1," I create lists of one through twenty nodes for each measure.[100] Plotting both the regular and distance-weighted reach scores against the number of insertion nodes creates a graph indicating when adding additional nodes becomes less efficient.

I then run Micro Simulation in "Information Diffusion" mode, set at 0.0, 0.5, and 0.9 resistance factors, using the lists of one, five, and ten key players. These resistance factors model low, medium, and very high reluctance to adopt the message and pass it to connected nodes. Higher resistance replicates either a poorly resonating message framed inappropriately for that particular network or other social factors that make messages less likely to be acceptable or passed along. One, five, and ten key players are chosen for illustrative purposes only. I then measure the time steps required until maximum information diffusion and create sociograms that visually depict what portions of the network are likely to be affected by the misinformation plan.

Micro Simulation has several diffusion modes, but "Information Diffusion" best fits the aims of this research. This mode looks at every node that has a resource (a piece of information in our case) and iteratively passes the resource to all outgoing nodes based on link weight. If a transmission can beat the resistance factor, the resource is passed. The transmissions continue for a specified number of time periods, using the following rules:

1.   An agent can give away information it has access to.

2.   An agent retains information even after giving it away.

---

[98] Borgatti, "Key Players," 27.

[99] I use ORA version 2.3.6, build date of September 2011.

[100] I use KeyPlayer version 1.45.

3.	An agent never loses information it gains.

4.	An agent never stops giving away information.[101]

I simplify the diffusion model by assuming that the message is perfectly transmitted according to the above rules, and that neither the message nor the network changes between time periods. These time periods are arbitrary and can reflect minutes or days. In actuality, the information may not diffuse uniformly because the communication patterns of individual agents do not necessarily line up with our chosen time periods.

As a final point, simulation has the added benefit of identifying nodes of interest that can potentially be used to provide feedback. It is a much more useful to have intelligence feedback about the effectiveness of diffusion already in place before delivering a message. If simulations show that certain parts of the network consistently are involved in spreading the message, than this is an area to assign intelligence resources to confirm or deny successful diffusion. Intelligence assets can also assist in identifying if the message is being altered as it propagates or if the network is shifting to adapt to the content of the message. This new information may be fed into simulations again to identify possible outcomes or prepare for contingencies.

## E.	METRICS OF INTEREST

### 1.	Fragmentation

The definition and meaning of both fragmentation and diffusion are important here. There are several ways to measure fragmentation. As Borgatti put it, "Perhaps the most obvious measure of network fragmentation is a count of the number of components. If the count is 1, there is no fragmentation. The maximum fragmentation occurs when every node is an isolate, creating as many components as nodes."[102] Maximal fragmentation in an insurgent network is not feasible, as this requires either eliminating every connection between individuals or removing every individual from the network. Removing every tie in the network is impossible, as some of our connections are blood

---

[101] ORA help file, "Micro Simulation."

[102] Borgatti, "Key Player," 26.

ties or other states of being rather than social or emotional connections. Removing every individual from the network through law enforcement or counter-insurgency operations is possible, but again, not feasible because of the amount of time and resources required as well as limitations in intelligence available on each node.

The normal *fragmentation score* in Borgatti's algorithm attempts to find solution sets that maximize the number of components created by removal of the set. The distance-weighted algorithm accounts for the reciprocal distance between nodes and weights a solution set based on transmission or transportation length in addition to trying to maximize the number of components created.[103] This is referred to as the *non-cohesion measure* in the "Key Player 1" software.

In this thesis, I compute distance-weighted fragmentation in addition to normal fragmentation, but generally display graphs based on the normal measure, as I can compare this measure against simple fragmentation based on node sets derived from centrality scores. I examine this comparison in Chapter IV.

2. Diffusion

According to Borgatti, diffusion is based on "the connection or cohesion that members of one set of nodes (the kp set) have with members of anther (the remainder of the network). To solve the problem, we need a direct measure of the amount of connection between a set and the rest of the graph."[104] The normal measure of diffusion (KPP-POS normal) uses a group degree centrality measure to identify the nodes of a given set size that maximizes the reach of the set.[105] This is measured in terms of the *percent of the network reached*.

The distance weighted diffusion score weights the solution set by the distance between linked nodes. This measure is referred to as the *reciprocal distance index* in the Key Player 1 software.

---

[103] Borgatti, "Key Player," 27.

[104] Borgatti, "Key Player," 28.

[105] Borgatti, "Key Player," 29.

Again, I calculate both normal and distance weighted measures, but I report the normal diffusion score to examine the percentage of the network reached by a set of nodes. Although simpler, this measure makes more intuitive sense than a reciprocal distance index and better explains the goal of operationalizing diffusion.

F.   CONCLUSION

In this chapter, I have identified the data and methods used in analyzing a terrorist network, looking for key nodes that would provide the most powerful fragmentation and information diffusion effects. Simulations help predict the extent of these effects. This analysis sets the stage for a discussion of the results and their implication for deception.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS AND ANALYSIS

A. INTRODUCTION

In this chapter, I identify the two sets of nodes generated through Keyplayer 1 and report fragmentation and diffusion scores. Next, I discuss fragmentation results and how centrality measures and Key Player fragmentation scores relate. Graphing the location of targeted nodes in the network and then graphing the structure of the network after removing these nodes provides a visual product that is useful in seeing how much the network would be affected by this fragmentation strategy. Next, I discuss diffusion results based on simulations and map the information as it flows through the network. I also show that sometimes the same amount of the network can be reached with a smaller number of starting nodes, thereby simplifying the targeting process somewhat.

B. KEY PLAYER ANALYSIS

The Key Player tool generates lists of nodes that optimize the extent of fragmentation or reach of diffusion, yet it does not prioritize the individuals within the list. Prioritization must be done elsewhere in the targeting process; however, lists made from centrality measures are prioritized based on the value of the respective centrality score. It is possible to assist prioritization of key player lists by using centrality scores, intelligence reports, and the commander's instinct to rank order a target set. It is extremely important to note that the Key Player list will change depending on the size of the list required. In other words, an individual who appears on a list of five may not be on the list of four targets or six targets.[106] It is also likely that Key Player will generate multiple solutions for certain list sizes. This means that there is more than one set of nodes for each list size that will provide the same fragmentation score. The lists of individuals will be presented in subsequent sections for both fragmentation and diffusion analysis.

---

[106] Borgatti calls this the "ensemble issue," which argues that certain sets of nodes produce a greater effect on the network than the sum of individual nodes would. See Borgatti, "Key Player," 24–25.

Having multiple sets of solutions is both a blessing and a curse to the targeting process. If further analysis reveals that a portion of one solution set is not readily accessible or if the IO strategy may not be successful, then switching to another solution set is an option. Unfortunately, it makes it difficult to direct intelligence assets onto a constantly changing list. Even though there are often overlaps of nodes between solution sets, care must be taken to ensure that the entire set is considered at the same time in order to expect a specific fragmentation result. Mixing and matching nodes into a custom solution may not be any more effective than randomly choosing targets, thereby defeating the whole purpose of network analysis.

I also generate lists of individuals from standard centrality measures (betweenness, closeness, and total degree). This allows for the comparison of fragmentation and diffusion effects between Key Player and centrality lists. It also indicates which individuals are likely the organization leaders and who should be the actual targets of our deception. Table 1 lists the top ten individuals based on their respective centrality scores, with higher scores indicating higher centrality.

Rank	Betweenness	Value	Closeness	Value	Total Degree	Value
1	Gun-Gun	0.090	Ubeid	0.027	Ubeid	0.293
2	Ahmad Rofiq Ridho	0.072	Chandra	0.027	Gun-Gun	0.278
3	Ubeid	0.062	Ahmad Rofiq Ridho	0.027	Chandra	0.273
4	Hambali	0.049	Hari Kuncoro	0.027	Hari Kuncoro	0.258
5	Chandra	0.045	Gun-Gun	0.026	Umar Patek	0.247
6	Abdul Aziz	0.044	Umar Patek	0.026	Ahmad Rofiq Ridho	0.232
7	Abdullah Sunata	0.038	Ali Imron	0.026	Ali Imron	0.217
8	Abu Bakar Ba'asyir	0.038	Umar2	0.026	Hambali	0.217
9	Usman bin Sef	0.035	Cholily	0.026	Umar2	0.217
10	Subur Sugiarto	0.035	Umar1 (Umar Burhanuddin)	0.026	Umar1 (Umar Burhanuddin)	0.202

Table 1.   Fragmentation list based on centrality measures

Table 2 is a summary of the Key Player analysis run against the Noordin Top network with dead individuals removed (n=199). As a reminder, KPP-NEG identifies the optimal set of nodes for fragmenting a network, and KPP-POS identifies the optimal set

of nodes for diffusing information through the network. The distance-weighted measures take into consideration path distances between nodes as described in Chapter III. Lists of up to 20 individuals are considered in the analysis.

# Nodes Used (target list size)	Fragmentation Score (KPP-NEG) [normal]	Non-cohesion Measure (KPP-NEG) [distance-weighted]	Percent network reached (KPP-POS) [normal]	Percent network reached (KPP-POS) [distance-weighted]
Base	0.330			
1	0.362	0.699	70.9%	53.8%
2	0.386	0.706	78.4%	62.1%
3	0.402	0.717	81.9%	67.5%
4	0.417	0.759	82.9%	71.8%
5	0.433	0.766	83.4%	74.3%
6	0.504	0.771	83.9%	76.5%
7	0.518	0.792	84.4%	78.1%
8	0.532	0.799	84.9%	79.1%
9	0.539	0.804	85.4%	80.3%
10	0.546	0.808	85.9%	81.2%
11	0.552	0.813	85.9%	81.7%
12	0.559	0.820	86.9%	82.4%
13	0.566	0.837	87.4%	82.7%
14	0.572	0.849	87.4%	83.2%
15	0.579	0.847	87.9%	83.9%
16	0.598	0.851	88.4%	84.4%
17	0.605	0.861	89.4%	84.9%
18	0.598	0.857	89.9%	85.2%
19	0.616	0.867	89.9%	85.7%
20	0.611	0.872	90.5%	86.2%

Table 2.   Key Player analysis summary measures for Noordin Top network with dead individuals removed (n=199)

C.   FRAGMENTATION ANALYSIS

I begin fragmentation analysis with a chart that compares the extent of network fragmentation of up to 20 nodes based on the KPP-NEG fragmentation score and centrality measures of betweenness centrality, closeness centrality, and total degree centrality. (See Figure 1.) The network has a baseline fragmentation score of 0.330, or 33%.
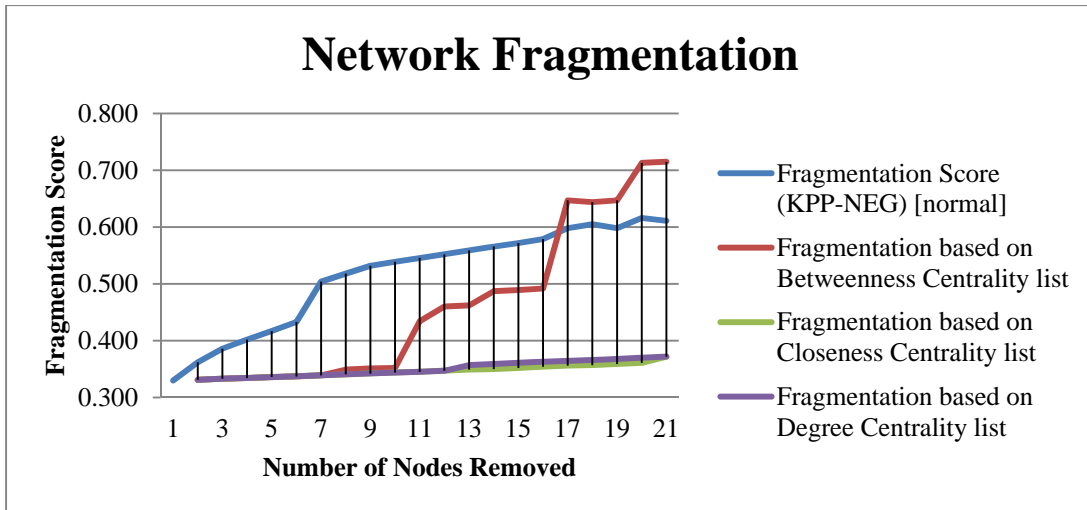
Figure 1. Graph of network fragmentation based on centrality measures and the Key Player fragmentation score.

Finally, Figure 2 shows sociograms (i.e., network maps) of the Noordin Top network before any fragmentation occurs and after removing the 10 nodes identified with Key Player. Although the number of isolated nodes has not substantially increased, there are now three significant components and a smaller three-person component that have been split away from each other.
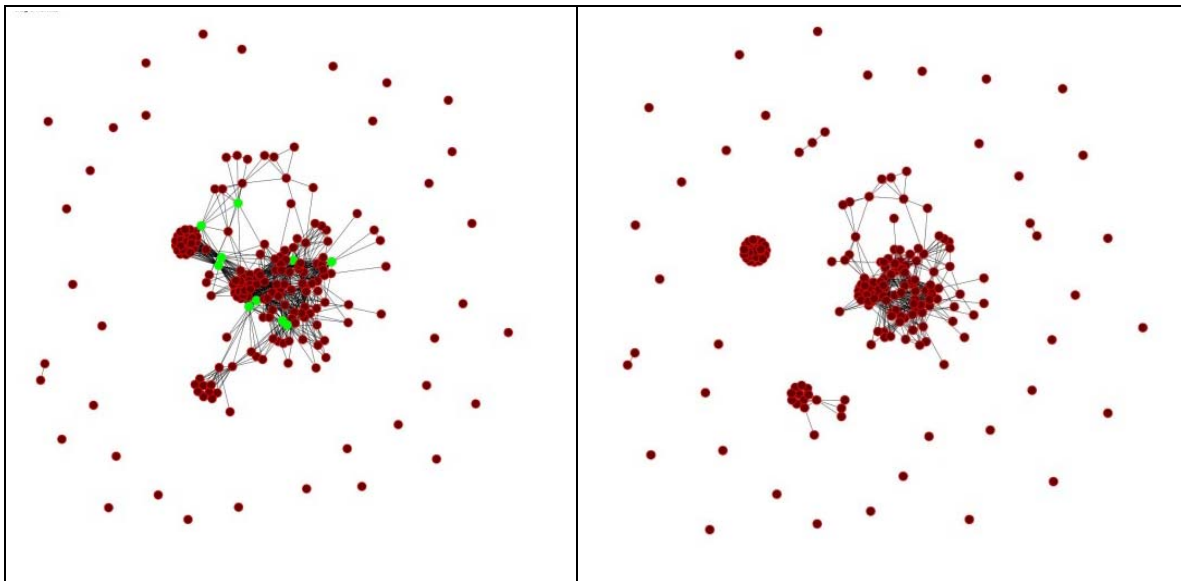

Figure 2. Left: Top 10 recommended deception targets identified by KPP-NEG normal, Right: Fragmentation results with targets removed (fragmentation = 0.546)

40

D. DIFFUSION ANALYSIS

For diffusion analysis, I use KPP-POS (regular) to identify key player sets of size one, five, and ten for illustrative purposes (see Tables 3, 4, and 5). This information identifies insertion points for ORA's Micro Simulation tool to model diffusion of a message and are insertion points for our deception plan. As noted in Chapter III, I run Micro Simulation set at 0.0, 0.5, and 0.9 resistance factors with the "Information Diffusion" option using all three lists to simulate difficulty of accepting the message and likelihood of passing it on.

Recommended diffusion target list (alphabetized) (KPP-POS [fixed size], 1 nodes, percent network reached = **70.9%**)			
Node ID	Name	Current Status	Technical Skills
32	Ahmad Rofiq Ridho	Jail	Bomb Maker, Courier

Table 3.   Recommended starting points for a diffusion plan (1 node)

Recommended diffusion target list (alphabetized) (KPP-POS [fixed size], 5 nodes, percent network reached = **83.4%**)			
Node ID	Name	Current Status	Technical Skills
24	Agus Ahmad	Jail	Facilitator
32	Ahmad Rofiq Ridho	Jail	Bomb Maker, Courier
49	Aris Susanto	Jail	Courier
54	Ayman al-Zawahri[107]	Alive	Strategist, Leader
183	Umar (Yemeni)	Alive	Bomber/Fighter

Table 4.   Recommended starting points for a diffusion plan (5 nodes)

---

[107] Note: Ayman al-Zawahri is the current spokesman/de-facto leader for al-Qa'ida. His inclusion in Noordin Top's network is incidental as he is obviously not a member directly involved with planning and coordinating operations with this network. This is a function of how Key Player Analysis looks for the ability to maximally reach anyone within the network who is not an isolated node. Al-Zawahri resides in a disconnected dyad, or pair of nodes, and is therefore included because of the key player algorithm design.

Recommended diffusion target list (alphabetized)			
(KPP-POS [fixed size], 5 nodes, percent network reached = **83.4%**)			
Node ID	Name	Current Status	Technical Skills
24	Agus Ahmad	Jail	Facilitator
32	Ahmad Rofiq Ridho	Jail	Bomb Maker, Courier
49	Aris Susanto	Jail	Courier
54	Ayman al-Zawahri	Alive	Strategist, Leader
82	Hasan (Saudi)	Alive	Bomber/Fighter
83	Helmi Hanafi	Alive	Facilitator
108	Jusuf Kalla	Alive	
118	Maslamah	Alive	Bomber/Fighter
142	Muhsin (Yemeni)	Alive	
148	Mustaqim4 (Ubeid's brother-in-law)	Alive	

Table 5.   Recommended starting points for a diffusion plan (10 nodes)

I also graph the diffusion over five theoretical time periods, assuming that both the network and the message will not change between time periods and that each node communicates uniformly. Figure 3 shows the reach of diffusion of one, five, and ten nodes over time at 50% resistance, while Figure 4 shows the same information at 90% resistance. At 50% resistance, it is interesting to note that both five and ten node sets provide similar message reach over time (82.4% and 84.9%, respectively) and a seed node of one reaches 77.4% of the network in the same time. When resistance to the message increases to 90%, the reach of diffusion drops off significantly. Ten seed nodes still reach the same 84.9% of the network, but one and five nodes only reach 47.2% and 65.3% of the network, respectively.
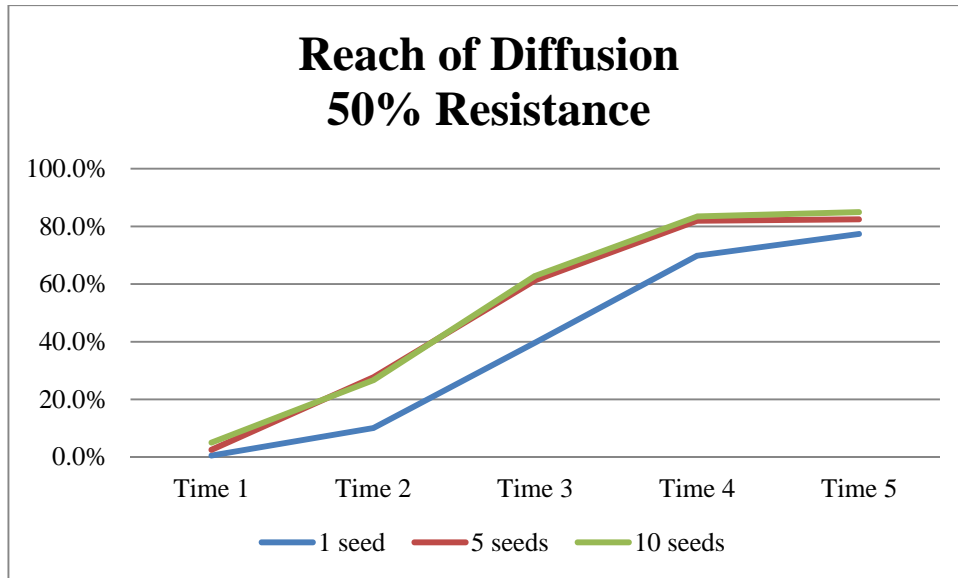
Figure 3. Percent of network reached over time using 1, 5, and 10 key player "seed" nodes at 50% resistance.
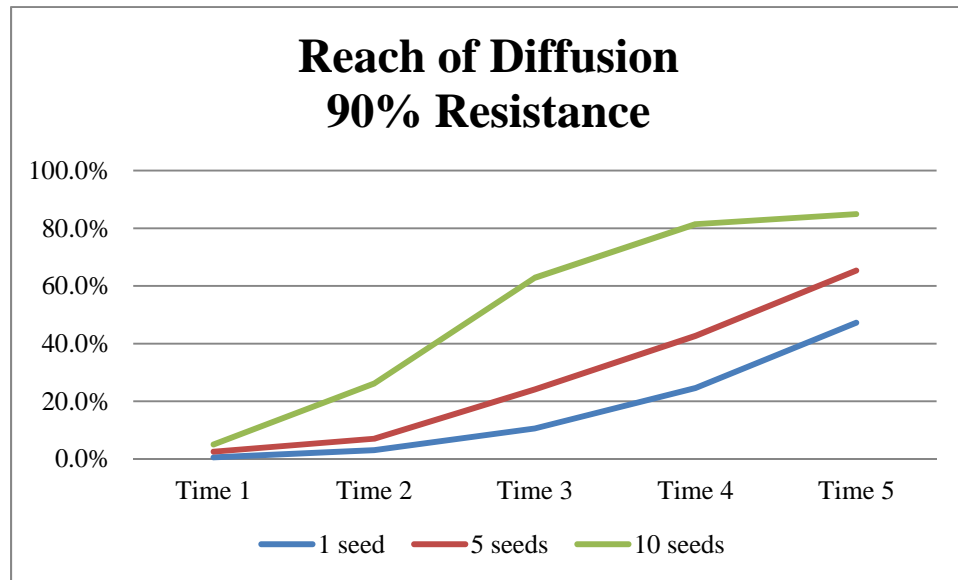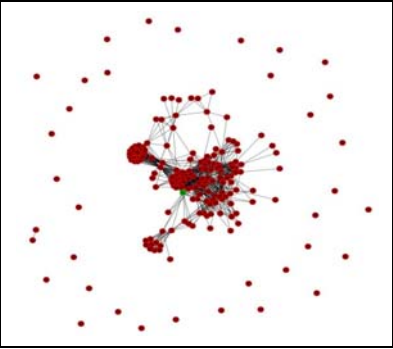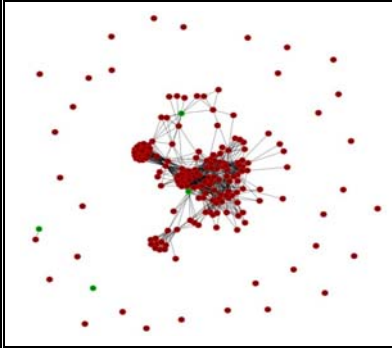

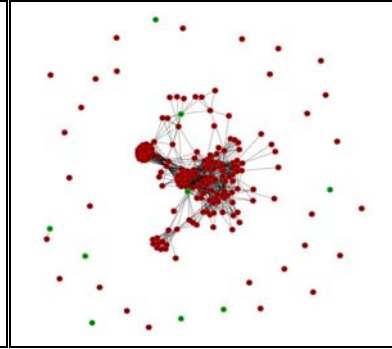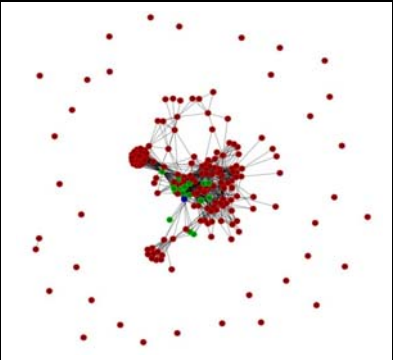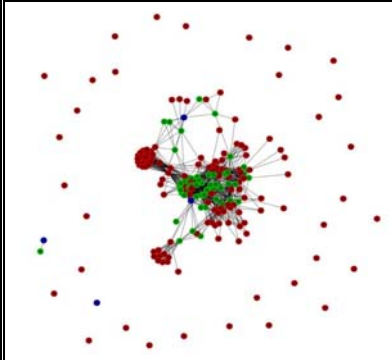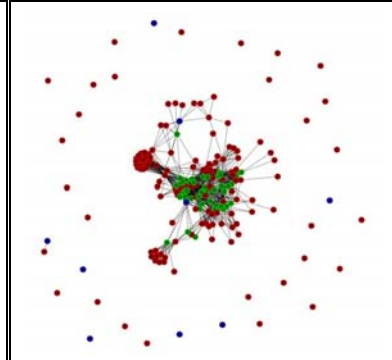Figure 4. Percent of network reached over time using 1, 5, and 10 key player "seed" nodes at 90% resistance.

The structure of the network is visible in the sociograms depicted in Table 7. There is a very closely connected central core with two relatively independent clusters slightly separated from the core. These network maps show nodes who have received the message in green (sometimes blue because of ORA's internal settings), whereas nodes that have not yet received the message remain red.

When a starting node is within the largest connected cluster (not an isolate) the maximum reach is 81.9% (163 out of 199 nodes). In order to reach 100% of the network, it would require injecting the message to each of the 36 isolated nodes separately. For brevity, I only show sociograms of information diffusion based on KPP-POS run in normal mode at 50% resistance, but the method is the same for lists generated using the distance-weighted algorithm as well as for graphing other resistance levels.

	Column 1 – misinfo. injected via 1 node KPP-POS, fixed, 50% resistance, **1 node**	Column 2 – misinfo. injected via 5 nodes KPP-POS, fixed, 50% resistance, **5 nodes**	Column 3 – misinfo. injected via 10 nodes KPP-POS, fixed, 50% resistance, **10 nodes**
Time 1			
	Diffusion **0.50%**	Diffusion **2.51%**	Diffusion **5.03%**
Time 2			
	Diffusion **10.05%**	Diffusion **27.64%**	Diffusion **26.63%**
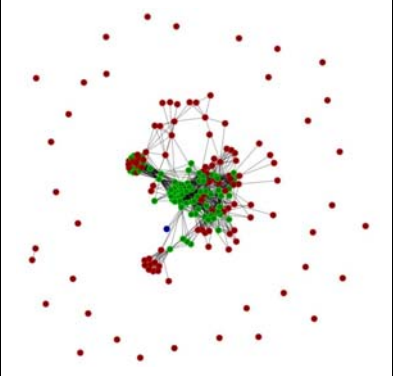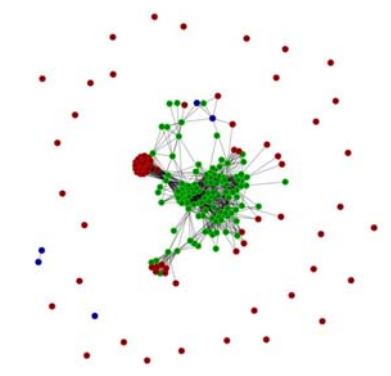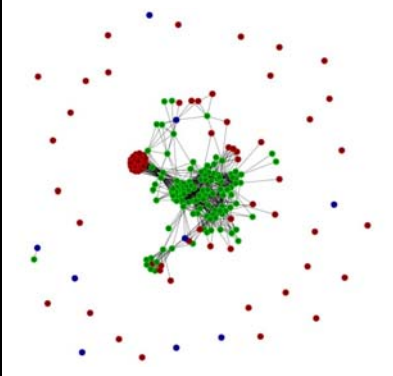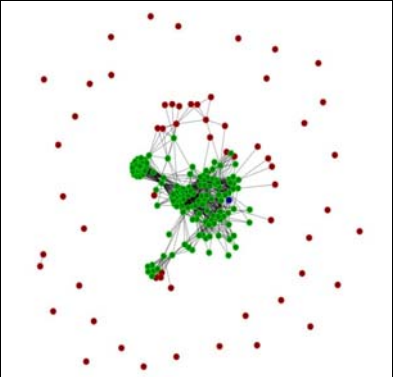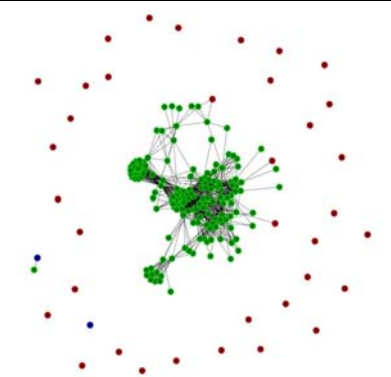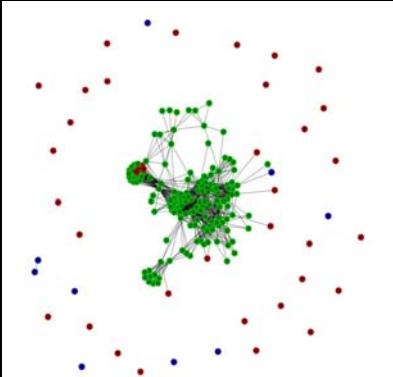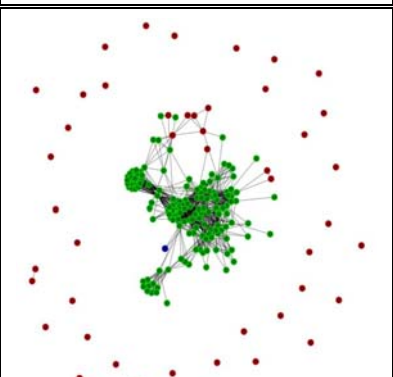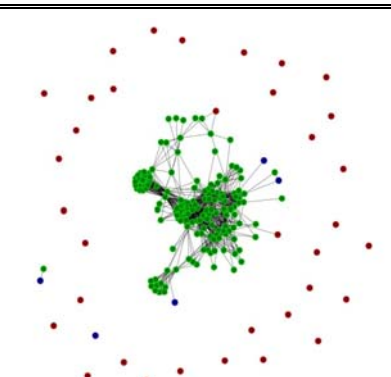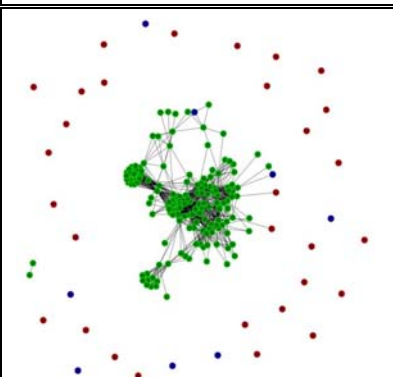
Diffusion **39.70%**	Diffusion **61.31%**	Diffusion **62.81%**
Diffusion **69.85%**	Diffusion **81.91%**	Diffusion **83.42%**
Diffusion **77.39%**	Diffusion **82.41%**	Diffusion **84.92%**

Table 6.   Sociograms of diffusion based on 1, 5, or 10 seed nodes (50% resistance)

45

E.   CONCLUSION

In this chapter, I analyzed the results from Key Player 1 and use an example list to show the effects of fragmentation compared to the fragmentation derived from standard centrality measures. I also explored a diffusion list generated by Key Player 1 and simulate how a message spreads through the network. Resistance to spreading and the number of starting nodes shows the ease or difficult in saturating the network with the message over time. The more nodes, the more time, or the more accepting a message is to the network, the higher the reach will eventually be.

V.   DISCUSSION

A.   FRAGMENTATION DISCUSSION

If we created a HPTL based on centrality measures alone (Table 1), we could conclude that Gun-Gun, Ahmad Rofiq Ridho, Chandra, or Ubeid would be ideal individuals for removal via lethal targeting or nonlethal IO. However, only Gun-Gun and Ahmad Rofiq Ridho appear on the top-ten list generated by the Key Player tool for optimal network fragmentation. Ubeid does not come up on the list until the target set is expanded to 12 or more and Chandra is not identified as a key node for optimal fragmentation at all. Targeting Ubeid or Chandra while expecting the network to fragment is probably a waste of resources. Therefore, a more appropriate HPTL based on Key Player analysis is found in Table 7. These are the individuals we want to *remove* from the network, and are not necessarily the targets for the deception itself.

Recommended fragmentation target list (alphabetized) (KPP-NEG [normal], 10 nodes, network fragmentation = **0.546**)			
Node ID	Name	Current Status	Technical Skills
3	Abdul Malik	Alive	Recruiter, Facilitator
12	Abu Bakar Ba'asyir	Jail	Propagandist, Religious Leader
32	Ahmad Rofiq Ridho	Jail	Bomb Maker, Courier
39	Amir Ibrahim	Jail	Resource Provider
57	Cholily	Jail	Courier, Bomb Maker
75	Gun-Gun	Alive	Courier
78	Hambali	Jail	Leader, Bomber/Fighter
99	Iwan Dharmawan	Jail	Local Leader, Recruiter
141	Muhammed Jibril	Jail	Resource Provider
190	Usman bin Sef	Alive	Resource Provider

Table 7.   Top ten list of key players recommended for removal via a deception strategy

I initially list a 10-node set based on KPP-NEG to illustrate a recommended target list. After 10 nodes, the rate of fragmentation increases faster when removing nodes based on high betweenness centrality, but the fragmentation score for KPP-NEG remains

higher until a set of 16 or more nodes are removed from the network. At this point, nodes prioritized on betweenness centrality appear to fragment the network more. Removing nodes high in closeness centrality or degree centrality have very little effect on the fragmentation of the network. A 10-node set shows a greater amount of disassociated clusters or components on the network map than would be visible with a more manageable two or three node set.

Developing a deception program that simultaneously discredits this number of people is extremely taxing on available resources. It is more reasonable to create a fully planned and resourced deception strategy aimed at causing the network to reject one or two individuals at a time; however, the removal of just one node in the Noordin Top network would have minimal effect (roughly 36%, or a 3% increase over the baseline). Jumping to 50% fragmentation requires the removal of just six nodes, which still might be a stretch in a resource-constrained environment, but it is much more efficient than 10 or 20 nodes. Balancing the effect the commander wants with the ability to resource an operation to get to that level is a major planning consideration. A more moderate six-node list is found in Table 8.

Recommended fragmentation target list (alphabetized) (KPP-NEG [normal], 6 nodes, network fragmentation = **0.504**)			
Node ID	Name	Current Status	Technical Skills
1	Abdul Aziz	Jail	Propagandist
3	Abu Malik	Alive	Recruiter, Facilitator
7	Abdullah Sunata	Jail	Religious Leader
39	Amir Ibrahim	Jail	Resource Provider
120	Mira Augustina's Father	Alive	
172	Subur Sugiarto	Jail	Courier

Table 8.   Top six list of key players recommended for removal via a deception strategy

Notice that the list of ten and the list of six have significantly different individuals. Recall that the Key Player algorithm creates "sets" of nodes that optimally fragment the network. In order to achieve a fragmentation of 50%, all six nodes would

need to be removed nearly simultaneously. Similarly, in order to achieve a fragmentation of 54.6%, all ten nodes from Table 7 would need to be simultaneously removed. Key Player analysis does not generate a prioritized list, so the analyst cannot simply add or subtract individuals and expect the same amount of fragmentation predicted by Key Player.

It is very reasonable to assume that the nodes whose removal would optimally fragment the network via a deception strategy may not actually be feasible targets. Two alternatives exist: the first is to recommend a lethal strategy that attempts to capture or kill key nodes in order to achieve optimal fragmentation;[108] the second is to accept a less optimal target set that is more accessible to our targeting efforts. Of course, the latter would reduce the fragmentation effects, but may be a feasible recommendation within a comprehensive plan with more than just IO methods. Alternately, a target who would be an optimal node for a lethal kill/capture operation but is not accessible that way (due to boundary restrictions, rules of engagement, political sensitivity, or lack of geolocation data) may be a perfect candidate for a deception plan.

B.   DIFFUSION DISCUSSION

In the analysis, I simulated diffusion with resistances of 0%, 50%, and 90% to replicate increasing difficulty in passing a message along. Comparing the amount of diffusion at different resistance levels and with different numbers of starting points can give the IO planner insight into how to prioritize resources. If sufficient message saturation were reached with fewer nodes, this would reduce the number key leader engagements or MISO products (television commercials, bulletin boards, text messages, etc.) required. However, if the network is assessed to be highly resistant to any external messages, more starting nodes may be required.

In Figure 3, I displayed a graph showing the percentage of the network reached with one, five, and ten starting nodes with a resistance factor of 50%. As noted, the percentage of the network reached with one and five nodes is very similar (roughly 82–84%). This means that in theory, we would need to inject misinformation through a single

---

[108] Roberts and Everton, "Strategies for Combating Dark Networks," 4.

source in order to cause the message to reach nearly everyone in the central core. The likely candidate for this would be Ahmad Rofiq Ridho, who is currently in jail. Unfortunately, using a single source for any type of information plan is often a bad idea as it figuratively puts all the eggs in one basket. A minimal amount of redundancy would help overcome the flaws inherent in moving from a simulation to a real world operation.

This redundancy should come from adding additional nodes. For example, using the list of five starting nodes (see Table 4) would provide additional input to the network, even though diffusion would not be any more rapid. One caveat would be to eliminate Ayman al-Zawahiri, the current spokesman for al-Qa'ida. His inclusion in Noordin Top's network is incidental as he is obviously not a member directly involved with planning and coordinating operations with this network. This is a function of how Key Player algorithms look for the ability to maximally reach anyone within the network who is not an isolated node. Al-Zawahri resides in a disconnected dyad, or pair of nodes, and is therefore included because of the key player algorithm design. Additionally, Umar (Yemeni) is an isolated node and cannot pass information to others (again, a function of Key Player algorithms choosing entire "sets"). The recommended insertion nodes are therefore Ahmad Rofiq Ridho, Agus Ahmad, and Aris Susanto.

Table 9 displays the fragmentation targets and the count of direct connections that must be reached in order meet the goal of getting the misinformation message to everyone associated with the target. Each time period, the message diffuses deeper into the network, and even with a 50% resistance factor, the entire set of direct connections is reached by time 5, and in some cases, as early as time 3. Of course, those targets with fewer connections generally have their personal networks saturated with the message sooner.

Recommended fragmentation target list (alphabetized) (KPP-NEG [normal], 6 nodes, network fragmentation = **0.504**)							
Node ID	Name	Direct Connections	Time 1	Time 2	Time 3	Time 4	Time 5
1	Abdul Aziz	16	15	12	10	5	0
3	Abdul Malik	18	17	11	1	0	0
7	Abdullah Sunata	35	34	22	3	1	0
39	Amir Ibrahim	10	9	4	0	0	0
120	Mira Augustina's Father	17	16	9	1	1	0
172	Subur Sugiarto	13	12	10	6	0	0

Table 9.   List of fragmentation targets and the number of direct connections. Each time period lists the number of direct connections who have NOT yet received the information.

C.   FEEDBACK AND INTELLIGENCE COLLECTION

Key Player analysis and Micro Simulation identify nodes that should be recommended for further research by the IO planner and the intelligence staff. More importantly, Key Player analysis and Micro Simulation identify parts of the network that would be better places to setup and deploy intelligence, surveillance, and reconnaissance resources before any disruption operation takes place. Early establishment of ISR helps capture indicators that the operation is actually happening in the manner we had intended. These indicators, or measures of effectiveness, are essential in order to show success or failure to the military commander. If these indicators are not present, then the IO planners can recommend changes to ISR allocation or changes to the strategy.

The majority of individuals in the diffusion list (Tables 3, 4, and 5) are alive and not in jail, which might reduce the accessibility for using them as a starting point for message diffusion. On the other hand, the ones in jail might be approached by intelligence personnel and be recruited or convinced to pass along our message. Ahmad Rofiq Ridho appears on the one-, five-, and ten-person diffusion lists. Aris Susanto and Agus Ahmad, both of whom are in jail, appear on both the five and ten node lists. These individuals would be priority recommendations for intelligence recruitment.

Ridho also has high closeness, degree, and betweenness centrality scores, meaning he has many connections and brokers resources in the network. Answering whether these connections are extant would be useful in determining if he could in fact disseminate a message as rapidly as the simulation indicates. Monitoring his prison visits and patterns of communication could provide insight into Ridho's influence.

D. LIMITATIONS TO SOCIAL NETWORK ANALYSIS

1. Boundary Accuracy

Predicting fragmentation and information diffusion is heavily dependent upon the boundaries of the network used. The choice to include a relationship is highly subjective. Does kinship include cousins? How about spouses of cousins? Can we suppose that two individuals who worked at an organization at the same time as having a relationship, or can we assume they even know each other? It is essential that the IO planner work with intelligence analysts to create a codebook that defines ties and relationships and whether an actor should be included or excluded. This document allows for consistent choices in creating the boundary around a network.

I chose one slice of the possible combinations of networks within Noordin Top's organization. Using a similar data set, Everton and Cunningham identify at least 20 possible configurations that could vary the outcome of Key Player and diffusion analysis.[109] It might be useful to do Key Player analysis on several configurations of the network (e.g., kinship network, trust network, operational ties, etc.) and find those individuals who continually surface as key players. This way, the analyst examines different aspects of social influence and can make an even more informed recommendation for targeting through deception.

2. Alternatives to Nodal Analysis

Nodal analysis looks at each entity as a single actor in the network, but there are other ways of looking at networks. Kempe et. al. argue that selecting individual nodes

---

[109] Sean Everton, "Social Network Change Detection," lecture, Monterey, CA: Naval Postgraduate School (October 18, 2012). See also Everton and Cunningham, "Detecting Significant Changes," 6–8.

may not be the most effective way of influencing the network (especially large ones) for a particular product or innovation to "go viral." Their research suggests that random target selection above a certain threshold outperforms selective targeting using centrality measures.[110] For military purposes, this product or innovation could be a desired behavior or attitude change favorable to U.S. interests. Viral adoption research might be useful for large audience mobilization desired by MISO, but might not be important for small or dark networks.

Targeting strategies that focus on the removal of single nodes (or small sets of nodes), especially those high in centrality measures are generally not effective, as the network has the ability to rapidly recover and heal from these surgical removals. Tsvetovat and Carley argue that nodes with structural equivalence to the targeted nodes are able to rebalance the flow of resources until the network stabilizes.[111]

Instead of looking at individuals in the network, one alternative is to strategize disruption plans around the group or the organization. Group targeting is centered on subsets of the network and organization targeting looks at more than a single network.[112] With the Noordin Top data set, social network analysis might collapse individuals into groups with similar attributes, such as bomb makers, logisticians and facilitators, and religious leaders, or those who live in the same geographic region. Applying fragmentation methodologies would indicate which group's removal would disrupt the network the most.

[110] David Kempe, Jon Kleinberg, and Eva Tardos, "Maximizing the Spread of Influence Through a Social Network," *SIGKDD* (2003): 7.

[111] Tsvetovat and Carley, "Structural Knowledge." For more on the effects of structural equivalence and position within the network, see Everton, *Disrupting Dark Networks*, Chapter 9.

[112] Roberts and Everton, "Strategies for Combating Dark Networks," 4.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

The methods I describe in this thesis are just one way to assist in the IO targeting process. They are intended to augment, not replace, thorough intelligence preparation and good staff work. SNA is useful in identifying nodes that assist the diffusion of a message. It is also useful in finding vulnerabilities of a covert network, such as where too many tasks or decision-making responsibilities lie with one person, or whether a broker of resources can be replaced with an equivalent actor.

A.   FUTURE RESEARCH

In addition to network fragmentation and the idea of message diffusion, there are other options for the IO strategist to consider that would benefit from social network analysis techniques. Roberts and Everton identify several non-kinetic options including capacity building, institution-building, and rehabilitation that can be studied on the individual, group, or organization levels.[113]

The ORA software program contains four diffusion simulation methods, of which I explored one, the information diffusion algorithm. Although the procedures are essentially "black box" with very little documentation about how they actually run, it would be interesting to test message propagation against one or more of these models. Perhaps a modification of the disease propagation or the diffusion of innovations models might better explain how humans receive, process, and pass along information. The resistance factor might vary depending on network location, time, or environmental factors that are currently not visible to the model.

ORA also contains a more complicated predictive simulation called Near Term Analysis, or Construct. This simulation investigates the dynamics of network behavior using complex socio-cultural variables. It uses sub-networks of actors, knowledge, tasks,

---

[113] Roberts and Everton, "Strategies for Combating Dark Networks," 5–7.

and resources to model behavior. Construct requires more input in terms of network coding, but may be able to better predict social and cultural influences in network behavior.[114]

Finally, there is a considerable amount of data in social networking applications that can better inform network structure and the social influences. Research in social media and social networking applications as a means for information diffusion would be an interesting use of SNA in IO targeting. There are indications that insurgents and terrorists using social media platforms both have the ability to influence others and are influenced themselves by the tools they use, thereby affecting their decisions.[115] Considering these social influence factors in the IO strategy is a wise choice.

B.   RECOMMENDATIONS FOR IO PLANNERS AND MILITARY COMMANDERS

This thesis takes a narrow slice of possible ways to disrupt an adversarial network. Because deception is only one method of conducting an information operation, which itself is only one facet of nonlethal targeting, it would be useful to military organizations to apply social network analysis in all intelligence, targeting, and planning teams. The benefits of fragmentation analysis using Key Player methods are obvious to the lethal targeting team, but what about Civil Affairs or reconciliation planners? Are there aspects of SNA that would provide civil capacity planners the ability to reach out to neutral and friendly audiences that would more efficiently utilize their precious funds?

The integration of IO and intelligence is of paramount importance in a deception plan as well as other methods of nonlethal strategies. Intelligence involvement in understanding both the human/social terrain as well as the information environment our

---

[114] For an introduction to Construct see Brian R. Hirshman, Kathleen M. Carley, and Michael J. Kowalchuck, "Specifying Agents in Construct," Pittsburgh: Carnegie Mellon University (July 25, 2007) and Brian R. Hirshman, Kathleen M. Carley, and Michael J. Kowalchuck, "Loading Networks in Construct," Pittsburgh: Carnegie Mellon University (July 26, 2007). Additionally, a study of network destabilization techniques can be found in Il-Chul Moon and Kathleen M. Carley, "Locating Optimal Destabilization Strategies," in *12th ICCRTS,* Pittsburgh: Carnegie Mellon University (2007). These can be found online at http://www.casos.cs.cmu.edu/publications/papers.php.

[115] M. Craig Geron, "IO in an Unpredictable World," *IO Sphere* (Winter 2007), 4.

targets operate in must occur well before any planning takes place.[116] Intelligence analysts must be trained to build databases of information that consider many different types and strengths of relationships. It is potentially more important to understand *why* a relationship exists between two people or groups than the mere fact that it does exist. Manipulating the social bond between two people requires understanding many of the social and cognitive factors described in Chapter II.

Resourcing the IO planning team with dedicated intelligence analysts who are trained in SNA methods allows for the rapid creation and analysis of different views of an adversarial network. These analysts would be able to assist with the background work needed to understand the human terrain as well as make appropriate recommendations for intelligence collection that best serve the execution and feedback of IO plans.

In summary, this thesis has explored how a deception plan against a terrorist network can be informed and prepared using social network analysis. First, I identified key nodes for removal that increase the amount of network fragmentation. Next, I identified nodes that could be used to insert misinformation and simulate how quickly it would theoretically spread through the network. Third, I looked for individuals connected to the fragmentation targets and checked to see they had the opportunity to receive the misinformation. Fourth, I recommended nodes that require intelligence collection in order to provide feedback about the success of message dissemination and the deception effort. Finally, I outlined some of the drawbacks to using SNA in IO planning and offered several recommendations for the use of SNA and the integration of intelligence and IO.

---

[116] Cox, "Information Operations," 17–24.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Books

Christakis, Nicholas A. and James H. Fowler. *Connected*. New York: Little, Brown and Company, 2009.

Cialdini Robert B. *Influence: The Psychology of Persuasion*. New York: Harper Collins, 2007.

Daniel, Donald and Katherine Herbig. *Strategic Military Deception.* New York: Pergamon, 1982.

Everton, Sean. *Disrupting Dark Networks*. New York and Cambridge: Cambridge University Press, 2012.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Tel Aviv: Tel-Aviv University, Jaffe Center for Strategic Studies, 1988.

Latimer, Jon. *Deception in War*. Woodstock, NY: Overlook Press, 2001.

Roloff, Michael. *Interpersonal Communication: The Social Exchange Approach*. Beverly Hills: Sage Publications, 1981.

Turner, John C. *Social Influence*. Bristol, PA: Open University Press, 1991.

United States Army. *Field Manual 3.0: Operations*. Washington, DC: Department of Defense, Feb. 2011.

United States Army. *Field Manual 3–05.30: Psychological Operations.* Washington, DC: Department of Defense, Apr. 2005.

United States Army, *Field Manual 3–60: The Targeting Process*. Washington, DC: Department of Defense, Nov. 2010.

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

Historical Documents

International Crisis Group. *Terrorism in Indonesia: Noordin's Networks*. Brussels, Belgium: International Crisis Group (2006).

International Crisis Group. *Indonesia: Noordin Top's Support Base.* Brussels, Belgium: International Crisis Group (2009).

Journal Articles

Asch, Solomon E. "Opinions and Social Pressure." *Scientific American* 193, vol 5 (November 1955): 31–35.

Baker, Ralph O. "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations." *Military Review* (May-June 2006): 13–32.

Borgatti, Stephen P. "Identifying Sets of Key Players in a Social Network." *Computational, Mathematical and Organizational Theory* 12 (2006): 21–34.

Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections* 24, no. 3 (2002): 79–92.

Cialdini, Robert B. and Linda J. Demaine, et al. "Managing Social Norms for Persuasive Impact." *Social Influence* 1 no. 1 (2006): 3–15.

Everton, Sean F. and Dan Cunningham. "Detecting Significant Changes in Dark Networks." *Behavioral Sciences of Terrorism and Political Aggression* (2012): 1–21.

Flynn, Michael T., Matt Pottinger, and Paul T. Batchelor. "Fixing Intel: A Blueprint for Intelligence Relevant in Afghanistan." *Voices from the Field*. Center for a New American Security (January 2010).

Fowler, Charles A. and Robert F. Nesbit. "Tactical Deception in Air-Land Warfare." *Journal of Electronic Defense* (June 1995): 37–44, 76–79.

Granovetter, Mark. "The Strength of Weak Ties." *American Journal of Sociology*, 78 (May 1973): 1360–1380.

Kempe, David, Jon Kleinberg, and Eva Tardos. "Maximizing the Spread of Influence through a Social Network." *Knowledge Discovery and Data Mining (KDD)*. Washington, DC (2003).

Milgram, Stanley. "Behavioral Study of Obedience." *Journal of Abnormal and Social Psychology* 67 (October 1963): 371–378.

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

Snow, David A., E. Burke Rochford, Jr., Steven K. Worden and Robert D. Benford. "Frame Alignment Processes, Micromobilization, and Movement Participation." *American Sociological Review* 51, no. 4 (Aug., 1986): 464–481.

Snow, David A. and Robert D. Benford. "Ideology, Frame Resonance, and Participant Mobilization." *International Social Movement Research* 1 (1988): 197–217.

Stark, Rodney and William S. Bainbridge. "Networks of Faith: Interpersonal Bonds and Recruitment to Cults and Sects." *American Journal of Sociology* 85, no. 6 (1980): 1376–1395.

Tajfel, Henri and John C. Turner. "The Social Identity Theory of Intergroup Behavior." In S. Worchel and W. G. Austin (Eds.). *Psychology of Intergroup Relations*. Chicago: Nelson-Hall, 1986.

Tsvetovat, Maksim and Kathleen M. Carley. "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence." *Journal of Social Structure* 6, no. 2 (2005).

Tversky, Amos and Daniel Kahneman. "The Framing of Decisions and the Psychology of Choice." *Science 211* no. 4481 (Jan. 30, 1981): 453–458.

Online Articles

Faint, Charles and Michael Harris. "F3EAD: Ops/Intel Fusion 'Feeds' the SOF Targeting Process." *Small Wars Journal* (January 31, 2012). Accessed November 13, 2012. http://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-"feeds"-the-sof-targeting-process.

Geron, M. Craig. "IO in an Unpredictable World." *IO Sphere* (Winter 2007): 3–4. Accessed February 19, 2012. http://www.au.af.mil/info-ops/iosphere/07winter/iosphere_win07_geron.pdf.

Gomez, Jimmy A. "The Assessments Process in Contemporary Operating Environment." *Small Wars Journal* (2011). Accessed February 19, 2012. http://smallwarsjournal.com/jrnl/art/the-assessments-process-in-contemporary-operating-environment.

Hanneman, Robert A. and Mark Riddle. *Introduction to Social Network Methods.* Riverside, CA: University of California, Riverside (2005). Accessed November 5, 2012. http://faculty.ucr.edu/~hanneman/.

JD, "Lethal Targeting in Iraq; Success on an Unprecedented Scale," *al Sahwa* (April 22, 2010). Accessed November 13, 2012. http://al-sahwa.blogspot.com/2010/04/lethal-targeting-in-iraq-success-on.html.

Eric T. Olson, "Q&A: Admiral Eric T. Olson," *Special Operations Technology* 6 no. 4 (2008). Accessed November 13, 2012. http://www.special-operations-technology.com/sotech-home/56-sotech-2008-volume-6-issue-4/423-qaa-admiral-eric-t-olson.pdf.

Rhoads, Kelton. "Working Psychology." (2004). Accessed 5 September 2012.
http://www.workingpsychology.com.

"Social Exchange Theory." *Wikipedia*. Accessed September 5, 2012.
http://en.wikipedia.org/wiki/ Social_exchange_theory.

"Social Psychology." *Wikipedia*. Accessed September 5, 2012.
http://en.wikipedia.org/wiki/ Social_psychology.

Theses and Papers

Adams, Barbara D., Jessica Sartori, and Sonya Waldherr. "Military Influence Operations:
Review of Relevant Scientific Literature." Toronto: Human Systems, Inc.
(November 2007).

Anonymous. "Deception 2.0: Deceiving in the Netwar Age." Unpublished Paper. Task
Force Iron, Iraq, 2009.

Cox, Joseph L. "Information Operations in Operations Enduring Freedom and Iraqi
Freedom—What Went Wrong?" Monograph. Fort Leavenworth, KS: United
States Army Command and General Staff College, 2006. Accessed February 19,
2012. http://www.fas.org/irp/eprint/cox.pdf.

Davis, James Kirkpatrick. "Spying on America: The FBI's Domestic Counterintelligence
Program." New York: Praeger, 1992.

Freeman, Michael and Hy Rothstein, eds. "Gangs and Guerrillas: Ideas from
Counterinsurgency and Counterterrorism." Monterey, CA: Naval Postgraduate
School, 2007.

Granger, Dewey A. "Integration of Lethal and Nonlethal Fires: The Future of the Joint
Fires Cell." Monograph. Fort Leavenworth, KS: U.S. Army Command and
General Staff College, 2009.

Hirshman, Brian R., Kathleen M. Carley, and Michael J. Kowalchuck. "Specifying
Agents in Construct." Pittsburgh, PA: Carnegie Mellon University, July 25, 2007.
Accessed November 7, 2012.
http://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-07–107.pdf.

Hirshman, Brian R., Kathleen M. Carley, and Michael J. Kowalchuck. "Loading
Networks in Construct." Pittsburgh, PA: Carnegie Mellon University, July 26,
2007. Accessed November 7, 2012.
http://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-07–116.pdf.

Moon, Il-Chul. "Destabilization of Adversarial Organizations with Strategic Interventions." Unpublished Doctoral Thesis. Pittsburgh, PA: Carnegie Mellon University, 2008. Accessed February 12, 2012. http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-08–124.pdf.

Moon, Il-Chul and Kathleen M. Carley. "Locating Optimal Destabilization Strategies." In *12th ICCRTS.* Pittsburgh, PA: Carnegie Mellon University (2007). Accessed November 7, 2012. http://www.casos.cs.cmu.edu/publications/papers/CCRT-imoon-2007.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
        Ft. Belvoir, VA

2.   Dudley Knox Library
        Naval Postgraduate School
        Monterey, CA

3.   Information Proponent Office
        Fort Leavenworth, KS

4.   1st IO Command
        Fort Belvoir, VA

5.   Marine Corps Information Operations Center
        Quantico, VA