

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTELLIGENCE COLLECTION, TARGETING AND INTERDICTION OF DARK NETWORKS

by

Darrin K. Tangeman

June 2014

Thesis Advisor: Sean Everton
Second Reader: Robert Schroeder

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
INTELLIGENCE COLLECTION, TARGETING AND INTERDICTION OF DARK NETWORKS

5. FUNDING NUMBERS

6. AUTHOR(S) Darrin K. Tangeman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT

To interdict dark networks and prevent terrorist attacks, security forces require consistent access to relevant intelligence and targeting data. Dark networks often react to a security force's targeting pressure by obscuring their activities and becoming increasingly covert. Network adaptation to targeting pressure can frequently lead to intelligence gaps and lulls in targeting that may be both predictable and preventable if identified early. This study will examine the efficacy of the two prevailing modes of targeting and their impact on resilient dark networks. To achieve this goal, this thesis will conduct a multivariate path analysis using temporal, geospatial, and relational data of a select dark network as these two modes of intelligence collection and targeting are employed against the network over time. By achieving this goal, this thesis will generate policy recommendations for operationalizing the outcomes of this study in order to better formulate how the prevailing modes of targeting can more effectively be implemented to address adaptive terrorist threats.

14. SUBJECT TERMS Intelligence, targeting, social network analysis, geospatial analysis, temporal analysis, dark networks, counterterrorism, HUMINT, national technical means, dark network decision cycle, strategic interaction model.			**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

Approved for public release; distribution is unlimited

INTELLIGENCE COLLECTION, TARGETING AND INTERDICTION OF DARK NETWORKS

Darrin K. Tangeman
Major, United States Army
B.G.S., University of Kansas, 1998
M.P.A., University of Colorado at Denver, 2014

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Author: Darrin K. Tangeman

Approved by: Sean Everton
Thesis Advisor

Robert Schroeder
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To interdict dark networks and prevent terrorist attacks, security forces require consistent access to relevant intelligence and targeting data. Dark networks often react to a security force's targeting pressure by obscuring their activities and becoming increasingly covert. Network adaptation to targeting pressure can frequently lead to intelligence gaps and lulls in targeting that may be both predictable and preventable if identified early. This study will examine the efficacy of the two prevailing modes of targeting and their impact on resilient dark networks. To achieve this goal, this thesis will conduct a multivariate path analysis using temporal, geospatial, and relational data of a select dark network as these two modes of intelligence collection and targeting are employed against the network over time. By achieving this goal, this thesis will generate policy recommendations for operationalizing the outcomes of this study in order to better formulate how the prevailing modes of targeting can more effectively be implemented to address adaptive terrorist threats.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. BACKGROUND 1
B. IMPORTANCE 5
C. KEY TERMS 7
1. Dark and Bright Networks 7
2. Network Resilience 8
3. Differentiation 9
4. Integration 9
5. Network Control 10
6. Social Network Analysis 11
7. Interdiction 11
D. PURPOSE AND OBJECTIVES 12
E. RESEARCH QUESTION 13
F. THESIS CHAPTER REVIEW 13

II. HYPOTHESIS AND LITERATURE REVIEW 15
A. DEFINING THE VARIABLES 15
1. Independent Variable 1 17
2. Independent Variable 2 18
3. Intervening Variable 18
4. Dependent Variable 18
B. HYPOTHESIS 19
C. LITERATURE REVIEW 22
1. Human Intelligence and Targeting 23
2. National Technical Means Intel and Targeting 27
3. Dark Network Change and Resilience 31
4. Literature Review Conclusions 33

III. DATA AND METHODS 35
A. DATA DESCRIPTION 35
1. DOCUMENT ANALYSIS AND DATA CODING 36
a. Document Analysis 36
b. Data Coding 37
2. Data Sources 38
a. All-Source Intelligence Analysis Reports 38
b. Significant Activity Reports 39
c. Interrogation Reports 39
d. Targeting Databases 39
e. HUMINT Reports 40
f. TECHINT Reports 40
g. Forensic Reports 41
B. ANALYTIC METHODS 41
1. Analytic Methods Workflow 42

a. Spatiotemporal Network Analysis in ORA 43
b. Network Topography 44
2. Path Analysis 46
IV. RESULTS AND FINDINGS 49
V. CONCLUSIONS, IMPLICATIONS AND POLICY RECOMMENDATIONS 55
A. CONCLUSIONS 55
B. IMPLICATIONS AND POLICY RECOMMENDATIONS 56
APPENDIX STRUCTURED MASTER DATA SET 59
LIST OF REFERENCES 61
INITIAL DISTRIBUTION LIST 65

LIST OF FIGURES

Figure 1. Diagram of Bright and Dark Network Spectrum 8
Figure 2. Diagram of Network Control Strategy 11
Figure 3. Hypothesis and Path Analysis 17
Figure 4. Hypothesis: Strategic Interaction Model 20
Figure 5. Data and Methods Diagram 42
Figure 6. Network Diagram at Time Perod 1 of 27 (ORA). 43
Figure 7. Path Analysis Model and Variables 47
Figure 8. Path Analysis Diagram with Statistics 49
Figure 9. Scatter Plot: HUMINT versus Spatial Degree Centralization 50
Figure 10. Scatter Plot: Spatial Degree Centralization versus Attacks Per Capita 52

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Path Analysis Statistics 53

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

COIN	counterinsurgency
CT	counterterrorism
FARC	Fuerzas Armadas Revolucionarias de Columbia
FBI	Federal Bureau of Investigation
FINO	failure or fault-intolerant network organizations
FOIA	Freedom of Information Act
HUMINT	human intelligence
IIR	intelligence information report
JI	Jemaah Islamiyah
LTTE	Liberation Tigers of Tamil Eelam
MK	Unkhonto we Sizwe
NTM	national technical means
NSA	National Security Agency
OPSEC	operational security
PIRA	Provisional Irish Republican Army
SEM	structural equation modeling
SEAL	sea air land
SIGACT	significant activity report
SNA	social network analysis
TECHINT	technical intelligence
TTP	tactics techniques and procedures

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I want to thank my wife and daughters for their immense patience, love, and support. I owe my wife a significant debt of gratitude for having supported me through this time-consuming and arduous process. I will live the rest of my life trying to live up to and return the love she shows me every day. I want to thank my parents for their eternal support and the work ethic that they instilled in me.

I sincerely thank my thesis advisor Dr. Sean Everton, and second reader Robert Schroeder, for their patience, expertise and support for the very long road I took to complete this work. I would also like to thank Karen Flaherty and Malcom Mejia for their assistance over the last year in the CORE Lab.

Finally, I would like to thank Dr. John Arquilla for the extended opportunity he gave me, as well as Jennifer Duncan and Professor Anna Simons for the time they took from their busy schedule to assist me along the way. Thank you.

De Oppresso Liber

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Following several casualty-producing attacks by a uniquely improvised explosive device, a combination of forensic intelligence, national technical means (NTM)[1] intelligence, and Internet media analysis linked an undisclosed foreign terrorist organization to the attacks. While targeting through NTM provided early success, over time the membership of this dark network[2] conducted denial operations[3] by modifying their activities and reverting to low technical modes of communication[4] in order to impede collection efforts by security forces.[5] The network's denial operations negatively impacted NTM collection efforts and directly reduced available actionable intelligence. Interrogations of captured

[1] National technical means (NTM) refers to technical intelligence collection (TECHINT), or the broad use of technologies rather than the direct use of humans to collect information through traditional espionage. Howard O. DeVore, 1999, *Jane's Special Report: China's Intelligence & Internal Security Forces* (Alexandria, VA: Jane's Information Group), ch. 7.

[2] "While ''bright'' and ''dark'' are metaphors, what we mean empirically is that a bright network is legal and visible and a dark network is illegal and tries to be as invisible as possible. Visibility refers to the question of how easy activity of a network is to discern without serious investigative efforts." H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems; Elements of a Theory," *International Public Management Journal* 9, no. 3 (2006): 334. For the purpose of this thesis, we will refer to covert terrorist networks as dark networks.

[3] "Denial refers to activities and programs designed to eliminate, impair, degrade, or neutralize the effectiveness of intelligence collection within and across any or all collection disciplines, human and technical." Roger Z. George and James B. Bruce, *Analyzing Intelligence: Origins, Obstacles and Innovations* (Washington, DC: Georgetown University Press, 2008), 123.

[4] Forms of low-tech communication can include human intelligence tradecraft practices such as dead drops, face-to-face meetings, cut-outs, and unwitting couriers.

[5] For the purpose of this thesis, security forces will refer to law enforcement and military forces that are tasked to conduct counterterrorism operations.

members of the network detained as a result of early targeting success provided only marginal actionable intelligence that ultimately diminished over time.[6]

As actionable intelligence deteriorated and the network moved further underground, several factors appeared to contribute to the widening intelligence gap that prevented successful targeting of the network. The increased concealment of the network's activities and reduction in open communications had rendered NTM collection efforts ineffective, while the absence of human intelligence (HUMINT)[7] source operations directed at the network left security forces with few options to reestablish active surveillance of the network. Eventually, the deficit in HUMINT source operations and mounting command pressure to remedy the intelligence gap led to a frenzy of information requirements directed at HUMINT collectors in hopes of penetrating the network. Unfortunately, HUMINT requires time to develop and cannot be quickly diverted or created where an intelligence gap has previously existed. This suggests that an early and persistent emphasis on HUMINT source operations may be required to successfully wage long-term counterterrorism operations against dark networks.

While it is apparent that security forces cited in this narrative achieved technological dominance, it is equally apparent that they will not always possess a technological advantage in the future. What this narrative demonstrates is that dark networks are capable of successfully employing denial operations by adapting low-tech communication strategies to thwart NTM collection efforts. Under these conditions, only the occasional and rare operational security

---

[6] The noted decline in actionable intelligence from interrogations can be attributed to the diminishing value and time sensitive nature of HUMINT interrogation information over time. Once captured, the relevant information a detainee can provide degrades as a detainee's insurgent network modifies their actions and modes of communication to prevent future targeting and disruption of the network.

[7] Human intelligence is defined as a category of intelligence derived from information collected and provided by human sources. Also called HUMINT. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02) (Washington, DC: Joint Chiefs of Staff, amended through 2009), 249.

(OPSEC) gaffe by dark network members will lead to potential NTM collection opportunities. Without these opportunities, the only alternative to rectify this intelligence gap and reestablish surveillance of the network is through the employment of HUMINT source operations.

On the other hand, it is also true that HUMINT source operations are vulnerable to denial operations through an increase in compartmentalization[8] and operational security measures. While overcoming HUMINT denial operations is a difficult task, the versatility of HUMINT collection can provide a comparatively greater menu of collection methods to increase a security forces probability of success against dark networks. These can be as simple as elicitation[9] or can be as elaborate and innovative as the Four Square Laundry Service cover businesses used by British Military Intelligence in Northern Ireland to collect information on the Provisional Irish Republican Army (PIRA).[10]

Although, the previous narrative demonstrates that sole dependency on NTM targeting has significant shortfalls, a fascination and affinity for the application of technology in fighting terrorist networks persists. It is no stretch to suggest that our dependency on technology has been advanced by our perceptions of information dominance in contemporary conventional warfare.

---

[8] In a dark network, it is often necessary for security purposes to structurally separate an organization down to its most basic structure, a cell. "The cell may be compartmentalized in order to protect the underground organization and reduce the vulnerability of its members to capture. Compartmentalization restricts the information any member has about the identity, background, or current residence of any other cell member. He knows individuals only by their aliases and the means by which they can be reached. This follows the underground "fail-safe" principle: if one element in the organization fails, the consequences to the total organization will be minimal. Furthermore, it is a security measure that protects not only the organization but the individuals in the compartmentalized cells." Department of the Army, *Human Factors and Consideration of Underground Insurgencies* (DA PAM 550-104) (Washington, DC: Department of the Army) 20.

[9] Elicitation (intelligence): Acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. A technique of human source intelligence collection, generally overt, unless the collector is other than he or she purports to be. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02) (Washington, DC: Joint Chiefs of Staff, 1999, amended through 2009), 183.

[10] Bradley W. C. Bamford, "The Role and Effectiveness of Intelligence in Northern Ireland," *Intelligence & National Security* 20, no. 4 (2005): 588.

This sentiment has carried over into modern counterterrorism operations where this fascination with technology has skewed our understanding of how best to defeat terrorist networks. Our tendency to emphasize and develop a narrow focus on the successes of technical intelligence is a dangerous precedent, and mirrors how the U.S. has historically underestimated the learning, development, and adaptability of militarily weaker enemies as was observed in Vietnam and Iraq. This phenomenon is illustrated in Ivan Arreguín-Toft's strategic interaction model, where he demonstrates that weak actors (like dark networks) are capable of defeating militarily stronger actors (security forces) by refusing to engage a strong actor where they have a strategic advantage. Ivan Arreguín-Toft explains that by adopting a strategy (asymmetric) that does not play into the strategic advantage of the strong actor, a weaker actor can avoid direct conflict by simply waiting until the stronger actor abandons or redirects their focus elsewhere.[11] Despite the lessons of Arreguín-Toft, many analysts continue to place emphasis on the employment of technical intelligence in defeating our terrorist adversaries, while underplaying the parallel function and strengths of HUMINT source operations.

For example, in *Countering the New Terrorism*, John Arquilla, David Ronfeldt, and Michele Zanini assert that because of the human limitations of HUMINT, "…it is ill-advised to pin significant hopes on the development of sufficient HUMINT sources to wage an effective counterterrorist campaign."[12] In *Brave New War*, John Robb states that the leveraging of technology by terrorists, "…has finally reached a point where small super empowered groups, and not yet individuals, now have the capability to challenge the state in warfare and win."[13]

---

[11] Ivan Arreguín-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge, UK: Cambridge University Press, 2005), 35.

[12] Ian O. Lesser et al., "Networks, Netwar, and Information-Age Terrorism," in *Countering the New Terrorism*, ed. John Arquilla et al. (Santa Monica, CA: Rand Corporation, 1999), 78–79.

[13] John Robb, *Brave New War, The Next Stage of Terrorism and the End of Globalization* (Hoboken, NJ: John Wiley and Sons Inc., 2007), 11.

Many leaders and policy makers also dismiss HUMINT on the false presumption that NTM intelligence will comparatively increase the degree of warning to impending terrorist attacks. However, as Katya Drozdova demonstrated in her analysis of al-Qaeda communications and operations, the use of high tech communications by al-Qaeda consistently peaked during an attack, rather than prior to the attack, making it improbable that NTM intelligence could play a significant role in the preventing terrorist attacks by more sophisticated terrorist organizations.[14]

B. IMPORTANCE

While the previously cited narrative demonstrates the utility of HUMINT in the conduct of counterterrorism campaigns, Western nations in general and the United States in particular, continue to gravitate towards technological solutions to defeat or prevent terrorist attacks. While there is evidence to support these policy prescriptions, it should not be overlooked or dismissed that the most sophisticated terrorists we face today have and are capable of conducting denial operations that can evade our most technologically advanced modes of intelligence collection and targeting for decades. A report released by the Federal Bureau of Investigation (FBI) under the Freedom of Information Act (FOIA), demonstrated that none of the 9/11 al-Qaeda hijackers were known to have owned a laptop, desktop computer, or electronic storage media, despite several of them arriving in the United States as early as 21 months prior to the attacks. The report also stated that the hijackers limited their use of technology and were cautious when making and receiving operational communications by using pre-paid phone cards in combination with pay phones, pre-paid cell phones, and

[14] Katya Drozdova, *Analyzing Terrorist Communications: Detecting Early Signals of Attack* (Stanford, CA: Hoover Institute on War, Revolution, and Peace, 2009), 21.

internet cafés. What is more telling is that they reserved their most sensitive preparation and planning for three face-to-face meetings that were conducted in 2001.[15]

As James Bamford and Scott Willis' 2009 documentary *The Spy Factory* illustrates, the precautions taken by the hijackers to reduce their communications signature and remain under the radar of the National Security Agency's (NSA) eavesdropping capabilities was savvy enough to be successful.[16] Not only did the 19 al-Qaeda operatives who conducted the 9/11 attacks practice low tech denial operations, but Osama Bin Laden himself evaded U.S. detection for at least 14 years through denial operations before his death in May 2011. Author Peter Bergen stated in his 2013 book *Manhunt, The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*,

> …Bin Laden started avoiding any electronic communications as early as 1997, understanding that they could be intercepted. Also, al-Qaeda's leaders had closely followed the April 1996 assassination of Dzhokhar Dudayev, the Chechen prime minister, who was killed by a Russian missile that homed in on the signal emitted by his cell phone. At the time, Chechnya was a major focus of al-Qaeda's efforts to foment global jihad.[17]

The same pattern of sophisticated operational security and denial operations was practiced by the military leader of Hezbollah, Imad Mughniyeh as he evaded targeted assassination for 16 years before ultimately being assassinated in 2008. With Al-Qaeda and Hezbollah having mastered denial operations against the most sophisticated and determined terrorist manhunts in recent history, it is imperative that the United States remain vigilant in identifying and preventing the low-tech terrorist threat into the immediate future.

---

[15] Federal Bureau of Investigation, *Report: The 11 September Hijacker Cell Model*, 2003, http://911workinggroup.org/FBI_FOIA.html

[16] James Bamford, *The Spy Factory* [television], directed by Scott Willis (Boston; NOVA/The Public Broadcasting System, 2009), http://www.pbs.org/wgbh/nova/spyfactory/credits.html

[17] Peter L. Bergen, *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad* (New York: Crown Publishing Group, 2012), Kindle Edition, 85–86.

C. KEY TERMS

In order to build a foundation for the research and theoretical framework of this thesis, I will define the properties and terms that directly relate to the discussion of the research topic of this study.

1. Dark and Bright Networks

H. B. Milward and Jörg Raab differentiate between dark networks and bright networks when they state,

> …a bright network is legal and visible and a dark network is illegal and tries to be as invisible as possible. Visibility refers to the question of how easy activity of a network is to discern without serious investigative efforts[18] (The spectrum of dark and bright networks is illustrated in Figure 1).

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

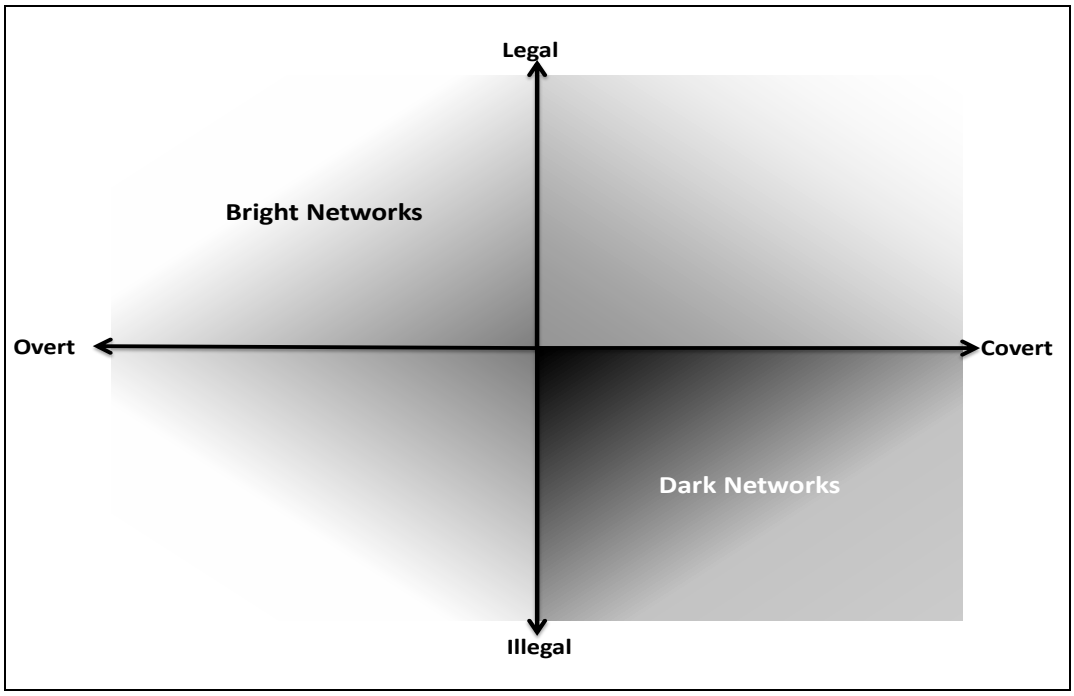


Figure 1. Diagram of Bright and Dark Network Spectrum[19]

2. Network Resilience

Milward and Raab describe resilient dark networks as those confronted with environmental pressures[20] and who, "…are, in principle, able to adapt their structures and behavior or even transform themselves altogether in order to react to changing conditions in their environments."[21] However, as dark networks adapt to these pressures, they must balance the capacity to achieve their goals

[19] Adapted from H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 335.

[20] H. B. Milward and Jörg Raab describe network adaptation to environmental pressures as the *strategic contingent perspective*, which is essentially a dark network variation on organizational contingency theory.

[21] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 334.

with their need for covertness, security, and ultimately survival. Milward and Raab argue that in order to be resilient, dark networks must adapt through the processes of differentiation and integration.[22]

3. Differentiation

For the purpose of this research, differentiation is defined here as the process by which dark networks establish a division of labor in order to replace the functional roles of the captured, killed, or disrupted members who once fulfilled the network's organizational goals. This is often a difficult process when the network's need for security and covertness often leads to increased compartmentalization. While compartmentalization increases the security of the network by restricting information flow between network communication structures, it can also restrict highly specialized roles like bomb makers from having a direct relationship (tie) with the members of the network who may be responsible for emplacing the bomb.

4. Integration

For the purpose of this research, integration is defined here as the process by which dark networks form linkages between specialized roles and operational role counterparts. Through integration, a network establishes mechanisms of communication, authority systems, and adherence to common goals that provide direction and motivation towards collective action. The more specialized roles are, the more reliant other members of the network are on their skills, and the more intricate the integration mechanisms that are required to achieve collective action.[23] A network's need for integration to achieve collective action leads us to a key and related concept of network control. The process of

---

[22] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 343.

[23] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 353.

integration infers that leaders exert control on network members by communicating plans and coordinating efforts to achieve organizational goals.

5. Network Control

For the purpose of this research, network control is conceptualized by Milward and Raab as consisting of two methods of communication that terrorist leaders employ in order to facilitate internal control of dark networks: structure and technology. While the foundation of internal network control is derived from human proximity and face-to-face communications (structure), technology can substitute for human structure and act as a control mechanism under certain conditions (the concept of network control is illustrated in Figure 2).[24] What the principal of network control demonstrates is that the choices of control for dark networks are constrained by the mechanisms of technology and human structure, and that these mechanisms parallel security forces' modes of human and technical intelligence collection and targeting. Furthermore, the parallels of network control and modes of collection and targeting create a basis for strategic interaction between security forces and terrorist networks. It is the process of strategic interaction and a dark networks tendency to adapt to environmental pressure that will form the basis of the theoretical framework for this thesis.

[24] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 346–347.

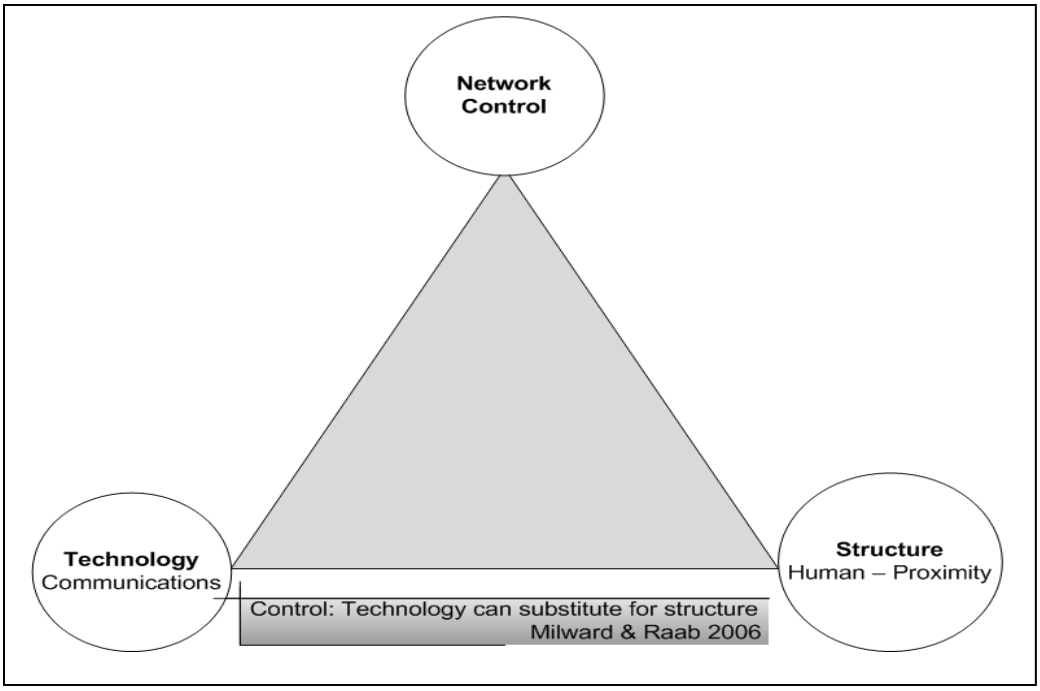


Figure 2. Diagram of Network Control Strategy[25]

6. Social Network Analysis

As described by de Nooy et al., the purpose of social network analysis is to detect and interpret patterns of social ties among actors within a network.[26] The application and measures of social network analysis will be applied in this research to map and describe the network and its activities as the network responds to the external pressure of security forces.

7. Interdiction

For the purpose of this research, the definition of interdiction is modified from Joint Publication 3-03 to specifically refer to an action taken by security forces to divert, disrupt, delay, or destroy a dark network's capability before it can

[25] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 346.

[26] Wouter de Nooy, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek*, 2nd ed. (Cambridge: Cambridge University Press, 2011).

be used against friendly forces, or to otherwise achieve objectives.[27] Through the modes of intelligence collection and targeting researched within this study, security forces operationalize actionable intelligence in order to interdict dark networks.

D. PURPOSE AND OBJECTIVES

This purpose of this thesis is to examine the efficacy of the two prevailing modes of counterterrorism intelligence collection and targeting and their impact on dark network adaptation and resiliency over time. Specifically, it will examine the strategic interaction between security forces' and dark networks and how the employment of HUMINT and NTM modes of collection and targeting compel dark networks to adapt to environmental pressures. In order for security forces to interdict dark networks and prevent terrorist attacks, they require consistent access to relevant and often actionable intelligence and targeting data. Despite a security force's inclination to conceal sources and methods of intelligence, dark networks often react to targeting pressure by obscuring their activities and becoming increasingly covert. Dark network adaptation to targeting pressure can frequently lead to intelligence gaps and lulls in effective targeting that may be both predictable and preventable if identified early in a counterterrorism campaign.

Ultimately, this thesis's objectives are to gain a broader understanding of the efficacy and application of HUMINT and NTM collection and targeting of dark networks. By achieving these objectives, it will generate policy recommendations for operationalizing the outcomes of this study in order to better formulate how HUMINT and NTM collection and targeting can be implemented to address adaptive dark networks. By better understanding the efficacy of each mode's impact on dark network adaptation, security forces will increase their capacity to

[27] Joint Chiefs of Staff, Department of Defense, *Joint Interdiction* (Joint Publication 3-03) (Washington, DC: Department of Defense, 2011), GL-4.

analyze and identify the strategies of dark networks and formulate intelligence and targeting strategies that more effectively address the adaptive ability of dark networks and minimize intelligence gaps in the future.

E. RESEARCH QUESTION

Given the ability of dark networks to adapt to environmental pressures and the constrained decisional framework in which they must control the balance of covertness and capacity to act, it is crucial to understand how security forces' intelligence collection and targeting efforts can be maximized to most effectively address the threat of terrorist networks. While anecdotal evidence indicates a capacity for dark networks to deny and evade national technical means (NTM) and human intelligence (HUMINT) collection and targeting, security forces must analyze the efficacy of each source of intelligence in order to determine how they may be optimally applied against the adaptation of dark networks. This research addresses the question: How can security forces increase the expected utility[28] of HUMINT and NTM intelligence towards interdicting dark networks?

F. THESIS CHAPTER REVIEW

Chapter I provides the background and importance of the research topic in relation to the contemporary operating environment, defines the key research terms, provides the purpose and objectives of the research topic and frames the research question that is the basis of this thesis. Chapter II presents the research hypothesis, defines the variables, and provides a literature review of the broad conceptual and empirical literature as it relates to the theoretical framework of this thesis. Chapter III provides a detailed description of the empirical data, background and special considerations, method and organization of data collection and coding employed in this research, and a detailed description of the methods used to test my hypothesis. Chapter IV presents a summary of the

[28] Von Neumann, John, and Oskar Morgenstern. *Theory of Games and Economic Behavior* (Princeton, NJ: Princeton University Press, 2007), 10.

results, description of the network's behavior in relation to the modes of intelligence collection and targeting, and detailed observations, descriptive analysis and results as they relate to the hypothesis. Chapter V concludes the thesis by providing a discussion of the key research findings, conclusions, policy recommendations and recommendations for future research.

II. HYPOTHESIS AND LITERATURE REVIEW

The primary goal of this chapter is to define the variables that support the research hypothesis, present the hypothesis within the conceptual framework of the strategic interaction model, and describe the nature of their relationships and potential effects between variables. Lastly, this chapter will survey the existing body of literature related to the field of intelligence collection and targeting and dark network adaptation and resilience in order to identify current research perspectives and identify areas where additional contributions can be made within this field of study.

A. DEFINING THE VARIABLES

In order to control for the contrasting expectations of efficacy for NTM and HUMINT targeting of dark networks, this thesis takes a multivariate approach in analyzing the stated research question. To achieve this goal, the hypothesis identifies several causal mechanisms that explain the relationships between the modes of target intelligence collection and the degree of influence that they have on successful counterterrorism operations. The hypothesis defines the independent variable (IV) as being the type of intelligence collection and targeting used by security forces to interdict dark networks. The types of intelligence that have been selected for the independent variable are the two dominant modes of intelligence collection and targeting: human intelligence (HUMINT-IV1) and national technical means (NTM-IV2). Each source of intelligence can either serve as a pure or mixed collection and targeting strategy when used independently or in tandem. The hypothesis predicts that each source of intelligence (HUMINT and NTM) will also serve as an antecedent condition when employed as a mixed strategy and under specific conditions.[29] This means that each independent variable serves to magnify the effect of the other

[29] I will describe how the independent variables will serve as antecedent conditions under specific criteria in the theoretical framework.

independent variable on the dependent variable when used in tandem. The hypothesis defines the intervening variable (IntV) to be a dark network's adaptation to environmental pressure. Dark network adaptation refers to the process of identifying environmental pressures and employing the network control mechanisms of technology (high-tech) or human structure (low-tech) to counter environmental pressure by balancing degrees of security and collective action (See network control strategy in Figure 2).[30] The hypothesis defines environmental pressure as the collection and targeting pressure exerted by state security forces on a dark network. The dark network's strategy for adaptation is divided into four choices: maintain the status quo (do nothing); employ a mixed strategy of high and low-tech communications; employ a pure strategy of high-tech communications; or employ a pure strategy of low-tech communications. Although there were varying measures of network effectiveness (raw interdictions or weighted significance of detainees) that could have been used to measure the causal relationship between the modes of intelligence collection and targeting, this study selected the network performance measure of "attacks per capita" over time as the dependent variable (DV) (see path analysis in Figure 3).

[30] Network adaptation under environmental pressure is essentially the use of control mechanisms to balance network visibility (covertness) and the capacity to act. Differentiation and integration as defined by H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006).

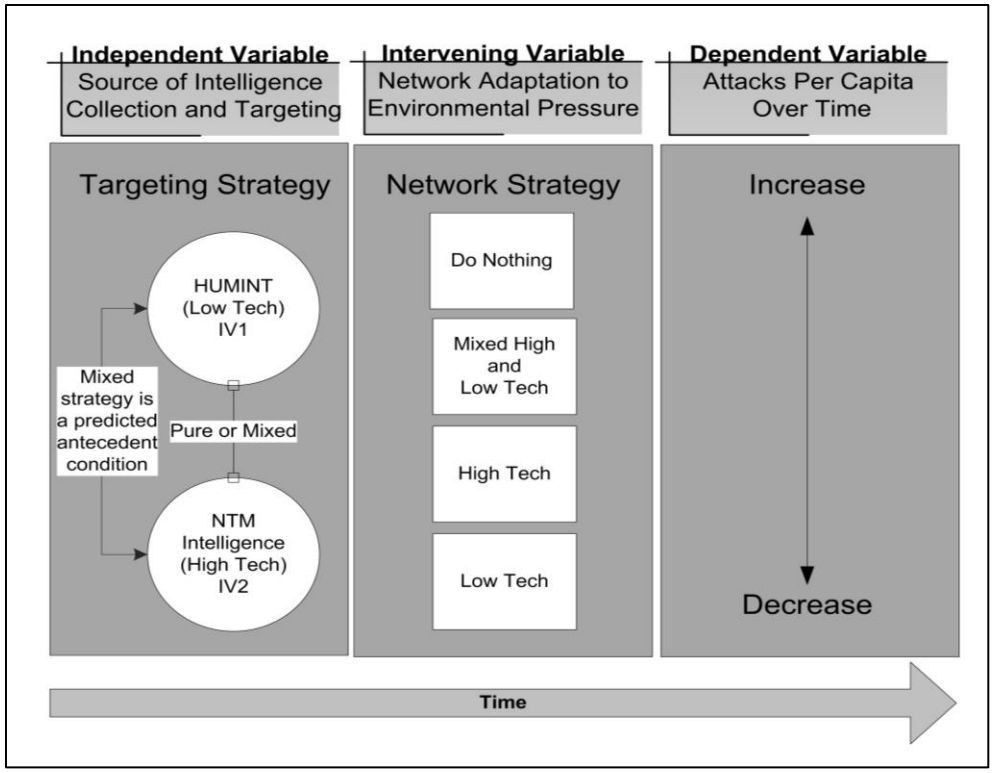


Figure 3. Hypothesis and Path Analysis

1. Independent Variable 1

HUMINT refers to human intelligence defined as a category of intelligence derived from information collected and provided by human sources.[31] However, human intelligence is a far more diverse intelligence collection tool than policy makers and practitioners realize. As Michael Butler describes,

> HUMINT in practice is a multifaceted process—an amalgamation of a variety of tools, including unilateral penetration operations, direct

[31] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02) (Washington, DC: Joint Chiefs of Staff, 1999, amended through 2009), 249.

recruitment of agents from an adversarial group, recruitment of access agents, interrogation, intelligence liaison, and the handling of walk-in agents.[32]

2. Independent Variable 2

NTM refers to technical intelligence (TECHINT), or the broad use of technologies rather than the direct use of humans to collect information through traditional espionage.[33] One such type of NTM was detailed in Mark Bowden's book, *Killing Pablo: The Hunt for the World's Greatest Outlaw*, when he described the radio direction-finding equipment used by special Columbian police in the search for Pablo Escobar.[34]

3. Intervening Variable

Network adaptation to environmental pressure is essentially the use of network control mechanisms to balance network visibility (covertness) and the capacity to act.[35] For the purpose of this thesis, network adaptation will be measured through the social network analysis measure of geospatial degree centralization, which will be described in greater detail in the methods section of this thesis.

4. Dependent Variable

In order to employ a more sophisticated and quantifiable measure of dark network performance as it relates to a security force's intelligence collection and targeting (external pressure) of the network, this thesis will use the measure of

---

[32] Michael Butler, "Killing Cells: Retooling Human Intelligence Collection for Global Decentralized Terrorism," presented at ISA's 50th Annual Convention, New York, February 2009, http://www.allacademic.com/meta/p310663_index.html

[33] Howard O. DeVore, 1999, *Jane's Special Report: China's Intelligence & Internal Security Forces* (Alexandria, VA: Jane's Information Group), ch. 7.

[34] Mark Bowden, *Killing Pablo: The Hunt for the World's Greatest Outlaw* (New York: Atlantic Monthly, 2001), 79.

[35] H. B. Milward and Jörg Raab, "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006): 346–347.

"attacks per capita" as defined by the total number of attacks divided by the total number of free network members during the given time period (during the span of time that security forces actively collected intelligence and targeted the network).

B. HYPOTHESIS

Given the mode of security forces' intelligence collection and targeting and the adaptation of dark networks to environmental pressure, the hypothesis should predict the probability of success of counterterrorism operations overtime. By employing a strategic interaction model (see Figure 4. below), the hypothesis frames the vulnerabilities and strengths of each strategy in order to predict what decisions will be made in order to reduce the risk or achieve the greatest benefit for each opponent. Similar to Ivan Ivan Arreguín-Toft's theory of asymmetric conflict, a dark network is more likely to create an asymmetric alignment of strategies between itself and security forces when it is confronted with a militarily stronger opponent.[36] In other words, a dark network is expected to employ a strategy that does not directly play into its opponent's strengths. This hypothesis predicts that a dark network will recognize the origin of environmental pressures applied by its opponent and modify its behavior in order to achieve an asymmetrical strategy—and consequently greater security.[37]

---

36 Ivan Arreguín-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge, UK: Cambridge University Press, 2005), 35.

37 It is not necessary for a dark network to pinpoint the specific origin or mode of targeting in order to create asymmetry. The spectrum of adaptation can range from completely open to completely closed organizations, with the latter achieving the greatest security in exchange for the lowest degree of trust and operational efficiency.

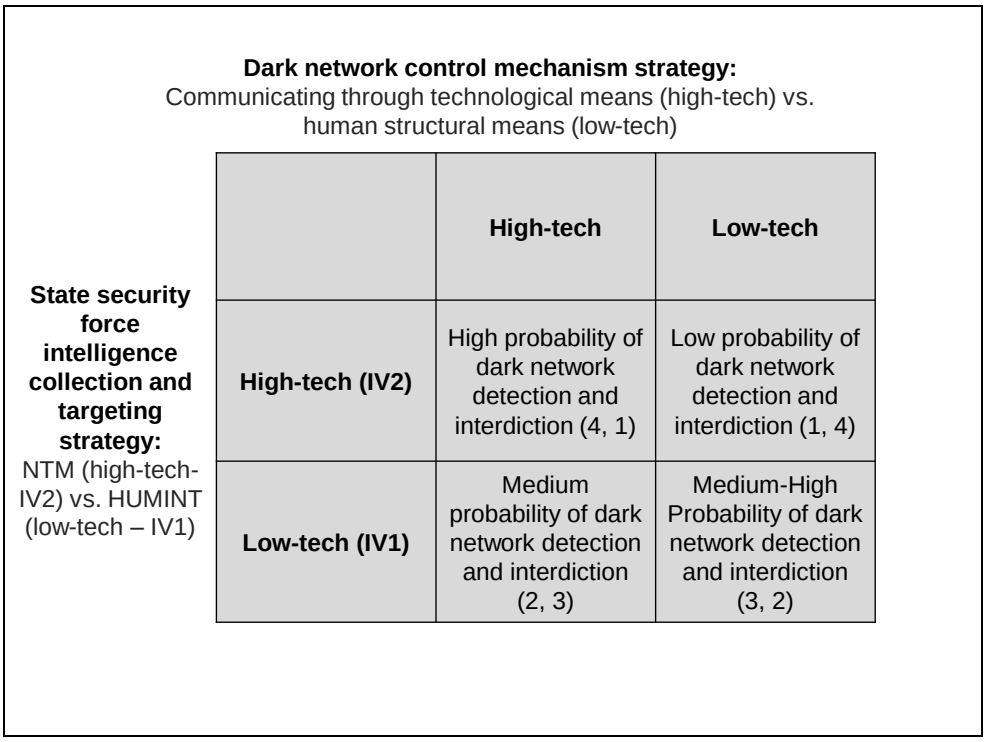


Figure 4. Hypothesis: Strategic Interaction Model[38]

This model demonstrates the strategic interaction between a dark network and the opposing security forces' selected mode of targeting (which I establish is an environmental pressure) on the network. When a dark network is faced with an environmental pressure of high-tech intelligence collection and targeting strategy from security forces, the network will choose to modify their behavior to a low-tech human control strategy (high-low). The resulting low-tech strategy affords the dark network the greatest degree of security and lowest probability of detection and interdiction. The dark network achieves greater security in a High-Low strategic interaction because the security forces' high-tech strategy is incapable of identifying and interdicting a dark network with a low-tech strategy.

[38] The strategic interaction model demonstrates opposing high and low technological strategies for security forces and dark networks. The model predicts a two-organization zero sum game. When a low-tech dark network strategy opposes a security forces high technology strategy, the hypothesis predicts a (1, 4) outcome with 4 being a winning strategy for the dark network and 1 being a losing strategy for security forces.

Conversely, if a dark network fails to modify its behavior and instead chooses to maintain a high-tech means of control, security forces' employment of a high-tech means of intelligence collection and targeting strategy will result in the highest probability of detection and interdiction of the dark network. Furthermore, if the dark network and security forces both select a low-tech strategy (Low-Low); security forces will maintain a greater potential advantage (though slightly degraded from the optimal High-High) over the dark network because of the versatile and resilient nature of HUMINT in combination with the security forces' greater material advantage. Finally, if a dark network chooses to maintain a high-tech strategy and opposing security forces employ a low-tech strategy (Low-High), the security forces are still able to maintain a greater potential advantage because HUMINT source operations are capable of collecting and targeting a dark network whether or not they employ a technological (high-tech) or human structure (low-tech) control mechanism.

It is important to note that a chosen strategy and an opponent's counter strategy are not necessarily dichotomous in this model, and that mixed strategies can be employed with increasing or decreasing degrees of success by both opponents. Based on this theoretical model, several inferences can be made in relation to mixed strategies by security forces. First, because a security forces' low-tech strategy can be employed in some degree across any control mechanism a dark network employs (high or low-tech), it can be reasoned that establishing a threshold of HUMINT in all quadrants would be beneficial to security forces. Second, since a high-tech strategy by security forces can only be effective against a dark networks high-tech strategy, it can be hypothesized that a high and low-tech mixed strategy against a dark networks high-tech strategy would increase the effectiveness of collection and targeting if collection is not wholly redundant.[39] Since I have established that a security forces' low-tech

[39] Even if collection is redundant, the information gleaned would provide greater clarity to decision makers on matters of targeting (i.e., all-source intelligence collection).

strategy can be employed in varying degrees of success across any network control strategy (High or Low-Tech), the inclusion of a high-tech strategy would serve as an antecedent condition capable of increasing the success of HUMINT (low-tech) driven network interdictions (High*Low versus High). The same inference of mixed strategy antecedent condition cannot be made when a dark network employs a low-tech strategy because a security forces' high-tech strategy has no antecedent relationship with a low-tech strategy under these conditions. The only other option available is for a dark network to employ a mixed strategy of their own, in which case, a mixed strategy by security forces would maintain a greater potential advantage because of the antecedent condition and greater material advantage (High*Low versus High+Low). The strategic interaction that frames this theoretical framework is represented in Figure 4.

As security forces continue to target terrorist networks with a predisposition for technical intelligence collection, security forces run the risk of generating intelligence gaps that are both predictable and preventable. While the sophistication and adaptability of the dark networks that will be examined in this narrative are not the norm, they do represent a dark network's most dangerous course of action against security forces and non-combatant populations. It is because of this danger that it is important that security forces understand the strategic interaction between intelligence collection and targeting and dark network adaptation to environmental pressures. The better security forces understand these dynamics, the more effectively they can apportion intelligence collection assets against emerging threats and better generalize the principles of this study in future counterterrorism campaigns.

C. LITERATURE REVIEW

This literature review seeks to achieve four objectives. First, it surveys the relevant historical body of literature related to research focused on the mode of human intelligence collection and targeting. Second, it examines literature related

to research focused on the mode of national technical means intelligence collection and targeting. Third, it explores literature related to research focused on dark network adaptation and resilience to external pressure. Finally, it summarizes the significance and implications of this review for my hypothesis. It is not intended to be fully comprehensive, but rather descriptive of the current state of research in this field of study.

In order to separate the opposing perspectives on the efficacy of low and high technological counterterrorism intelligence collection and targeting, I have extracted the principal intelligence collection themes from each work within the greater body of literature. While a number of works within this body of literature advocate all-source collection as the primary mode of targeting, a deeper examination of these works reveals a predisposition for one mode of targeting over the other. I have also included intelligence collection works focusing on counter-insurgency doctrine, as the two fields are closely related when reduced down to the effective modes of targeting for both strategies. While counterinsurgency deals with the application of grand strategy, counterterrorism is more narrowly focused on the related counterinsurgency tactic or strategy subset of countering or suppressing terrorist actions against security forces and or a non-combatant population. Finally, this review will briefly explore several perspectives on war in the information age and its significance in understanding how dark network's communicate, adapt, and survive when confronted with external pressure.

1. Human Intelligence and Targeting

A review of the historical body of literature pertaining to human intelligence (HUMINT) collection and targeting demonstrates that while numerous academics and intelligence analysts have long praised the impact of HUMINT on counterterrorism operations, there is still an organizational aversion by many U.S. intelligence officers and senior military leaders to prioritize HUMINT as the

primary collection and targeting platform for interdicting terrorists. Retired Air Force Colonel Steven O'Hern has explained why this cultural bias is prevalent in the military intelligence community:

> There are several reasons why leaders of military intelligence organizations favor technical intelligence. Officers who rise to become general officers within military intelligence organizations nearly all arise from backgrounds that involve technical intelligence gathering, including collecting and analyzing electronic signals such as radio communications and supervising satellites and reconnaissance aircraft and the analysis of the images they produce.[40]

Despite O'Hern's anecdotal evidence of organizational bias favoring technical intelligence within the U.S. military intelligence community, there are also several tangible reasons why this attitude persists. HUMINT admittedly has its faults and those shortcomings often color the perceptions of commanders who strongly prefer NTM intelligence because of its perceived reduced susceptibility to human influence and error. With increasing emphasis by senior military leaders to expand and develop U.S. military's cyber operations and security capabilities, existing organizational bias towards NTM intelligence will likely persist into the immediate and long-term future. However, O'Hern provides critical insight into the rationale of military decision makers and analysts who are responsible for developing counterterrorism intelligence collection and targeting plans. By understanding these organizational perspectives, policy prescriptions can be more effectively formulated and presented to address these known biases and concerns.

In Katya Drozdova and Michael Samoilov's 20101 study of al Qaeda communications, they develop a predictive analysis model for detecting the traceability of both high-tech and low-tech terrorist communications in order to prevent future terrorist attacks. Their findings provide a foundation for the

---

[40] Steven K. O'Hern, *The Intelligence Wars: Lessons from Baghdad* (Amherst, NY: Prometheus Books, 2008), 119.

proposed causal framework (strategic interaction model) of this thesis, enhance the understanding of dark network vulnerabilities in relation to network communication choices, and provide a contextual understanding of how dark networks adapt their modes of communication to increase resilience. First, they describe actions taken by dark networks to reduce structural network vulnerabilities through their chosen modes of communication, leading them to conclude that:

> Modern hi-tech devices create electronic traces of organizational activity. Monitoring these traces improves opponent's knowledge of the FINO,[41] increasing its risk of detection and damage from counteraction. Alternatively, low-tech choices leave physical or social traces that may be difficult to follow in a timely manner—if at all—thus effectively concealing information about FINO vulnerabilities.[42]

Their findings assert that a dark network's use of high-tech communications increases its vulnerability to NTM intelligence collection and targeting, while the use of low-tech communications reduces structural network vulnerabilities to NTM and makes it more resilient overtime. They reason that external network pressure (shock) compels dark networks to decentralize and minimize their traceability in order to limit network damage and provide time and space for recovery.[43] This suggests that the effectiveness of NTM intelligence collection and targeting diminishes over time as dark networks adapt to external pressure.

---

[41] FINO is described by Drozdova and Samoilov as failure or fault-intolerant network organizations, which are networks where the loss of a single node could result in catastrophic failure of the network.

[42] Katya Drozdova and Michael S. Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory 16* (2010): 67, DOI: 10.1007/s10588-009-9058-2.

[43] Katya Drozdova and Michael S. Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory 16* (2010): 66, DOI: 10.1007/s10588-009-9058-2.

Another key finding in this study concludes that low-tech signals (spikes in behavior that differ from normal baseline behavior) consistently occur prior to attacks, providing an early warning, while a similar analysis of high-tech communication signals does not produce a traceable signal to assist security forces in preventing attacks.[44] These findings are significant to my hypothesis in that they parallel a dark network's communication strategy in relation to a security forces mode of intelligence collection and targeting. Although the study indirectly advocates for a security forces use of HUMINT collection and targeting against dark networks, the final policy recommendations advocate for a multi-source (all-source intelligence) data approach for detecting low-tech and high-tech signals in order to predict and prevent future terrorist attacks.

In Michael Butler's 2004 paper on retooling human intelligence for global decentralized terrorism, he proposes a change from what he coins the current recruitment-centered model (RCM) of HUMINT collection to a more threat identification-centered model (TICM) of HUMINT collection.[45] Although the purpose of his paper is to provide policy prescriptions for changing the outdated Cold War model of HUMINT collection to a more threat centric model for counterterrorism, many of Butler's policy prescriptions are still germane to this thesis. The significance of his research and recommendations to this thesis is the TICM's application to decentralized dark networks and the broad menu of options presented within the mode of HUMINT collection and targeting. Butler specifically focuses on developing a threat centric collection plan that primarily recruits a network of access agents to map terrorist network(s) and provide opportunities for employing the additional options of intelligence liaison, unilateral network

---

[44] Katya Drozdova and Michael S. Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory 16* (2010): 81, DOI: 10.1007/s10588-009-9058-2.

[45] Michael Butler, "Killing Cells: Retooling Human Intelligence Collection for Global Decentralized Terrorism," paper presented at ISA's 50th Annual Convention, New York Marriott Marquis, New York, February 2009, http://www.allacademic.com/meta/p310663_index.html

penetration, terrorist walk-ins, interrogations, and direct recruitment of terrorists for network penetration. Most importantly, Butler's policy prescriptions provide a basis for formulating HUMINT collection and targeting options within broader all-source intelligence strategy, and provide a menu of relevant recommendations that can be applied to the results and findings of my thesis.

2. National Technical Means Intel and Targeting

A review of the historical body of literature pertaining to national technical means (NTM) intelligence collection and targeting indicates a developed research focus on the growing technological savviness of ordinary individuals and their ability to leverage technology to achieve a comparative advantage over the state security apparatus. In his book, *Brave New War*, John Robb states that the leveraging of technology by terrorists, "…has finally reached a point where small super empowered groups, and not yet individuals, now have the capability to challenge the state in warfare and win."[46] Robb is an advocate of fourth generation warfare (4GW), which has been deemed by some scholars (Echevarria, 2005)[47] to be a rebranding of insurgency doctrine. He contrasts with traditional 4GW decentralized warfare advocates in his use of technology and the information age as an antecedent condition for achieving decentralized collective action (attacks). He sees globalization and the transference of technology as empowering individuals and ideologues to join dark networks and enabling them to coordinate attacks and rapidly adapt to changes in tactics and strategies of the state security apparatus.

Robb's 4GW perspective is likely influenced by Arquilla and Ronfeldt's research on netwar and swarming phenomena observed in decentralized

---

[46] John Robb, *Brave New War, The Next Stage of Terrorism and the End of Globalization* (Hoboken, NJ: John Wiley and Sons Inc., 2007), 311.

[47] Antulio Joseph Echevarria, *Fourth-Generation War and Other Myths* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2005).

warfare.[48] This perspective is not unlike the actions of flash mobs where disparate individuals organized through social media suddenly swarm public locations in order to achieve an innocuous act of collective action and then disappear as quickly as they appeared. More deleterious examples of this phenomenon have been observed in the online homegrown self-radicalization of terrorists similar to the alleged activities of the Tsarnaev brothers prior to the Boston Marathon bombings in April 2013.

Although technology has enabled highly decentralized dark networks to train, coordinate, and achieve collective action, these networks are not immune to detection or surveillance. While technological dominance of state security forces ebbs and flows, there are strong indications that both centralized and decentralized dark networks are still vulnerable to intelligence collection and targeting. Recent indictments by the U.S. Department of Justice of Chinese military hackers conducting elicit hacking of U.S. businesses[49] and the publication of Mandiant's exposé (February 2013)[50] on the Chinese People's Liberation Army (PLA) hacking unit 61398 demonstrates that even the world's most centralized, sophisticated, and technologically advanced hackers are vulnerable to intelligence collection and targeting. Similarly, recent arrests by the FBI of 90 hackers across 19 different countries associated with illegal and malicious activity using Blackshades remote malware demonstrates that even highly geospatially decentralized networks can be surveilled and interdicted across international boundaries.[51]

---

[48] John Arquilla and David F. Ronfeldt, *Swarming & the Future of Conflict* (Santa Monica, CA: RAND, 2000).

[49] Ashley Fantz, "Chinese Hackers Infiltrated U.S. Companies, Attorney General Says," CNN, May 19, 2014, http://m.cnn.com/primary/wk_article?articleId=cnn/2014/05/19/justice/china-hacking-charges&branding=&category=cnnd_latest&pagesize=10.

[50] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013).

[51] Evan Perez, "More than 90 People Nabbed in Global Hacker Crackdown," CNN, May 19, 2014, http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/.

Jennifer Sims's study on intelligence and counterterrorism advocates for a "constructively redundant" method of all-source collection and targeting for counterterrorism operations. Although she focuses on the application of multiple sources of intelligence, her conclusions indicate that her focus on rapid response and technology in counterterrorism operations is indicative of an unintentional organizational bias towards NTM.[52] This bias is further evidenced throughout her study with examples of terrorist technological communications countered by a baseline of NTM collection with OSINT and HUMINT only serving as enablers or 'additional' sources for intelligence corroboration. Although it is important to respond quickly to terrorist threats in order to prevent attacks, research conducted by Katya Drozdova demonstrates that the application of HUMINT and not NTM is a more effective source of intelligence for preventing terrorist attacks conducted by sophisticated dark networks.[53]

However, the most relevant element of Sims's research to my thesis is her observation on the effectiveness of the modes of intelligence collection and targeting in relation to decisions and actions of dark networks. Her observations provide a construct for explaining the strategic interaction between a security forces mode of intelligence collection and targeting and a dark network's mode of communication (network control structure). She describes the degree of effectiveness of the modes of intelligence collection and targeting as:

> The productivity of any of these collectors against a particular target will depend on that collector's access to the target's most vulnerable point. For example, if a network of spies uses wireless radios, picking up their electronic emissions (TECHINT) will be an effective way to find them; if they use couriers, human agents secretly opening the letters and packages (HUMINT) is likely to work best; if the adversary believes he is unobserved, collecting the

[52] Jennifer Sims, "Intelligence to Counter Terror: The Importance of All-Source Fusion," *Intelligence and National Security*, 22, no. 1 (2007): 38–56.

[53] Katya Drozdova, *Analyzing Terrorist Communications: Detecting Early Signals of Attack* (Stanford, CA: Hoover Institute on War, Revolution, and Peace, 2009), 21.

> names of those he visits from a phone book or the sites he visits while traveling as an ostensible tourist (OSINT) would be useful.[54]

In summary, Sims's observation not only enforce the strategic interaction model within my hypothesis, it also provides a framework for formulating all-source policy prescriptions for developing more effective intelligence collection plan that is focused on a dark network's mode(s) of communication (network control structure).

Jackson et al.'s study on terrorist's counter-technology strategies provides a basis for understanding terrorist denial strategies against a state security forces' technology based counterterrorism efforts.[55] They establish that most counterterrorism technologies are degraded by counter-technology strategies over time. They also address how terrorist organizations adapt to technologies by "…altering operational practices, making technological changes or substitutions, avoiding the defensive technology, and attacking the defensive technology."[56] Their findings re-enforce the hypothesis that the effectiveness of NTM collection and targeting of dark networks erodes over time. Specifically, every terrorist organization they analyzed (JI, LTTE, PIRA, Hamas, Palestinian Islamic Jihad) focused counter-technology strategies on avoiding specific modes of high-tech communication in order to negate intelligence collection and targeting. They also determined that by continuing to employ technical intelligence collection and targeting, security forces compel dark networks to continually employ counter strategies to avoid technical intelligence collection-increasing the network's operational risk.

---

[54] Jennifer Sims, "Intelligence to Counter Terror: The Importance of All-Source Fusion," *Intelligence and National Security*, 22, no. 1 (2007): 42.

[55] Brian A. Jackson et al., *Breaching the Fortress Wall Understanding Terrorist Efforts to Overcome Defensive Technologies* (Santa Monica, CA: Rand Corporation, 2007), 132.

[56] Brian A. Jackson et al., *Breaching the Fortress Wall Understanding Terrorist Efforts to Overcome Defensive Technologies* (Santa Monica, CA: Rand Corporation, 2007), 116.

3. Dark Network Change and Resilience

The final body of literature relevant to this thesis is research focused on the characteristics and dynamics of dark network change and resilience. In order to develop a qualitative understanding of network resiliency to assist in the modeling of this study's dark network data set, it is important to develop an understanding of what renders dark networks resilient to exogenous and endogenous pressure (shock). Bakker, Raab, and Milward[57] propose a comprehensive theory of why some dark networks demonstrate greater resiliency than others. By conducting a with-in and cross-case analysis of three dark network data sets (Unkhonto we Sizwe (MK), Liberation Tigers of Tamil Eelam (LTTE), and Fuerzas Armadas Revolucionarias de Columbia (FARC)), they develop a framework of networked capabilities (replacing actors, linkages, and balancing integration and differentiation) and network characteristics (resources and legitimacy) that contribute to network resiliency and increased operational activity (network performance).[58] Their findings re-enforce existing research on network topology and resilience by identifying network centralization and motivation as moderating variables that impact resiliency. They conclude that highly centralized networks magnify the effect of shock to a network's legitimacy and resources, while more decentralized networks are more effectively structured to mitigate the impact of shock. Furthermore, they argue that network motivation influences network resilience through the recruitment of new members and the replacement of nodes and linkages. Networks motivated by grievances are more likely to be impacted by changes in legitimacy, while networks motivated by greed were likely to be impacted by changes in resources. In summary, Bakker, Raab, and Milward provide an excellent contextual framework for interpreting

[57] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[58] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

analytic results related to network resilience and performance and offer several potential approaches for measuring the effects on the dependent variable of my hypothesis.

One of the infrequently researched areas in the analysis of dark network resilience and change has been the use longitudinal analysis to better understand how dark networks change over time. Specifically, very few studies have analyzed how dark networks adapt in a hostile environment to the exogenous pressure (shock) of security forces intelligence collection, targeting and interdiction. The absence of research in this area has been largely due to sparse longitudinal data on dark networks. However, a 2011 study by Everton and Cunningham employs longitudinal analysis to examine the Noordin Top terrorist network, providing insight into dark network adaptation, effectiveness and performance over time.[59] Using descriptive statistics, multivariate regression, and topographic metrics (density, centralization, and fragmentation) to examine the Noordin Top network, they arrived at several conclusions relevant to this thesis. They determined that the Noordin Top network became increasingly dense (average degree) during times of increased exogenous pressure (shock) or concern for security and decreased as the network reduced its operational activities. Additionally, the network became increasingly centralized as it planned and conducted high profile attacks. This network behavior is consistent with previous research that indicates dark networks occasionally adopt fault-intolerant network organizational (FINO) structures (i.e., increasing centralization) when planning and executing attacks. Drozdova and Samoilov attribute this decision to a cost-benefit analysis that prioritizes the success of the mission over the survival of operational nodes.[60] This increased centralization may also explain why the

[59] Sean F. Everton and Dan Cunningham, "Terrorist Network Adaptation to a Changing Environment" in *Crime and Networks*, ed. Carlo Morselli (New York: Routledge, 2011), 287–308.

[60] Katya Drozdova and Michael S. Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory* 16 (2010): 66, DOI: 10.1007/s10588-009-9058-2.

Noordin Top network became increasing fault-intolerant (vulnerable) over time and ultimately collapsed following the death of Top in September 2009. Finally, topographic fragmentation metrics indicated that the network became increasingly cohesive (low fragmentation) during times of high operational activity and became increasingly fragmented following successful counterterrorism operations against the network. The findings of this study provide a foundation for interpreting the results and analysis of the longitudinal data set of this thesis and offer a preliminary model for formulating the path analysis that will be used to test my hypothesis.

4. Literature Review Conclusions

An examination of the existing literature found that there are three key points of analysis absent in relation to my hypotheses. First, the balance of existing literature lacks any relevant study of the causal relationship between the mode of targeting, the intervening variable of network adaptation to environmental pressure (shock),[61] and the predicted interaction and subsequent causation that these two variables have on varying measures of dark network performance over time.

Secondly, while a great number of COIN and counterterrorism intelligence related literature emphasizes HUMINT, only a small percentage of these works address the decision framework of terrorist networks in response to security force intelligence collection and targeting efforts. Of the small percentage of works that examine the strategic interaction between terrorists and the environmental pressures of intelligence collection and targeting, none advance these ideas beyond simple recognition of the phenomena into a more useful empirical analysis for improving intelligence collection strategies.

---

[61] The strategic interaction between dark networks and security forces is similar to *Strategic Contingency Perspective* in the field of organizational theory and design. H. B. Milward and Jörg Raab, "Dark Networks as Problems," *Journal of Public Administration Research and Theory* 13, no. 4 (2003): 415.

Finally, nearly all of the existing literature related to intelligence collection and targeting in some degree advocates one source of intelligence over the other, but there has been no examination of the scale of intelligence collection required to sustain successful counterterrorism operations over time. This analytic void begs the question of how much intelligence collection (HUMINT or NTM) is necessary to achieve a threshold[62] of collection capable of adapting and overcoming predictable intelligence gaps.

[62] While collection efforts are determined by the anatomy of the environment and terrorist organization, there are clearly levels of collection that must be achieved in order prevent future intelligence gaps. An intelligence collection infrastructure must be flexible enough to detect emerging threats and provide sufficient actionable intelligence to provide security forces the time and space to establish effective collection efforts against those threats.

III. DATA AND METHODS

A. DATA DESCRIPTION

The anonymized terrorist network data used for this study was generated by multiple government organizations over a period of 27 months. This network was selected due its sophistication, advanced tradecraft, and resilience to security force's targeting. Temporal, geospatial, and relational data were aggregated from all known free, killed, or captured members of the network. The total number of network members was determined to be 409 at the time of coding with 40 of those members having been identified as senior leadership within the network.

The raw unstructured data collected consisted of all-source intelligence analysis reports, significant activity reports (SIGACTs), interrogation reports, targeting databases, human intelligence reports, technical intelligence reports, and forensic reports related to forensic attack analysis. Human intelligence reports from detainees and human source operations were analyzed to compliment and validate the network's raw data and provide a greater qualitative understanding of the network's adaptation to environmental pressures and the degree of intelligence tradecraft it employed to evade targeting by security forces.

The scope and richness of data used in this study provided an excellent opportunity for exploring network structure across relational, geospatial, and temporal boundaries. Observations on the security forces' pressure on the network (raids, interdictions, modes of intelligence used) and the dark network's activities and responses to exogenous pressure (attacks, disposition, and modes of communications used) provided an excellent opportunity to test the strategic interaction model and identify the magnitude of performance and resiliency observed in the dark network. Although, relational ties were aggregated on all 409 members, the relatively small number (40) of senior leadership nodes and

observed HUMINT driven interdictions (9) posed some challenges in the application of statistical analysis and significance measures when conducting path analysis. These issues are addressed in further detail in the methods portion of this chapter.

1. DOCUMENT ANALYSIS AND DATA CODING

a. Document Analysis

Because of the extensive scope and nature of available data for this study, the method of document analysis was employed to review all available intelligence reporting and analytic products related to the observed network and security force's activities. Document analysis was selected as a method to complement and corroborate the quantitative methods utilized in this study. From the base of information established through document analysis, I was able to increase the validity, granularity, and contextual understanding of the quantitative results and findings. Glenn Bowen[63] defines the method of document analysis as:

> …a systemic procedure of reviewing or evaluating documents-both printed and electronic (computer-based and internet-transmitted) material. Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge.[64]

Although some of the limitations of document analysis are derived from the selection of documents examined, this study methodically reviewed all

[63] Glenn Bowen, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9, no.2 (2009): 27–40.

[64] Glenn Bowen, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9, no.2 (2009): 28.

available intelligence and operational reporting and analytic products of the observed network in order to reduce potential bias and increase the triangulation[65] of the analytic methods of this study.

b. Data Coding

In order to develop structured quantitative data from a host of unstructured (raw) intelligence and targeting documents analyzed in this study, content analysis (quantitative extension of document analysis)[66] was used to code all documents along the themes and variables relevant to my hypothesis. Data coding is described by Gough and Scott as a method to:

> …organize, manage, and retrieve the most meaningful bits of our data. The usual way of going about this is by assigning tags or labels to the data, based on our concepts. Essentially, what we are doing in these instances is condensing the bulk of our data sets into analyzable units by creating categories with and from our data.[67]

Content analysis coding was achieved using the Palantir software program through the process of tagging (structuring) available intelligence and targeting reports selected during document analysis. Special care was taken to establish standards for coding objects, properties, and relationships in order to not bias the data from inconsistent coding. Since Palantir had already been used to code and analyze data from previous terrorist organization data sets, the existing ontology provided an excellent foundation to code the observed network.

---

[65] Triangulation is defined as, "a process that uses multiple data sources, data collection methods, and or theories to validate research findings, help eliminate bias, and detect errors or anomalies in discoveries" By employing methodological triangulation, this study corroborated different sources of data and increased the overall validity of the findings and recommendations. Charles Lusthaus, *Organizational Assessment: A Framework for Improving Performance* (Ottawa: International Development Research Centre, 2002), 190.

[66] Glenn Bowen, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9, no.2 (2009): 28.

[67] Stephen Gough and William Scott, "Exploring the Purposes of Qualitative Data Coding in Educational Enquiry: Insights from recent research," *Educational Studies* 26, no.3, (2000): 339–354, DOI: 10.1080/0305569005013714

The existing ontology was only slightly modified to account for unique properties and events associated with the observed network. I was able to map the network and structure rich one-mode and two-mode data sets covering a wide range of object properties and relationships (attributes and affiliations), as well as link and geocode individual members to network activities (capture, kill, attacks, meetings, etc.). Additionally, security forces' activities were coded to provide geocoded and temporally categorized data for targeted raids. The mode(s) of intelligence collection and targeting was also included and was ultimately linked to the specific members of the network who were captured or killed. Once the structured data coding and network visualization were completed in Palantir,[68] the structured social network data was exported into Organizational Risk Analyzer (ORA)[69] in order to generate both longitudinal and spatial observations of the network as well as conduct analysis.

2. Data Sources

a. All-Source Intelligence Analysis Reports

All-source intelligence reports provided a holistic understanding of the network's leadership, activities (attacks, etc.), motivations, resources (funding activities), communications, and capabilities (tradecraft, denial capacity). This information was updated regularly in order to provide the most up-to-date picture of the network to other analysts and decision makers. These documents were the result of multiple analysts across multiple intelligence disciplines working together to provide the most comprehensive picture of the network as possible.

---

[68] Palantir Technologies Software, can be purchased for use from the Palantir government website: http://www.palantirtech.com/government.

[69] ORA (Carley 2001-2011) can be downloaded for free for noncommercial use from the ORA website: http://www.casos.cs.cmu.edu/projects/ora/.

b. Significant Activity Reports

Significant activity (SIGACT) reports used for this research were published regularly by security forces during the 27 months the network was observed for this study. They included a detailed snapshot of hostile attacks against the government, security forces and non-combatants. A SIGACT snapshot included the: who, what, when, where, and why (5Ws) of attacks related to bombings, small arms attacks, mortar, and rocket attacks. If a group (dark network) claimed responsibility for an attack or the attack had an easily recognizable operational or forensic signature of a specific network, that information was normally included in the report as well.

c. Interrogation Reports

Interrogation reports used for this study included information related to interrogations of enemy prisoners of war. These provided standard demographic information of the detainee as stipulated in the NATO standardization agreement (STANAG 2033). They also included details about the date, time, location, and circumstances of capture, time of report, capturing unit, date of birth, place of birth, nationality, detainee number, languages, marital status, documents and equipment on detainee when captured, physical condition, job, mental condition, education, experience, information gathered during the interrogation session, and an evaluation of the reliability of information provided. Finally, the reports provided information related to family members and known associates.

d. Targeting Databases

Targeting databases used for this study included information about past, present, and current members of dark networks within the security forces' area of operations. These databases provided information about the position (leadership, courier, logistician, financier, bomb maker, etc.) that each targeted member held within the network (if known), known connections (ties), family members (if known), and where the individual was last reported to be located at the time of

the report. If captured, these databases included the mode of intelligence used in the capture, as well as the time and location of capture. Finally, uncaptured members within the database were prioritized based on their targeting importance, which was often subjectively assigned at the direction of commanders and decision makers. The information in these reports were updated weekly, which allowed for security forces to conduct trend analysis and identify significant movement of network members from one week to the next.

e. HUMINT Reports

Human intelligence reports (intelligence information reports (IIR)) included in this study were derived from human intelligence sources and used to report HUMINT information in response to command directed collection requirements. This information provided context and information related to the network's activities, relationships, ties, leadership, motivations, intentions, finances, resources, composition, disposition, communications, and capabilities (not wholly inclusive). Each report also included the reliability of the human source of information so that individuals using the report could determine the reliability of the source of information.

f. TECHINT Reports

Technical intelligence (TECHINT) reports included in this study were derived from technical intelligence sources (NTM) and used to report information in response to command directed collection requirements. TECHNIT reports primarily provide information related to the network's activities, composition, disposition, communications, and capabilities (not wholly inclusive). TECHINT reports typically included analytic comments as a result of the difficulty in discerning intent from technical intelligence reporting.

g. Forensic Reports

Forensic reports used in this research provided information gathered, exploited and analyzed from attacks or recovered enemy weapons (bombs, IEDs, mortars, small arms, etc.) that provided specific forensic signatures (biometric, DNA, etc.) that tied specific attacks to dark networks. They typically included the date, time, and location of the attack or capture of enemy weapons, known tactics, techniques, and procedures (TTPs) of the enemy network, as well as any network members that were biometrically or genetically (DNA) tied to an attack. They also often included analytic comments to provide greater context of the exploited and analyzed materials identified in the report.

B. ANALYTIC METHODS

Many noteworthy and respected studies have conducted research on terrorist and insurgent groups (dark networks) using quantitative methods in order to better understand and predict organizational behavior. Many of the successful quantitative methods used include regression analysis (Everton and Cunningham[70]), structural equation modeling and path analysis (Friedkin[71]), as well as spatial, longitudinal, and relation analysis of dark networks (Krebs 2001; Bakker, Raab, Milward;[72] Everton and Cunningham[73]). Due to the numerous antecedent conditions and multivariate nature of my hypothesis, I selected a quantitative methods approach to test the magnitude and strength of direct and indirect relationships between my independent variables (HUMINT & NTM),

---

[70] Sean F. Everton and Dan Cunningham, "Terrorist Network Adaptation to a Changing Environment" in *Crime and Networks*, ed. Carlo Morselli (New York: Routledge, 2011), 287–308.

[71] N. E. Friedkin, "Social Networks in Structural Equation Models," *Social Psychology Quarterly* 53 (2001).

[72] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[73] Sean F. Everton and Dan Cunningham, "Terrorist Network Adaptation to a Changing Environment" in *Crime and Networks*, ed. Carlo Morselli (New York: Routledge, 2011), 287–308.

intervening variable (Network Adaptation: Spatial Degree Centralization), and dependent variable (Network Performance: Attacks Per Capita).

1. Analytic Methods Workflow

The purpose of this section is to summarize the workflow of analytic methods used to test my hypothesis (see data and methods diagram in Figure 6). It provides a summary of the spatiotemporal network analysis, social network analysis, and statistical analysis (multiple linear regression, structural equation modeling, and path analysis) methods used in this thesis.

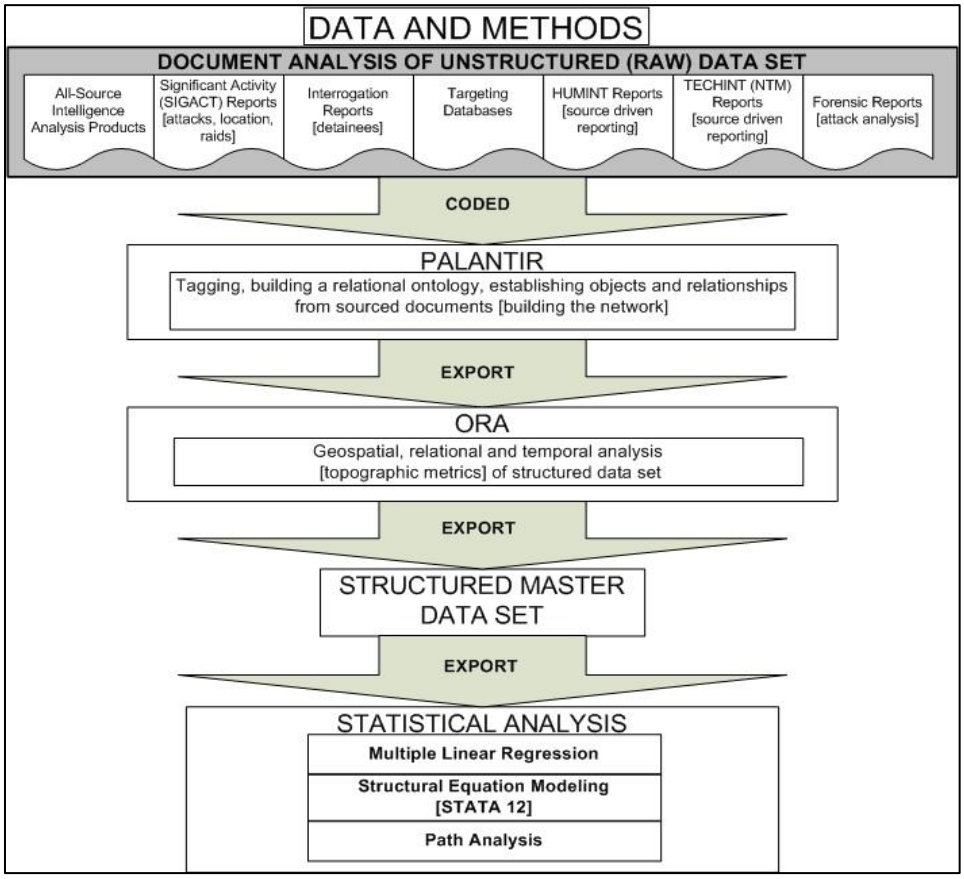


Figure 5. Data and Methods Diagram

a. Spatiotemporal Network Analysis in ORA

Following content analysis coding and export of structured network analysis data from Palantir,[74] the data were loaded into ORA[75] in order to analyze the network both longitudinally and geospatially (spatiotemporally) over a period of 27 months (1 month = 1 time period). Longitudinal analysis was selected examine and test changes in network resiliency, structure, and performance in response to security forces' modes of intelligence collection and targeting over time.

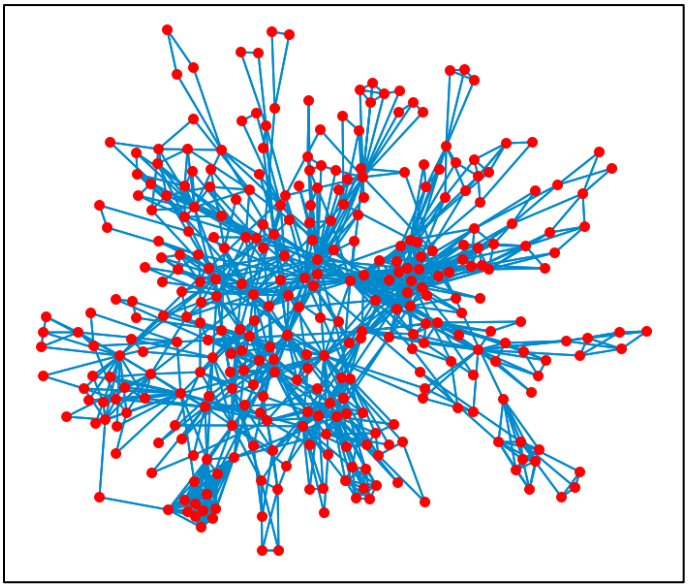


Figure 6. Network Diagram at Time Perod 1 of 27 (ORA).[76]

Recent studies in longitudinal network analysis on dark networks (Carley and McCulloh;[77] Bakker, Raab and Milward[78]) have proven effective in delivering

[74] Palantir Technologies Software, can be purchased for use from the Palantir government website: http://www.palantirtech.com/government.

[75] Kathleen M. Carley et al., *ORA User's Guide 2013* (technical report CMU-ISR-13-108) (Pittsburgh, PA: Carnegie Mellon University, 2013). ORA (Carley 2001-2011) can be downloaded for free for noncommercial use from the ORA website: http://www.casos.cs.cmu.edu/projects/ora/.

[76] Kathleen M. Carley et al., *ORA User's Guide 2013* (technical report CMU-ISR-13-108) (Pittsburgh, PA: Carnegie Mellon University, 2013).

relevant findings and insight in the detection of network change relating to exogenous and endogenous pressure (shock). The use of geospatial network analysis (multi-mode) was chosen as a result of anecdotal observations that the network leadership (N=40) were compelled to geographically disperse to avoid targeting and capture due to pressure exerted by security forces. Using the meta-matrix[79] technique within ORA, I conducted spatiotemporal network analysis of the observed network over 27 time periods. The resulting network topographic metrics produced by the spatiotemporal analysis in ORA provided 27 separate observations (time periods) of the network of the network that were included in the structured master data set of this study.

b. Network Topography

Network topography denotes the overall structure of the network and consists of topographical measures used in the analysis and observation of network change to endogenous and exogenous factors.[80] The measures of density (average degree) and centralization (spatial degree centralization) were used in order to measure the impact of the independent variables (modes of intelligence collection and targeting of the network) on the intervening variable (network adaptation to environmental pressure) in order to describe and track measures of network adaption over time.

---

[77] Ian McCulloh and Kathleen M. Carley. "Detecting Change in Longitudinal Social Networks," *Journal of Social Structure* 12 (2011): 1–37.

[78] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[79] Meta-Matrix technique: "The design structure of an organization is the relationship among its personnel, knowledge, resources, and tasks entities. These entities and relationships are represented by the Meta-Matrix. Measures that take as input a Meta-Matrix are used to analyze the structural properties of an organization for potential risk. Kathleen M. Carley et al., *ORA User's Guide 2013* (technical report CMU-ISR-13-108) (Pittsburgh, PA: Carnegie Mellon University, 2013), iii.

[80] Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2012), 403.

It is important to note that there are three significant limitations to network topography that can potentially skew results: incomplete information leading to missing nodes and links, fuzzy boundaries leading to the dilemma of who to include within analysis, and the dynamic and changing nature of dark networks. These factors make it impossible to achieve a resolute picture of the network at any one time.[81] In order to minimize the impact of these limitations, I ensured that the most up to date and inclusive data sets were used for my analysis and I employed a whole network perspective in mapping the network's structure and relationships.

(1) Spatial Degree Centralization. The network topographic metric of spatial degree centralization was selected to operationalize the intervening variable of my hypothesis. Previous research suggests that increased network centralization can serve to magnify the effect of exogenous pressure (shock) on a dark network, while more decentralized networks are more effectively structured to mitigate the impact of shock (Bakker, Raab and Milward;[82] Arquilla and Ronfeldt[83]). By using spatial degree centralization to measure the intervening variable (network adaptation to environmental pressure), the path analysis model will provide feedback on how network structure impacts network performance measured in the dependent variable (attacks per capita). Because the spatiotemporal network analysis conducted in ORA produced the metric spatial degree centrality scores for each of the network actors,[84] it was possible to calculate spatial degree centralization. For the purpose of this research, spatial

---

[81] Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks* 13 (1991): 251–274.

[82] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[83] John Arquilla and David Ronfeldt, "The Advent of Netwar," in *Networks and Netwars* (rev.), ed. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001), 1–25.

[84] The spatial equivalent of degree centrality, degree centrality is the count of the number of an actor's ties. Everton, *Disrupting Dark Networks,* 399.

degree centralization was calculated for the leadership network only (N=40; time period 1) using Wasseman and Faust's 1994 formula for degree centralization.[85]

(2) Average Degree. Average degree is defined as the average number of ties among all actors in the network.[86] It was used as a control variable in order to control for the size and density of the network as it changed in size over time. With the network changing in size from time period to time period, it was important to control for these potentially spurious effects.

2. Path Analysis

Path analysis is an extension of multiple regression analysis and is a prominent method of statistical analysis first developed by geneticist Sewall Wright in 1920. It is used to test the research hypothesis by examining the direct and indirect relationships between the dependent variable (response variable) and two or more independent variables (explanatory variables).[87] Path analysis was selected because of the multivariate complexity of the causal model. It also tests the magnitude and strength of the effect that each of the independent variables have on the Intervening the dependent variables. This analytic contribution allows the model to test the comparative strength of both modes of intelligence collection and targeting in relation to the resilience and performance of the network, which is central to my hypothesis. Path analysis also provides the capacity to test direct relationships between variables, control for indirect effects (control variables), and decompose effects between variables over time. Limitations and weaknesses of path analysis include recursivity and

---

[85] Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications* (Cambridge: Cambridge University Press, 1994), 176.

[86] Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2012), 397.

[87] Christy Lleras, "Path Analysis," in *The Encyclopedia of Social Measurement* (New York: Academic Press, 2005), 25.

unidirectional causal flow, which limits causality of the model in one direction and limits the model to correlations instead of proving causation.[88]

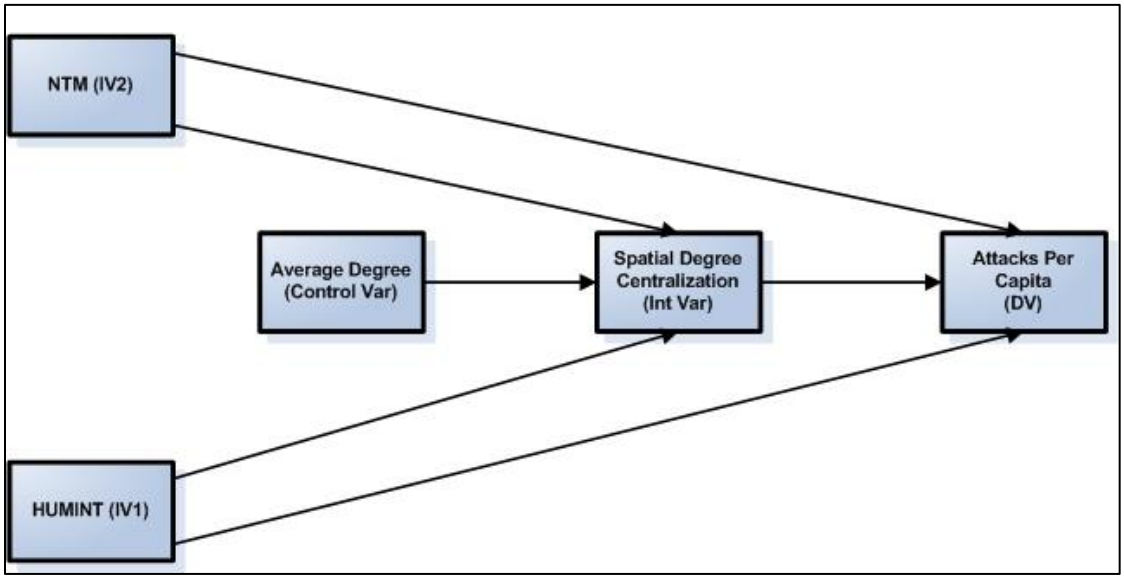


Figure 7. Path Analysis Model and Variables

In addition to the intervening (spatial degree centralization) and control variable (average degree) defined earlier in this section, the path analysis also defined the two independent variables as the security forces modes of intelligence collection and targeting (HUMINT-IV1 and NTM-IV2). In order to control for the delayed effect that each mode of intelligence collection and targeting has on the intervening and dependent variables, a lag of one month (1 time period = 1 month) was calculated for both independent variables. As a result of the calculated one-month lag, the overall observations were reduced from 27 to 26 time periods. Additionally, research on dark network communications (Drozdova and Samoilov 2010) also demonstrates that the use of high-tech communications increases the networks vulnerability to endogenous pressure (shock) and compels dark networks to decentralize and minimize its traceability

[88] Christy Lleras, "Path Analysis," in *The Encyclopedia of Social Measurement* (New York: Academic Press, 2005), 29.

in order to limit network damage and provide time and space for recovery.[89] Because of this research and specific anecdotal evidence identifying intelligence gaps during the targeting of the observed network, the independent variable 2 (national technical means-IV-2) was formulated with a decomposition effect by taking the total number of NTM interdictions during a given time period divided by the time period (minus 1 month lag) in which the interdiction occurred in order to account for the decomposition path effect over time.

In order to provide a more sophisticated measure of network performance than simple interdictions of the network, the dependent variable was defined to account for the network's performance in relation to security forces' mode of intelligence collection and targeting. The dependent variable (attacks per capita) was defined as the total number of attacks divided by the total number of free network members during the given time period. The structural equation modeling (SEM) function within the statistical software program STATA 12[90] was used to conduct the path analysis and test the stated hypothesis.

[89] Katya Drozdova and Michael S. Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory 16* (2010): 66, DOI: 10.1007/s10588-009-9058-2.

[90] Stata Corp. *Stata Statistical Software: Release 12* (College Station, TX: Stata Corp LP, 2011).

IV. RESULTS AND FINDINGS

The final path diagram model (see Figure 8) is virtually unchanged from the original hypothesis in Chapter II. The two independent variables, HUMINT and NTM, the intervening variable, spatial degree centralization, and the control variable, average degree, are unchanged. The dependent variable has been modified from the initial model, which used the raw count of interdictions in relation to the security forces' mode(s) of targeting. The final model uses a more nuanced metric of network performance: attacks per capita (DV).

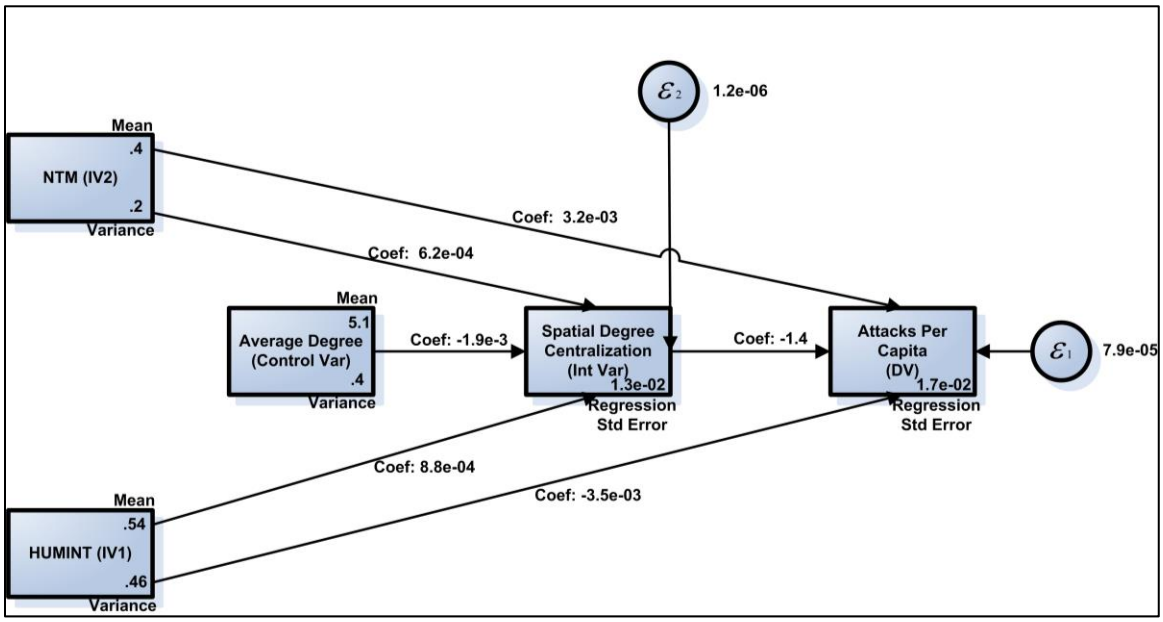


Figure 8. Path Analysis Diagram with Statistics

Figure 8 provides a diagram of the path analysis model with regression output of significant paths. Table 1 provides a tabular summary of the same results. The independent and control variables include inset statistics that indicate the variable's mean and variance over time. The causal flow of each of the paths and the standard error is for both spatial degree centralization (Int Var) and attacks per capita (DV). We consider each of these coefficients in turn.

The negative path coefficient from average degree on spatial degree centralization of -0.0019 (p-value = 0.00) indicates that average degree is inversely associated with spatial degree centralization. This result is consistent with Carter Butt's 2004 finding that degree centralization is a function of average degree[91] and reinforces the rationale to control for average degree.

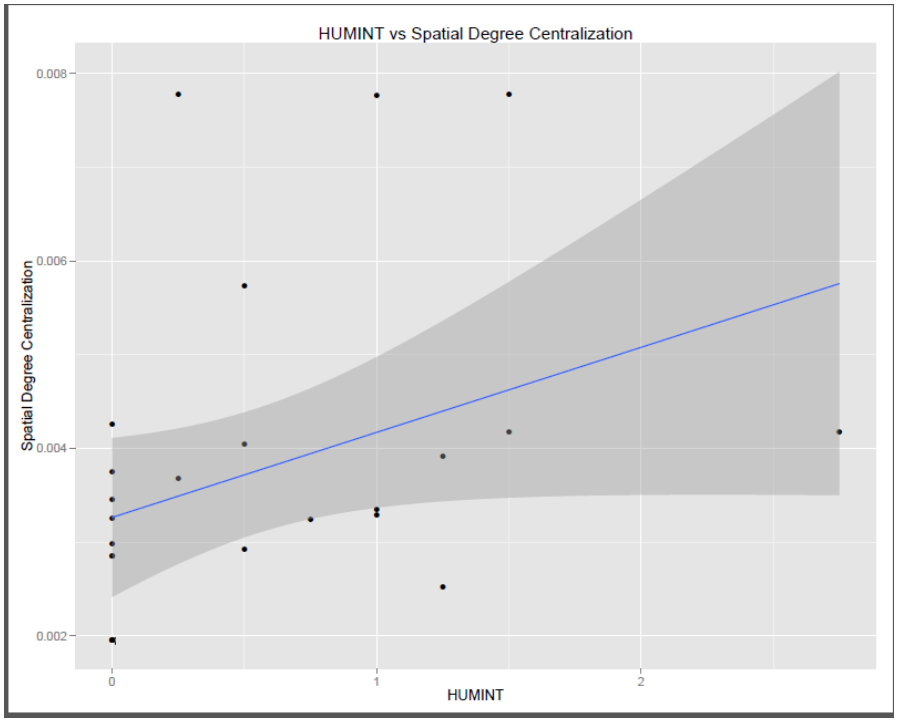


Figure 9. Scatter Plot: HUMINT versus Spatial Degree Centralization

The positive HUMINT coefficient of 0.00088 (p-value = 0.034) on spatial degree centralization indicates that HUMINT Intelligence collection and targeting increases the network's spatial degree centralization. In other words, as HUMINT increases, so does spatial degree centralization (see Figure 9), and as we will see below, an increase in spatial degree centralization led to a decline in the network's performance (as measured by attacks per capita—see Figure 10). This

[91] Carter T Butts, "Exact Bounds for Degree Centralization," *Social Network* 10 (2006): 283–296, DOI:10.1016/j.socnet.2005.07.003

result is consistent with previous research, which has found that an increase in network centralization can have a deleterious impact on performance (Bakker, Raab and Milward[92]). Furthermore, although the path coefficient (-0.0035) from HUMINT on attacks per capita is not statistically significant (p-value = 0.320), it is negative. And since the lack of statistical significance probably reflects the small number of observations,[93] the negative coefficient suggests that HUMINT may have also directly contributed to a reduction in the network's performance. Taken together these results suggest that HUMINT intelligence collection and targeting is vital to development of a security forces' counterterrorism collection and targeting plan.

Unexpectedly, NTM had a positive effect on attacks per capita (coefficient of 0.0032 with a p-value of 0.531), which suggests that NTM may have led to an increase the network's performance, which was not the desired result. On the positive side, NTM, like HUMINT, had a positive effect (0.00062 with a p-value of 0.367) on spatial degree centralization, which as noted above, led to a decrease in network performance. To be sure, both effects are statistically insignificant, but additional tests suggest that NTM's effect on spatial degree centralization is nevertheless genuine.[94] Finally, as noted above, spatial degree centralization had a large and negative effect (-1.37 with a p-value of 0.220) on attacks per capita. This relationship is captured graphically in Figure 10. Here again, the effect is statistically insignificant (0.220), but additional tests suggest that it is genuine.[95] This finding corresponds with Arquilla and Ronfeldt's theory on flatter networks (lower centralization score) being more capable of achieving greater

---

[92] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience." *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[93] Statistical significance is, in part, a function of sample size. As sample size increases, the threshold for obtaining statistical significance decreases. Indeed, the same results with a tenfold increase in the number of observations (i.e., 260) produced statistically significant effects for all path coefficients except NTM's effect on attacks per capita.

[94] See footnote 2.

[95] See footnote 2.

operational success as discussed in the literature review.[96] Table 1 provides additional detail on the multivariate statistics produced from the path analysis for this study and includes the path coefficients, P-values and standard errors for both the explanatory and response variables for each of the regressions conducted for this analysis (see Table 1).

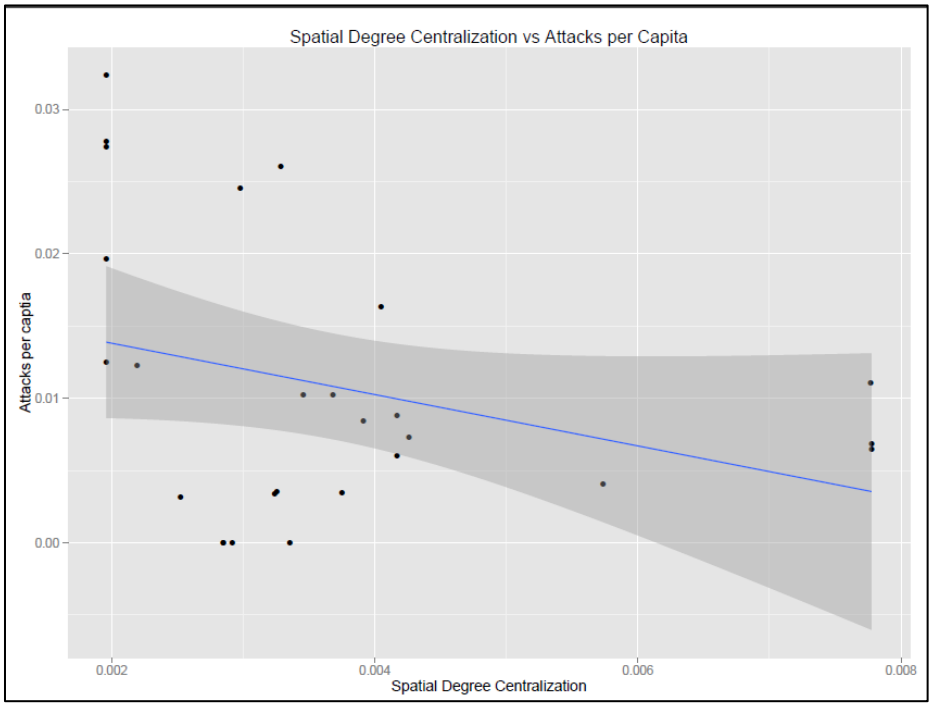


Figure 10. Scatter Plot: Spatial Degree Centralization versus Attacks Per Capita

[96] John Arquilla and David Ronfeldt, "The Advent of Netwar," in *Networks and Netwars* (rev.), ed. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001), 1–25.

Table 1. Path Analysis Statistics

Path Analysis: (N=26)

Structural Model	Spatial Degree Centralization	
Variables	Coefficient	P-Value
Average Degree (Ctrl Var) -> Spatial Degree Centralization	-0.0019 (0.00038)	0.000
NTM (IV-1) [Lag1] -> Spatial Degree Centralization	0.00062 (0.00069)	0.367
HUMINT (IV-2) [Lag1+decay] -> Spatial Degree Centralization	0.00088 (0.000418)	0.034
Constant -> Spatial Degree Centralization	0.013 (0.0019)	0.000
HUMINT (IV-1) [Lag1] -> Attacks per Capita	-0.0035 (0.0036)	0.320
NTM (IV-2) [Lag1+decay] -> Attacks per Capita	0.0032 (0.0051)	0.531
Spatial Degree Centralization -> Attacks per Capita	-1.370 (1.120)	0.220
Constant -> Attacks per Capita	0.0165 (0.0045)	0.000
Error on Spatial Degree Centralization	0.00000125 (3.46E-7)	
Error on Attacks per Capita	0.0000789 (2.19E-5)	

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS, IMPLICATIONS AND POLICY RECOMMENDATIONS

A. CONCLUSIONS

Over the last 30 years, the world has witnessed some of the most sophisticated, OPSEC savvy, and well trained terrorist organizations conduct spectacular attacks on Western interests both domestically and abroad. Not only have they conducted these attacks with near impunity, but they have also evaded the consequences of their actions for decades. Men like Osama bin Laden, the 19 al-Qaeda operatives who perpetrated the 9/11 attacks, and the military leader of Hezbollah, Imad Mughniyeh, all understood and adapted to the counterterrorism capabilities of their state adversaries. These men recognized their vulnerabilities to high-tech intelligence collection and targeting and modified their actions and communications to low-signature and low-tech communications in order to evade detection and capture. In the cases of Osama bin Laden and Imad Mughniyeh, they effectively evaded capture for more than a decade before being killed.

Anecdotal evidence suggests that an institutionalized organizational bias exists within the U.S. military intelligence community towards a reliance on national technical means (NTM) intelligence collection and targeting for counterterrorism operations. NTM has become the quick fix for military leaders who prioritize the preponderance of their intelligence collection plans on NTM derived intelligence. The recent advent of cyber security units and new cyber occupational specialties indicates that bias will likely only get worse in the coming decades unless commanders and intelligence consumers better understand the adaptability and resilience of dark networks. Western nations must understand and adapt to the strategic interaction between a dark network's mode(s) of communication and their own security forces' mode of intelligence collection and targeting. This genesis of this study grew out of recognition that an institutional bias towards NTM exists and that commanders and intelligence consumers must

become better educated on the efficacy of each mode of intelligence and targeting in order to more effectively target sophisticated and highly adaptable dark networks.

This study's findings uncovered an association between the mode of human intelligence and targeting and the centralization of the observed dark network. It confirmed previous research, which argued that highly centralized dark networks are more fault intolerant and become increasingly susceptible to collapse (Bakker, Raab and Milward;[97] Arquilla and Ronfeldt[98]) when exposed to exogenous pressure (shock). Another critical finding was that HUMINT intelligence and targeting has an effect on reducing a dark network's performance as measured by the number of attacks per capita. The combination of these two findings indicates that HUMINT collection and targeting can be effective in increasing the vulnerability (increased centralization) and reducing the performance (attacks) of dark networks.

B. IMPLICATIONS AND POLICY RECOMMENDATIONS

The implications are clear. The more Western nations skew their intelligence collection and targeting plans towards a heavy reliance on national technical means intelligence, the more that sophisticated dark networks will rely on low-tech communications and low signature activities to conduct their attacks and evade capture. As long as commander's and intelligence consumers continue to play lip service to all-source intelligence and ignore the efficacy of HUMINT in counterterrorism operations, the more likely they will experience intelligence gaps and lulls in targeting of dark networks.

So how can counterterrorism forces increase the expected utility of intelligence collection towards the targeting and interdiction of dark networks?

---

[97] René M Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (2012): 33–62.

[98] John Arquilla and David Ronfeldt, "The Advent of Netwar," in *Networks and Netwars* (rev.), ed. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001), 1–25.

The recommendations are simple. Commanders must integrate HUMINT into balanced all-source intelligence collection plans. Because HUMINT requires time to develop and cannot be quickly diverted or created where an intelligence gap exists, commander's must identify terrorist threats early (left of the line, phase zero) and develop HUMINT intelligence operations before conflicts or counterterrorism campaigns are necessary. Unquestionably, commanders must place an early and persistent emphasis on HUMINT source operations in order to successfully wage long-term counterterrorism operations against dark networks.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX STRUCTURED MASTER DATA SET

Time Period	Nodes Leader	Total Network Count	HUMINT + Lag 1 +Decay (IV1)	NTM + Lag 1 + Decay (IV2)	Attacks Per Capita (DV)	Spatial Degree Centralization (IV)	HUMINT Interdictions	NTM Interdictions	NTM + HUMINT Combined	Average Degree (Cont Var)	IEDs Attacks	Mortars Attacks
1	40	409			0.0122249	0.002194197	0	0	0	5.75	5	0
2	40	408	0	0	0.0245098	0.002977058	0	1	0	5.75	10	0
3	40	407	0	0.3333333	0.019656	0.001959514	0	1	0	5.75	7	1
4	40	402	0	0.25	0.0323383	0.001959514	0	2	0	5.75	13	0
5	40	402	0	0.4	0.0273632	0.001959514	0	0	0	5.75	7	4
6	40	401	0	0	0.0124688	0.001959514	0	1	0	5.75	5	0
7	40	396	0	0.1428571	0.0277778	0.001959514	1	4	1	5.75	9	2
8	39	384	1	0.5	0.0260417	0.003285846	0	12	0	5.7948718	10	0
9	36	367	0.5	1.333333	0.0163488	0.004048403	1	17	1	5.5555556	6	0
10	34	355	1.25	1.7	0.0084507	0.003914489	1	12	1	5.5294118	3	0
11	31	342	1.5	1.090909	0.0087719	0.004170345	2	11	0	5.6774194	3	0
12	31	332	2.75	0.9166667	0.0060241	0.004170345	0	10	0	5.6774194	2	0
13	31	321	1.25	0.7692308	0.0031153	0.002524368	0	11	0	5.6774194	1	0
14	30	315	0.5	0.7857143	0	0.002917488	0	6	0	5.5333333	0	0
15	29	308	0.25	0.4	0.0064935	0.007775765	1	7	1	4.7586207	2	0
16	30	298	1	0.4375	0	0.003353448	1	9	0	5	0	0
17	30	294	1.5	0.5294118	0.0068027	0.007775862	0	4	0	5	2	0
18	29	294	0.75	0.2222222	0.0034014	0.00323836	0	0	0	4.7586207	1	0
19	29	293	0.25	0	0.0102389	0.003681054	1	0	0	4.7586207	2	1
20	28	293	0	0	0.003413	0.003749846	0	0	0	4.8571429	1	0
21	28	293	0	0	0.0102389	0.00345755	0	0	0	4.8571429	3	0
22	28	286	0	0	0.0034965	0.003255231	0	1	0	4.8571429	0	1
23	28	286	0	0.0434783	0	0.002847151	0	0	0	4.8571429	0	0
24	28	280	0	0	0	0.002847293	0	6	0	4.8571429	0	0
25	26	274	0	0.24	0.0072993	0.004261167	1	5	0	3.9230769	2	0
26	25	272	1	0.1923077	0.0110294	0.007767391	0	2	0	3.84	0	3
27	24	247	0.5	0.0740741	0.0040486	0.005735771	0	25	0	3.5833333	0	1

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arquilla, John and David F. Ronfeldt. *Swarming & the Future of Conflict*. Santa Monica, CA: RAND. 2000.

Arquilla, John and David F. Ronfeldt. "The Advent of Netwar." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt (rev), 1–25. Santa Monica, CA: RAND. 2001.

Arreguín-Toft, Ivan. *How the Weak Win Wars: A Theory of Asymmetric Conflict.* Cambridge, UK: Cambridge University Press, 2005.

Bakker, René M, Jörg Raab, and H. Brinton Milward. "A Preliminary Theory of Dark Network Resilience." *Journal of Policy Analysis and Management* 31, no.1 (2012):33–62.

Bamford, Bradley W. C. "The Role and Effectiveness of Intelligence in Northern Ireland," *Intelligence & National Security* 20, no. 4 (2005): 581–607, DOI:10.1080/02684520500425273

Bamford, James. *The Spy Factory* [Television]. Directed by Scott Willis. Boston; NOVA/The Public Broadcasting System. 2009. http://www.pbs.org/wgbh/nova/spyfactory/credits.html

Bergen, Peter L. *Manhunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*. New York: Crown Publishing Group, 2012. Kindle Edition.

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

Bowen, Glenn. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal* 9, no. 2 (2009): 27–40.

Bruce, James B. and Roger Z. George. *Analyzing Intelligence: Origins, Obstacles and Innovations*. Washington, DC: Georgetown University Press, 2008.

Butler, Michael. "Killing Cells: Retooling Human Intelligence Collection for Global Decentralized Terrorism." Presented at ISA's 50th Annual Convention. New York, February 2009. http://www.allacademic.com/meta/p310663_index.html

Butts, Carter T. "Exact Bounds for Degree Centralization." *Social Networks* 10 (2006): 283–296. DOI:10.1016/j.socnet.2005.07.003

Carley, Kathleen M., Jürgen Pfeffer, Jeffrey Reminga, Jon Storrick, and Dave Columbus. *ORA User's Guide 2013* (Technical Report CMU-ISR-13-108). Pittsburgh, PA: Carnegie Mellon University, 2013.

de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek*, 2nd ed. Cambridge: Cambridge University Press, 2011.

Drozdova, Katya. *Analyzing Terrorist Communications: Detecting Early Signals of Attack*. Stanford, CA: Hoover Institute on War, Revolution, and Peace, 2009.

Echevarria, Antulio Joseph. *Fourth-Generation War and Other Myths* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College. 2005.

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

Everton, Sean F. and Dan Cunningham. "Terrorist Network Adaptation to a Changing Environment" in *Crime and Networks*, edited by Carlo Morselli. 287–308. New York: Routledge.2011.

Fantz, Ashley. "Chinese Hackers Infiltrated U.S. Companies, Attorney General Says," CNN. May 19, 2014. http://m.cnn.com/primary/wk_article?articleId=cnn/2014/05/19/justice/china-hacking-charges&branding=&category=cnnd_latest&pagesize=10

Federal Bureau of Investigation. *Report: The 11 September Hijacker Cell Model*. 2003. http://911workinggroup.org/FBI_FOIA.html.

Friedkin, N. E. 1990. "Social Networks in Structural Equation Models." *Social Psychology Quarterly* 53 (2001).

Gelernter, Judith & Carley, Kathleen M. "Spatiotemporal Network Analysis and Visualization." *International Journal of Applied Geospatial Research*, Special Issue. 2011. 1–25.

Gough, Stephen and William Scott. "Exploring the Purposes of Qualitative Data Coding in Educational Enquiry: Insights from recent research," *Educational Studies* 26, no.3 (2000): 339–354. DOI: 10.1080/0305569005013714.

Jackson, Brian A, Peter Chalk, R. Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple. *Breaching the Fortress Wall Understanding Terrorist Efforts to Overcome Defensive Technologies*. Santa Monica, CA: Rand Corporation, 2007.

DeVore, Howard O. *Jane's Special Report: China's Intelligence & Internal Security Forces*. Alexandria, VA: Jane's Information Group.

Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02). Washington, DC: Joint Chiefs of Staff, 1999, amended through 2009.

Joint Chiefs of Staff, Department of Defense. *Joint Interdiction* (Joint Publication 3-03). Washington, DC: Department of Defense, 2011.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, Brian Michael Jenkins. "Networks, Netwar, and Information-Age Terrorism," in *Countering the New Terrorism*, edited by John Arquilla, David Ronfeldt, and Michele Zanini. 39–81. Santa Monica, CA: Rand Corporation, 1999.

Lleras, Christy. "Path Analysis." In *The Encyclopedia of Social Measurement*. New York: Academic Press, 2005.

Lusthaus, Charles. *Organizational Assessment: A Framework for Improving Performance*. Ottawa: International Development Research Centre. 2002.

Mandiant. *APT1 Exposing One of China's Cyber Espionage Units.* Alexandria, VA: Mandiant. 2013.

McCulloh, Ian & Kathleen M. Carley. "Detecting Change in Longitudinal Social Networks." *Journal of Social Structure* 12 (2011): 1–37.

Milward, H. B. and Jörg Raab. "Dark Networks as Organizational Problems," *International Public Management Journal* 9, no. 3 (2006). 333–360.

O'Hern, Steven K. *The Intelligence Wars: Lessons from Baghdad.* Amherst, NY: Prometheus Books, 2008.

Perez, Evan. "More than 90 People Nabbed in Global Hacker Crackdown." CNN. May 19, 2014. http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/

Robb, John. *Brave New War, The Next Stage of Terrorism and the End of Globalization.* Hoboken, NJ: John Wiley and Sons Inc., 2007.

Sims, Jennifer. "Intelligence to Counter Terror: The Importance of All-Source Fusion." *Intelligence and National Security*, 22, no. 1 (2007): 38–56.

Sparrow, Malcolm K. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks*.13, no. 3 (1991): 251–274. DOI: 10.1016/0378-8733(91)90008-H

Stata Corp. *Stata Statistical Software: Release 12*. College Station, TX: Stata Corp LP. 2011.

Von Neumann, John, and Oskar Morgenstern. *Theory of Games and Economic Behavior.* Princeton, NJ: Princeton University Press, 2007.

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

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California