How Terrorist Groups Survive: A Dynamic Network Analysis Approach to the Resilience of Terrorist Organizations

A Monograph
by
Major Glenn A. Henke
U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2008-09

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
21-05-2009	Monograph	JUL 2008 – MAY 2009

4. TITLE AND SUBTITLE
How Terrorist Groups Survive: A Dynamic Network Analysis Approach to the Resilience of Terrorist Organizations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Glenn A. Henke

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth, KS 66027

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
100 Stimson
Fort Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC, SAMS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See Abstract.

15. SUBJECT TERMS
Terrorism, Counterterrorist Operations, Dynamic Network Analysis, Radicalization

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			COL Stefan Banach
(U)	(U)	(U)	(U)		**19b. PHONE NUMBER** *(include area code)* 913-758-3300

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJ Glenn A. Henke

Title of Monograph: How Terrorist Groups Survive: A Dynamic Network Analysis Approach to the Resilience of Terrorist Organizations

This monograph was defended by the degree candidate on 19 March 2009 and approved by the monograph director and reader named below.

Approved by:

_____ Daniel G. Cox, Ph.D.	Monograph Director
_____ Christof Schaefer, COL, German Army	Monograph Reader
_____ Stefan J. Banach, COL, IN	Director, School of Advanced Military Studies
_____ Robert F. Baumann, Ph.D.	Director, Graduate Degree Programs

Abstract

How Terrorist Groups Survive: A Dynamic Network Analysis Approach to the Resilience of Terrorist Organizations, by MAJ Glenn A. Henke, U.S. Army, 59 pages.

The purpose of this paper is to explore the question of how modern terrorist groups manage to survive in the face of aggressive counterterrorist operations by security forces. Al Qa'ida survives to this day, despite the destruction of their Afghanistan sanctuary, the loss of countless key personnel, and continuous pressure by the United States and their allies. Why has al Qa'ida survived? Since much of the literature on terrorism focuses on how to eliminate them, this research paper focuses on why they still endure. In other words, instead of asking, "How do we kill them," this research asks, "Why don't they die?"

This research employs a dynamic network analysis approach to explore the primary research question of terrorist survival. This analysis combines aspects of traditional social network analysis with a new multi-agent model that describes how terrorist groups raise agents through the organization to positions of prominence. The key to this process is the radicalization of members based on time, connectivity, and belief intensity. The testing dataset comes from the 1998 Tanzania Embassy bombing, expressed in the form of a meta-network.

After four testing program iterations, the author concludes that terrorist organizational survival is based on the internal dynamics of leader selection and growth within the group as new members advance. These findings imply a number of recommendations for counterterrorist operations and intelligence activities in order to disrupt the growth and development of new leaders. Additionally, these results imply that current Joint and Army doctrine on network analysis insufficiently addresses the dynamic processes that network diagrams are intended to depict. American military counterinsurgency and counterterrorist operations can be greatly enhanced by moving from a network analysis approach based on structure to one based on dynamics.

TABLE OF CONTENTS

INTRODUCTION

How do terrorist groups survive? This question may seem to be simply the inverse of asking how to kill a terrorist organization. Further examination demonstrates that while this is technically correct, approaching the problem from the perspective of the terrorists themselves should yield considerable insight into their enduring presence. Despite this, there is surprisingly little literature that asks this seemingly obvious question and almost no attempts to systematically study the inverse of the question that most researchers and practitioners ask. Ironically, examining and understanding how terrorist groups survive might shed more light on strategies and tactics to marginalize or destroy terror groups. Therefore, the purpose of this monograph is to provide insight into the question of how terrorist groups survive by analyzing them at the middle range, the level of analysis that focuses on the processes of how terrorists act in groups.[1]

Using social and dynamic network analysis, this monograph demonstrates how terrorist groups survive in the face of continued attrition by counterterrorist forces. The vehicle for this analysis is an original multi-agent model that provides an academic operationalization of the radicalization process based on the interplay of beliefs, time, and network connectedness. The output of this radicalization process is a numeric radicalization index which is then used to determine an agent's suitability for further advancement in the organization.

Upon completion of multiple testing iterations, the author concludes that terrorist groups survive through an agent-based decision making process that determines how and when agents are linked to each other. Central to this process is the agent's belief intensity, which is the seed of radicalization. This process also provides numerous opportunities for counterterrorist forces to exploit a terrorist organization's weakness at critical junctures based on losses of critical nodes. This model also provides a potential explanation for the dynamics of splinter or spin-out terrorist groups.

[1] Marc Sageman, *Leaderless Jihad: Terror Networks in the 21st Century*, (Philadelphia: University of Pennsylvania Press, 2008): 23.

The research also calls into question current doctrinal network analysis and non-doctrinal publications on network analysis. Current joint and Army doctrine use middle-range analysis to model enemy networks and systems. The U.S. Army and Marine Corps counterinsurgency manual contains an appendix on applying network analysis for studying insurgent groups.[2] Joint doctrine also provides an overview of network analysis.[3] Unfortunately, these examples are almost exclusively concerned with the structure of networks and not the dynamics of the networks. Instead of describing the nature and dynamics of the interactions, they focus on targeting specific nodes or sets of nodes for destruction in order to cripple the enemy network. The doctrine is not restricted to analyzing the social networks, but instead utilizes the PMESII construct to organize the network. Before the commander of U.S. Joint Forces Command disavowed Operational Net Assessment and System-of-Systems Analysis in his 14 August 2008 memorandum on Effects Based Operations (EBO), official non-doctrinal publications on EBO utilized a system of network analysis that failed to account for dynamics by focusing on the placement and connectivity of nodes. Although discredited by General Mattis, ONA and SOSA advocates have vigorously defended their methodology in numerous publications. The research presented in this monograph provides additional support to the JFCOM commander's critique of these methodologies. Additionally, this research demonstrates that current joint doctrine fails to meet its full potential due the failure to focus on dynamics.

The present monograph is organized into six main sections. The first section is a review of relevant literature on terror network disruption, with particular emphasis on social and dynamic network scholarship. The second section, the theory section, provides a theoretical background on social and dynamic network theory applicable to this research question and proposes a testable hypothesis. The next section develops the multi-agent model in detail and describes the basic testing regimen. The analysis section then discusses the experimentation results and describes general trends. Closely linked to the

[2] Field Manual 3-24, *Counterinsurgency*, (Washington, DC: Government Printing Office, 2006), B-10.

[3] Joint Publication 5-0, *Joint Operation Planning* (Washington, DC: Government Printing Office, 2006), III-18.

analysis section is the future research section, which is designed to describe further research programs based on the principles described in the theory and modeling sections. The monograph ends with a conclusion and series of recommendations for real-world counterterrorist operations, based on the findings of the research testing.

LITERATURE REVIEW

In the past decade, researchers from numerous disciplines have expended considerable energy on answering the question of how to destroy a terrorist network. This research includes the efficacy of undermining terrorist groups by understanding their origins, analyzing religious and social doctrine motivating terrorists (Islamic terrorism in particular), as well as research into the dynamics of terrorist groups, to name a few. However, much of this research has failed to look at the inverse of this question, which is why do terrorist groups survive? In light of the policy implications of such a question, focused research on what causes a terrorist group to survive could provide important insights for counterterrorism officials. This research attempts to analyze the mechanics of terrorist group survival using social network analysis in order to penetrate one specific aspect of this question.

Network science has gained considerable interest since the late 1990s due to the broad applicability of these analytical tools on a wide range of scientific disciplines. While a number of popular books on the subjects are currently in print, the two best general overviews are *Linked* by Albert-Lásló Barabási, and *Six Degrees* by Duncan J. Watts. Barabási is best known for his co-discovery of scale-free networks that obey connectivity power laws by proving that both the World Wide Web and Internet are scale-free networks.[4] Watts and co-researcher Steven Strogatz developed mathematical models for small-world networks, familiar to most modern readers as the "six degrees of separation" phenomenon discovered by Stanley Milgram in the 1960's.[5] Both of these works discuss the applicability of this research to all manner of scientific fields, to include terrorism research. For the more mathematically-inclined readers interested in the specific statistical mechanics of small-world and scale-free networks,

[4] Albert-Lásló Barabási, *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*, (New York: Plume, 2003), 34. Despite the popular use of the word "Internet" as shorthand for the World Wide Web (and vice versa), they are separate entities. The Internet describes the physical information network of routers and connections that enables applications such as the World Wide Web, which is an virtual network based on the topology of pages.

[5] Duncan J. Watts, *Six Degrees: The Science of a Connected Age*, (New York: W.W. Norton and Co., 2003), 133. Watts points out in his work that Milgram's research did not decisively prove the six degrees property, which Watts and researchers subsequently proved in 2003.

comprehensive papers by Albert and Barabási (2002),[6] and Newman (2003),[7] are the standard texts. Although these two works do not address terrorism specifically, the mathematical techniques described are applicable to terrorist network analysis.

At approximately the same time that physicists and mathematicians began making new discoveries about networks, terrorism research also gained renewed interest. Since the terrorist attacks of September 11, 2001, network researchers have poured tremendous energy into applying their science to the question of terrorism. However, some research on terrorist networks in general and al Qa'ida in particular were published before the 9/11 attacks. Arquilla, Ronfeldt, and Zanini (1999) called the African embassy attacks by al Qa'ida "the opening shots of a war between a leading state and a terror network,"[8] a work widely considered to be the first dedicated analysis of information age terrorism. The authors also discussed the distributed nature of modern terrorist networks as well as the policy implications of these networks. Sageman extended the application of network science to terrorism in 2004 by applying small-world network theory to al Qa'ida as it existed prior to 9/11. Using open-source biographies of al Qa'ida operatives, Sageman constructed a small-world network of four geographically based terrorist clusters constituting the greater al Qa'ida network. Najara and Anderson at Cambridge University (2005) synthesized much of the existing research on network science and applied it to covert networks by using a game theoretic approach that concluded the best network structure in terms of resilience and robustness in the aftermath of attacks are cellular structures with small-world network properties.[9] Ressler provides an

[6] Réka Albert and Albert-Lásló Barabási, "Statistical Mechanics of Complex Networks," *Reviews of Modern Physics*. Vol. 74 (January 2002): 47-97.

[7] M. E. J. Newman, "The Structure and Function of Complex Networks," *SIAM Review*, Vol. 45, No. 2 (June 2003), 167-256.

[8] John Arquilla, David Ronfeldt, and Michell Zanini, "Networks, Netwar, and Information Age Terrorism" in *Countering the New Terrorism*, Ian O. Lesser et al. (eds), (Santa Monica, CA: RAND Corporation, 1999), 39.

[9] Shishir Nagaraja and Ross Anderson, "The Topology of Covert Conflict," *University of Cambridge Computer Laboratory Technical Report*. No. 637 (July 2005), 14.

article-length literature review of social network analysis and terrorist networks, which should serve as a starting point for any reader new to the field.[10]

For research on the mechanics of disrupting terrorist networks, the single best resource is the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University, administered by Dr. Kathleen Carley. Carley and the CASOS researchers have published scores of papers on this subject, as well as research on bio-terrorism mechanics and the command and control implications of network science. Two particular CASOS papers are significant for terrorism network research in general and this current work in particular. Carley (2002) proposed that terrorist networks are much more than simple social networks; they also include knowledge networks, task networks, and resource networks.[11] This expands counterterrorism science beyond analyzing social network ties, enabling a comprehensive look at the entire network that includes financial and expertise networks. This work also discussed some specific techniques to inhibit adaptation, which Carley and other CASOS researchers expanded in subsequent works to develop general destabilization strategies.[12]

Although few works have discussed how terrorist networks survive in light of attacks by security forces, a number of works have addressed this issue with theoretical networks. Much of this work leverages existing research on information networks that routinely suffer router failures but manage to sustain functionality. Albert, Jeong, and Barabási (2000) published the paper on attack tolerance of complex networks that serves as the basis for most research on scale-free and small-world network attacks. They discovered that scale-free networks can sustain a much higher level of random node

[10] Steve Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs*, Vol. 2, No. 2 (July, 2006), 1-10.

[11] Kathleen M. Carley, "Inhibiting Adaptation," *Proceedings of the 2002 Command and Control Research and Technology Symposium*, (Monterrey, CA: Naval Post Graduate School, 2002), 1.

[12] Kathleen M. Carley, Jeffrey Reminga, and Natasha Kamneva, "Destabilizing Terrorist Networks," *Proceedings of the 8th International Command and Control Research and Technology Symposium*, (Washington DC: National Defense War College, 2003), 4.

removals, but that the networks quickly degrade when the most connected nodes or hubs are removed.[13] Later research quantified this destruction figure at 15% of the most connected nodes to cause network collapse while remaining efficient despite the loss of 80% of nodes in undirected attacks.[14] The implications of this research for terrorism studies is that random removal of agents can continue almost indefinitely as long as the most connected agents survive. Tsvetovat and Carley (2003) addressed this implication directly in their discussion of how terrorist networks recover in light of attacks since they still have the ability to enlist new nodes and can sustain "transactive" memory, such as training manuals or databases. [15] This finding is another key concept for this work. Additional research has also proposed the existence of "ultra-robust" networks that simultaneously minimize failures due to task overload (congestion) and failures due to the destruction of other portions of the network.[16] This same paper also concludes that only minor changes in a network structure are required to achieve "ultra-robustness," a somewhat dispiriting finding for counterterrorism officials.

Although no specific terrorist research has concerned itself with the question of why a terrorist group survives, RAND Corporation researchers have recently come the closest to answering this question by asking how terrorist groups end, if they end at all. In their 2008 monograph, Jones and Libicki discovered that of all terrorist groups that ended since 1968, 43% ended their existence by entering politics and police forces defeated 40% of the groups. Military force destroyed only 7%, and 10% of the groups ended their existence by achieving victory.[17] Despite the fact that they do not directly address why groups survive since their time scale extends to the present and therefore biases the sample against groups

[13] Réka Albert, Hawoong Jeong, and Albert-Lásló Barabási, "Error and Attack Tolerance of Complex Networks," *Nature* 406, No. 6794 (July 27, 2000), 380.

[14] Paolo Crucitti, et al, "Error Tolerance of Complex Networks." *Physica A*, No. 340, (2004), 391.

[15] Maksim Tsvetovat and Kathleen M. Carley, "Bouncing Back: Recovery Mechanisms of Covert Networks," *Proceedings of the 2003 North American Association of Computational Social and Organization Science*, Kathleen. M. Carley (ed.) (Pittsburgh, PA: Carnegie Mellon University, 2003), 1.

[16] Dodds, Watts, and Sabel, "Information Exchange and the Robustness of Organizational Networks," 5.

[17] Seth G Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering Al Qa'ida*, (Santa Monica, CA: RAND Corporation, 2008), 18.

that have not yet ended, their research suggests that terrorist network destruction is only half of the question. Clearly, additional research must address the dynamics that allow a terrorist network to survive in spite of losses, which is where the remainder of this work focuses.

One is also obliged to review the literature of the counterterrorism community of practice, specifically the Department of Defense, in order to discern a practitioners' perspective on terrorist group durability. Despite the experience gained through nearly a decade of continuous pursuit of al Qa'ida, existing doctrine also neglects the issue of why terrorist groups survive. However, Joint and U.S. Army doctrine do address network analysis methodologies as a method of disrupting these groups. Joint doctrine uses a systems approach to networks, typically revolving around the PMESII construct (Political, Military, Economic, Social, Infrastructure, and Information). The doctrine states that social networks are only part of the picture of an enemy, and the interconnection between the layers of the operational environment provides additional insight into strengths and vulnerabilities.[18] Joint doctrine also states that the systems are both complex and dynamic, and therefore not amenable to "systems engineering approaches."[19] Unfortunately, supporting joint doctrine does not address the dynamics of the system but instead focuses on the structure of the system. Emerging joint intelligence and counterinsurgency doctrine focuses exclusively on structural measures of networks such as centrality, closeness, and density.[20] Army counterinsurgency doctrine provides a more nuanced and less abstract view of networks, but still focuses on structure by emphasizing roles and position.[21] Both Army and Joint doctrine assume that understanding network structure is a key to defeating a networked organization, an implicit assumption in JP 5-0 and an explicit assumption in FM 3-24.[22] This monograph looks to see if this is in fact true.

[18] JP 5-0, *Joint Operation Planning*, III-17.

[19] Ibid., III-18.

[20] Joint Publication 3-24, *Counterinsurgency Operations* (Revision First Draft), G-2.

[21] FM 3-24, *Counterinsurgency*, B-17.

[22] Ibid., B-17.

THEORY SECTION

Before embarking on the remainder of this research, some explanation of the general and specific theories on network analysis is essential. Many of the network analysis techniques applied to this monograph are technical from a mathematical perspective as well as a conceptual perspective. Although many readers may be already familiar with some rudimentary network analysis procedures like those found in popular applications such as *Analyst Notebook*, the research presented in this work moves well beyond this level of analysis. Therefore, a familiarization with both basic and intermediate aspects of network theory as well as the theory behind the specific techniques applied in subsequent sections is necessary. This discussion first focuses on general network theory with regards to the significance of network topologies and provides three relevant network models commonly utilized in terrorist network research. This discussion on general network theory as applied to terrorism then shifts to a discussion of meta-network theory, which is a crucial concept to this research and may be unfamiliar to many readers. This section then transitions into a comprehensive review of the dynamics of network evolution, coupled closely to the notion of network attack. In order to fully understand the implications of this research approach, this theoretical discussion concludes with a summary of the limitations to this form of analysis. Finally, this section concludes by presenting the author's theory on the resilience of network terrorism and proposes a testable hypothesis.

General Theory – Structure and Topology

At this point a fair question requiring a responsible answer is "Why focus on the specifics of networked terrorist groups?" The most direct answer to this question is that the structure of the network, or topology, presents a set of constraints based on explicit and implicit choices made by any organization. By understanding how the structure exists and restricts action, counterterrorism officials have a window into the organizational constraints that bound an organization such as al Qa'ida in Iraq or FARC in Columbia. Structure dictates how individuals interact and the nature of these interactions, as well as the

nature of interactions to external entities. In most cases, organizational topology is the key to network dynamics because this structure dictates (or constrains) the spread of ideas, information, and innovations. Additionally, the dynamics of the organization based on this topology also influences how the organization evolves in the future.[23]

An important point on networks as applied to organizations is that of hierarchy. Just because a given organization is "networked" does not mean that there is no hierarchy to the organization or that no given individual is in charge. All organizations are hierarchical to some degree regardless of the type of structure that organization conforms; the structure dictates how control is effectively or ineffectively exerted, which may vary by situation. As a result, viewing terrorist networks as "leaderless" does not accurately depict the reality at hand. Although an organization may establish a structure that allows subordinates to operate with considerable independence, the hierarchy and structure of the organization is what enables this capacity. For instance, although al Qa'ida elements have considerable autonomy from Osama bin Laden and what is commonly referred to as al Qa'ida Central,[24] al Qa'ida identity implies some adherence to the core leadership. Ayman al Zawahiri's 2005 rebuke of Abu Musab al Zarqawi is one example of this hierarchy exerting itself on a subordinate commander.[25] While one can argue that Zawahiri's efforts were ineffective and proves the theory of so-called "starfish" organizations, the fact that al Qa'ida Central perceived a dominant relation over al Qa'ida in Iraq indicates an inherent perception of hierarchy. Therefore, this work does not adopt the prevalent tendency to view networked organizations as hierarchy-free.

The first major category of networks is small-world networks, characterized by short path length between nodes. The generally accepted model of small-world networks is the Watts-Strogatz model, a mathematical network model constructed by linking each node in the network to any immediate neighbors

[23] Albert and Barabási, "Statistical Mechanics of Complex Networks," 91-92.

[24] Jones and Libicki, How Terrorist Groups End, 115.

[25] Combating Terrorism Center at West Point Harmony Database, "Summary of Zawahiri's Letter to Zarqawi," http://ctc.usma.edu/aq/pdf/Zawahiri-Letter-Summary.pdf.

and then linking a given number of nodes to a randomly selected node in the network. These random links are the defining feature of small-world networks, since they allow for nodes to access "far" nodes using the shortcuts provided by the random links. Almost all social networks have small world topology and get their label from the universal phenomenon of when two people discover they have a mutual friend from a separate context, remarking that "It's a small-world." An example of this experience is when two colleagues in a professional school learn that one colleague was recently divorced from a woman the other colleague knew in college. Another example is the "Six Degrees of Kevin Bacon" game popular in the late 1990's where people tried to link celebrities or obscure actors to Kevin Bacon in the shortest number of steps. The current CAC Commander (LTG Caldwell) links to Kevin Bacon in three steps, since LTG Caldwell appeared on *The Daily Show with Jon Stewart* in 2008, who was in the movie *Mixed Nuts* (1994) with Steve Martin, who appeared in *Novocaine* (2001) with Kevin Bacon.

Despite the emphasis on social networks, the small-world property appears in many natural and information networks and may in fact be a general property of large networks.[26] Small-world networks are typically described by the average shortest path length between nodes, which is called the diameter *d*. Due to the random links across the network, even a very large network can have a very small diameter: experimental testing shows that rewiring as few as five nodes on *any* sized network decreases the average shortest path length (the diameter *d*) by 50%.[27] The trick for all networks is knowing how to navigate the network to search for the correct node.

[26] Duncan J. Watts and Steven H. Strogatz, "Collective Dynamics of 'Small-World Networks." *Nature*, Vol. 393 (June 4, 1998): 441.

[27] Watts, *Six Degrees*, 89.

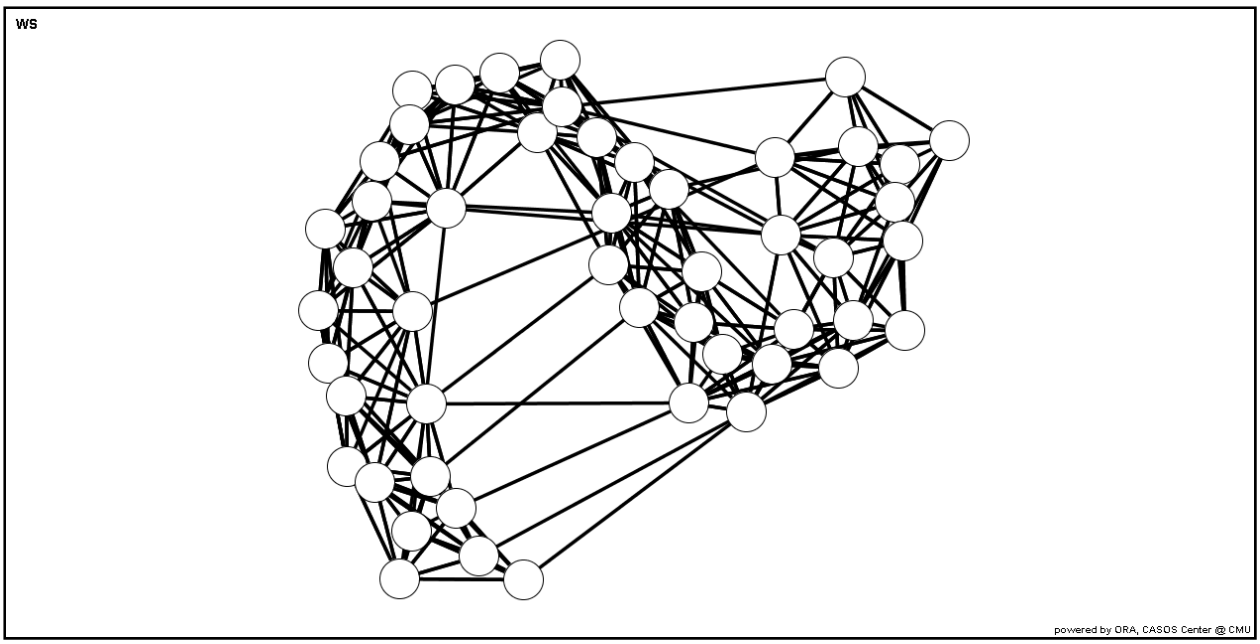

Figure 1: Small-world network example

The notion of network search underlies much study of small-world networks because it is a non-trivial problem (mathematically known as *NP*-complete), meaning that even the best search algorithms on the fastest computers will labor to find a "shortcut" to solve the problem, simply due to the fact that there is a lot of network to search.[28] In other words, in *NP*-complete problems the best algorithm will not perform much better than brute force, which in the context of networks means exploring every possible combination of network paths. There is currently no efficient search algorithm to find shortest paths in the Watts-Strogatz network, meaning that computers will probably underperform humans in this task despite computing speed since humans have the benefit of insight and context.[29] Additionally, the shortest path in a network is in no way the most likely path, since an individual in a given social network typically only has a complete understanding of their local network and have a much more limited understanding of the

[28] Barabási, *Linked*, 37 and 171.

[29] Melanie Mitchell, "Complex Systems: Network Thinking," *Artificial Intelligence*, Vol. 170, Issue 18 (December 2006): 10.

global network.[30] Despite the limitations on information, people in social networks make these connections all the time, implying that people use other factors besides physical distance to locate other people.[31] This is partially due to the fact that in the real world people can have multiple identities based on any number of factors such as religion, hometowns, profession, online communities, etc. This set of factors serves as a set of contexts that are the crucial determinant of establishing social network. In other words, real people have social identities, which drive the creation of actual social networks.[32] Additionally, not all people in a social network have the same number of connections, leading to the obvious notion that some people have significantly more links than others.

This leads to the next type of network, called scale-free networks. Scale-networks describe those networks where a small number of nodes have significantly more links than other nodes. Unlike a random graph where degree distribution *K* follows a Poisson curve (as opposed to a Gaussian or bell curve), scale-free networks obey a power law whereby a small number of nodes have the majority of links in the system. This power law is similar to Pareto's Principle or "80/20" rule, where less than 20% of the people control 80% of any given asset.[33] Because of these high-degree nodes, scale-free networks also possess the small-world property and can therefore be considered as a subset of small-world networks.[34] However, unlike small-world models, scale-free network models focus on capturing the dynamics of a network since the scale-free property typically arises when the networks can grow using the notion of preferential attachment.[35] Simply put, preferential attachment means that new nodes are more likely to link to high degree *K* nodes, a phenomenon observed in social networks, financial networks, and information networks such as the World Wide Web. This observation is sometimes referred to as the

[30] Peter Sheridan Dodds, Roby Muhamad, and Duncan J. Watts, "An Experimental Study of Search in Global Social Networks," *Science*, Vol. 30 (August 18, 2003): 827.

[31]Duncan J. Watts, Peter Sheridan Dodds, and M. E. J. Newman. "Identity and Search in Social Networks," *Science*, Vol. 296, No. 5571 (May 17, 2002): 1.

[32] Watts, *Six Degrees*, 116-117.

[33] Barabási , *Linked*, 66.

[34] Mitchell, "Complex Systems," 7.

[35] Albert and Barabási, "Statistical Mechanics of Complex Networks," 71; Barabási, *Linked*, 86.

"Matthew Effect," whereby the well-connected nodes are more likely to gain new links whereas the poor nodes will stay poor.[36] In these types of networks, new nodes insert into the network over time and at no point is there a "master designer" who determines the structure. The Internet is the supreme example of preferential attachment, since each router and local hub comes on line in an ad-hoc manner by linking into another backbone hub typically dictated by proximity and cost. Preferential attachment in its various forms is simply an attempt to quantify the notion that some nodes are more attractive to link to than others and formalizes the notion of "the rich get richer" or "the fit get richer."[37] The use of scale-free networks to describe real world networks is also an acknowledgement that most real networks are open systems that continually grow and add more nodes.[38] As a general rule of thumb, any network that is growing could be considered a potential scale-free network, and any network that is scale-free is in all likelihood growing by adding new nodes. Growing networks that are not scale-free include those networks without "cheap links", meaning that the cost per unit of distance is relatively static throughout the network. Road networks are one example of a growing network that is not scale-free but is instead random, since the cost of a road per unit of distance does not reward "shortcuts," whereas an airport network is scale-free because the cost of links is much lower.[39]

[36] Watts, *Six Degrees*, 108.

[37] Barabási, *Linked*, 96.

[38] Albert and Barabási , "Statistical Mechanics of Complex Networks," 71.

[39] Barabási, *Linked*, 71.

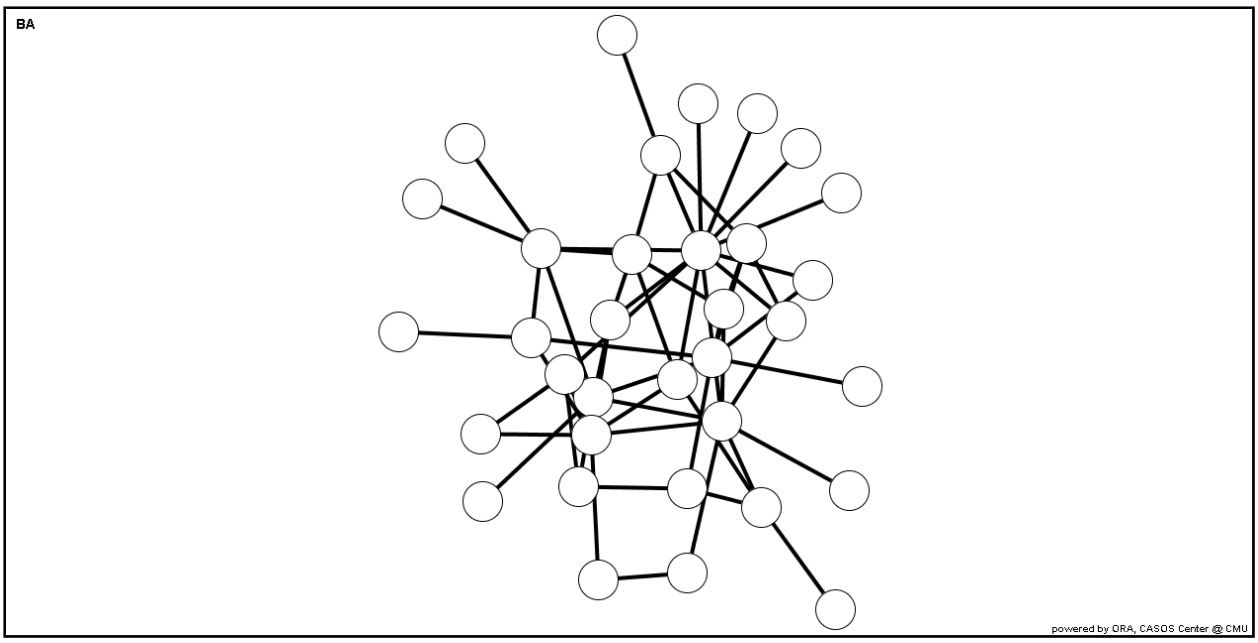

Figure 2: Scale-free network example

While the scale-free and small-world network models provide a basis for analyzing a wide range of networks, researchers dispute the applicability of these models. Most real-world networks do not fit cleanly into the scale-free or small-world *mathematical* models,[40] although this does not necessarily mean that these networks cannot exhibit scale-free or small world properties. For this reason, a third model is needed to complete this survey of network models, which is cellular design model. Cellular models are comprised of small clusters of nodes, sometimes called cells, which are linked together loosely or linked to a central control cluster or node. Each cluster is densely connected to each node within the cluster, as compared to the connectivity between individual clusters. As a network model, a cellular network can also exhibit the small-world property since any node can be reached in a relatively short number of links. However, due to the fact that members of clusters are densely interconnected, it is less likely that the scale-free property is observed. A notable exception occurs within the makeup of the cluster itself, since a cluster can also be organized within itself as groups of smaller clusters. In this instance, a scale-free

[40] Maksim Tsvetovat and Kathleen M. Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," *Computational and Mathematical Organization Theory* 13, No. 1 (March 2007): 76.

structure can emerge with the cluster "leaders" as the most connected nodes in accordance with the power law.

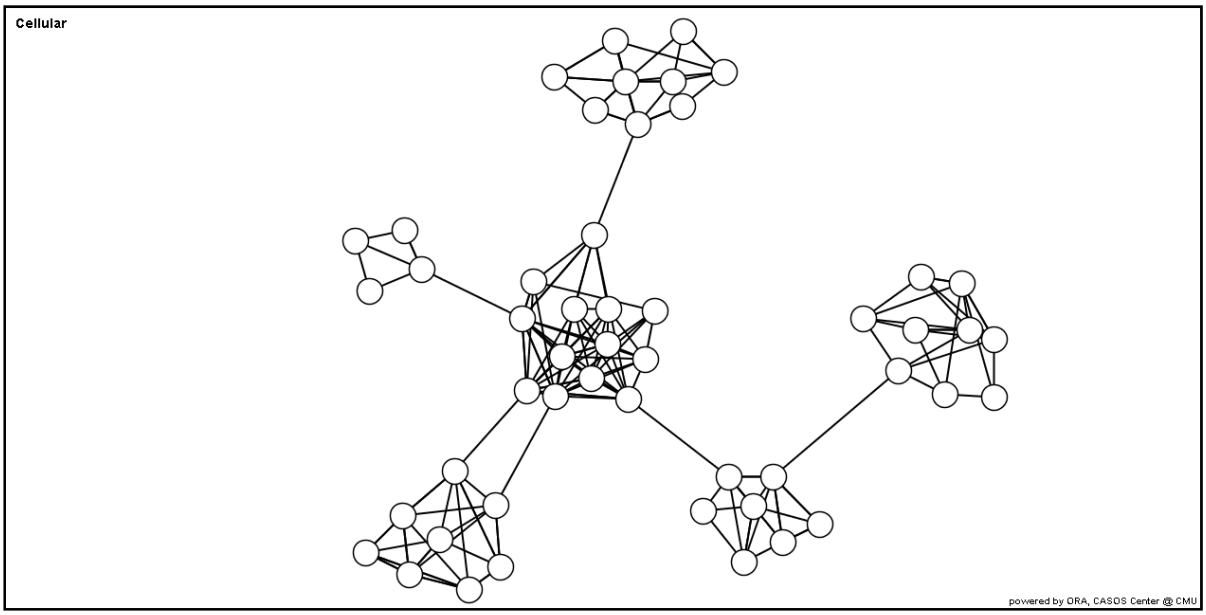

Figure 3: Cellular network example

As an organizational model, cellular designs are more applicable to covert groups when compared with the two previous models due to the need to minimize security breaches. Tsvetovat and Carley (2007) described five properties that account for the distributed command characteristics of cellular organizations: 1) the entire network is a connected component, 2) the network is redundant at each level, 3) the network is small and dynamic at the local level, 4) the network is not managed through control but instead through what military officers recognize as "intent-based" guidance, and 5) the organizational structure is not a deliberate decision but an emergent property based on security constraints.[41] However, an important distinction is that none of these properties described are mutually exclusive, meaning that some networks may exhibit all three properties simultaneously.

[41] Tsvetovat and Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," 67-68.

Meta-Networks

Unfortunately, knowing the social network is insufficient to understanding a terrorist network as a whole. For starters, the social network does not necessarily indicate the hierarchy and who is in charge. If assessing leadership is not possible from even a complete picture of the network, then pure social network analysis is insufficient. This fact is especially important for counterterrorism, since counterterrorism analysts almost always infer the structure of the terrorist network in question from interrogation or intelligence operations. Ultimately, knowing the social network structure does not describe what the nodes decide to do with their particular knowledge of the network, since knowledge is limited and impacts their ability to find the most coherent and economical connections.[42] Social networks alone also fail to capture the other requirements and attributes of a terrorist organization. In order to prosecute attacks, a terrorist cell requires resources, information on the target, expertise with weapons and surveillance, locations in which to hide, as well as the people who will execute the mission. As a result, analysts must also analyze and map additional networks in order to develop a more complete understanding of how work flows through the network. Fortunately, this concept of "workflow" is inferable from the social network if additional context is provided.[43] This leads to the notion of meta-networks, which is a network of networks.

The meta-network has two defining characteristics, which are that it is multi-mode with several different entity classes such as agents, actions, locations, and so on, as well as multi-plex with several different types of connections such as financial and directive.[44] These are also known as bi-parite networks, where nodes of the same class are not connected to each other but instead linked to nodes of a

[42] Mitchell, "Complex Systems," 12.

[43] Il-Chul Moon, Kathleen M. Carley, and Alexander Levis, "Vulnerability Assessment on Adversarial Organization: Unifying Command and Control Structure Analysis and Social Network Analysis," *SIAM International Conference on Data Mining, Workshop on Link Analysis, Counterterrorism and Security*, (Atlanta, GA: April 26, 2008): 1-2.

[44] Kathleen M. Carley, "Destabilization of Covert Networks," *Computational and Mathematical Organization Theory* 12, No. 1 (April 2006): 52.

different class.[45] One unfortunate side effect of the meta-network approach is that the actual number of potential networks involved increases from one network (the agent to agent) to n^2 networks, where n is the number of node classes. Fortunately, not all these networks are always relevant to the given task or are even logical, and this section will discuss only a few of these networks.[46] The Agent networks are the most commonly understood since they involve people. Aside from the Agent to Agent network, some of the relevant agent networks are the Agent to Group network (since people can belong to more than one group), the Agent to Knowledge network, the Agent to Resource network, the Agent to Location network, and the Agent to Belief network.[47] Knowledge networks are essential to meta-network analysis, since it allows counterterrorist officials to understand how an organization acts. Moon and Carley argue that knowledge diffusion is the key performance measure for terrorist organizations.[48] Closely linked to the Knowledge networks are the Location networks, since both knowledge and agents may be geographically distributed. Certain pieces of knowledge may only be accessible at a specific location, such as intelligence gathered from a surveillance mission. Location networks may also indicate regional terrorist training sites.[49] A similar concept is that of the task environment, defined by the rate of message passing and distribution and can differ based on location. Stable regions have low information exchange rates, whereas higher information exchange rates characterize volatile environments.[50]

---

[45] Watts, *Linked*, 119.

[46] An example of an illogical network is the Knowledge-to-Agent network. While the reverse of this network make sense since it indicates what a given Agent knows or needs to know, the Knowledge-to-Agent network indicates what Agents the Knowledge requires. While one could argue this point on the grounds that Knowledge needs to be possessed by something, the notion of "Knowledge's needs" is irrelevant to this research.

[47] Kathleen M. Carley, "Estimating Vulnerabilities in Large Covert Networks," *Proceedings of the 8th International Command and Control Research and Technology Symposium Conference. (Washington DC: National Defense War College, 2003):* 8-9.

[48] Il-Chul Moon and Kathleen M. Carley, "Locating Optimal Destabilization Strategies," *Proceedings of ICCRTS, (Newport, RI: June 2007)*: 3.

[49] Il-Chul Moon and Kathleen M. Carley, "Modeling and Simulating Terrorist Networks in Social and Geospatial Dimensions," *IEEE Intelligent Systems* 22, No. 5 (September/October 2007): 45.

[50] Peter Sheridan Dodds, Duncan J. Watts, and Charles F. Sabel, "Information Exchange and the Robustness of Organizational Networks," *Proceedings of the National Academy of Science of the United States of America*, Vol. 100, No. 2 (October 14, 2003): 8.

One difficulty in applying meta-networks to a global terrorist movement is that the networks do not exist in isolation from the societies they inhabit. Although they may seek to maximize their security, not all terrorists can hide in the middle of a desert until they decide to execute attacks on another country or target. Since a given terrorist can belong to more than one social circle, they may have more than one affiliation, which also means that terrorist groups are embedded to some degree within the society they originate in. This is due to the intersection of their various affiliation networks based on their ability to belong to more than one group.[51] Bounding the system is difficult under these circumstances. On the other hand, it is relatively easy to apply meta-network analysis to a relatively isolated tribal society. The tribal society has complex but somewhat self-contained social, economic, military, and knowledge networks. This self-contained meta-network description of tribal societies could help explain why these groups can be quickly adapted for military action.[52]

Network Evolution

As previously discussed, networks are not static entities that are "locked" into their structure for extended periods of time, which necessitates a generalized model of how networks evolve. In fact, the whole concept of network analysis is of questionable value without some theory of dynamics, since the theory is supposed to represent networks that are acting and therefore evolve as a result of their own interactions.[53] Unfortunately, this very fact of dynamic networks complicates the understanding of networks in the first place, since they can change from minute to minute.[54] While various approaches to this problem already exist, this research must restrict the scope of inquiry to the evolution of networks over the near term, ignoring some of the long-term trends of network evolution. Given the fact that terrorist organizations battling government forces face attrition and recruiting, any long-term model of

[51] Watts, *Linked*, 128.

[52] Brian Reed, "A Social Network Approach to Understanding an Insurgency," *Parameters: U.S. Army War College Quarterly*, Vol. 37, No. 2 (Summer 2007): 25.

[53] Watts, *Linked*, 51 and 28.

[54] Steven H. Strogatz, "Exploring Complex Networks," *Nature 410*, No. 6825 (March 8, 2001): 268.

network evolution must account for the reality that the short-term dynamics are more relevant for analysis. In fact, one could go so far as to say that the long-term dynamics of a terrorist network are purely the product of the short-term dynamics unless the organization is isolated from government attacks and has minimal recruiting. Watts proposes two types of dynamics which are both required in order to fully understand how networks evolve over time. The type of dynamics most commonly used in social network analysis are those dealing with the nature of interactions between nodes as a consequence of the network structure, which is called dynamics *on* the network.[55] This category governs how nodes react to each other based on the overall structure of the network. The second type of network dynamics, dynamics *of* the network, governs the changes in the network structure and evolution of that structure.

For terrorist networks, dynamics *of* and *on* the network are primarily governed by agent attrition and recruitment. As counterterrorist forces or defection removes terrorists from the network, the dynamics *on* the network dictate how people will interact with the new diminished structure. If security forces kill a key member of a terrorist cell, the remaining agents must use other existing links to continue operating and communicating. Much of the existing research applicable to dynamics *on* terrorist networks is based on information networks such as the Internet, which routinely face failure of critical hubs thereby requiring dynamic message rerouting. Unfortunately, the time scale applied to much of this research does not allow for creation of new links or the addition of new nodes, since a new router or hub cannot be added to the network in real time, and therefore limits some of the applicability of dynamics research based on information networks. This leads to the dynamics *of* the network since these same agents will in all likelihood generate new network structure, primarily through recruiting new members. Additionally, these agents may learn to communicate with other nodes or activate latent links to other agents in order to sustain functionality. While existing terrorist network research has neglected the internal mechanics of

[55] Watts, *Linked*, 55.

creating new links due to the obvious lack of useful data, Sageman provides a useful model of terrorist recruitment by viewing it as a social endeavor.[56]

Growth dynamics are essential in order to gain a fundamental understanding of real-world networks, since the growth itself dictates many of the structural characteristics of networks and indicates a general organizing principle.[57] This growth is typically accomplished through preferential attachment and triadic closure, whereby nodes are linked together if they both have a common neighbor.[58] Sageman's model of terrorist network growth utilizes the notion of preferential attachment to show the networks do not grow or evolve in a completely random fashion.[59] Even without the addition of new nodes, the concept of triadic closure allows a network to continue to evolve as actors with common neighbors link together in their own right. In meta-networks, this also applies to the other networks besides social networks, since other people may gain access to resources or make connections to types of information over time.

Attack Theory

One crucial factor bearing on terrorist networks is the fact that they are typically under attack from military or law enforcement counterterrorist forces. As a result, a general understanding of attacking networks is required for any analysis on terrorist meta-networks. Attacks on networks in existing theoretical works generally take the form of disrupting links or removing nodes, with node removal as the more effective technique in damaging network structure. The structure of the network is a key determinant in the effectiveness of the attack in disrupting operations, which also translates into the notion that attack effectiveness is dependent on the organizational architecture since networks represent

[56] Marc Sageman, *Understanding Terror Networks*, (Philadelphia: University of Pennsylvania Press, 2004): 110 and 120.

[57] M. E. J. Newman, "The Structure and Function of Complex Networks," *SIAM Review*, Vol. 45, No. 2 (June 2003): 212.

[58] Newman, "The Structure and Function of Complex Networks," 212.

[59] Sageman, Understanding Terror Networks, 139.

organizations.[60] Random attacks on scale-free networks are generally ineffective in causing the network to collapse (meaning that significant portions of the network are disconnected to the degree that they cannot transfer information in a meaningful way) due to their high tolerance against random failures, but targeted attacks against highly connected nodes are more effective against scale-free networks.[61] The Barabási-Albert scale-free network model loses 50% of its efficiency after removal of 15% of the most connected nodes. In order to destroy a scale-free network, attackers must remove 35% of the most connected nodes using a targeted approach,[62] as opposed to removing 80% of the nodes using a random approach.[63] In the case of large networks (to include terrorist networks), this resilience from attacks is implemented at the local level instead of at the global level through some notion of centralized control, since the local network can reroute information as required.[64] Experimentation suggests that networks constructing smaller independent networks of cliques, clusters, or cells, are more resilient to attack than scale-free and small-world networks.[65] However, this form of network is typically constructed consciously and may not be an appropriate model at higher attrition rates due to the ad-hoc nature of replacements in this situation.

Aside from attacking the social network, which is generally physical in nature, there are ways to attack some of the more abstract networks associated with terrorist networks such as the knowledge network. In these situations, a meta-network approach is helpful. Some ways to attack the knowledge networks are to limit training, disrupt access to knowledge, and reduce adaptivity, a strategy best described as attacking transactive knowledge.[66] Every agent has some form of transactive knowledge

---

[60] Carley, "Inhibiting Adaptation," 8.

[61] Albert, Jeong, and Barabási, "Error and Attack Tolerance of Complex Networks," 381.

[62] Crucitti, et al, "Error Tolerance of Complex Networks," 391.

[63] Petter Holme, et al, "Attack Vulnerability of Complex Networks," *Physical Review E*, Vol. 65, Issue 5, (May 7, 2002): 8.

[64] Nagaraja and Anderson, "The Topology of Covert Conflict," 4.

[65] Najara, Anderson (2005), 14.

[66] Carley, "Inhibiting Adaptation," 3-5.

describing each agent's understanding of the social network and how they operate, to include access to resources, which are used by agents to operate within the network; the more accurate this knowledge, the more effective the organization.[67] Stored transactive memory can be as simple as a phone book or a database used to store institutional knowledge and train successors. A terrorist network utilizing such a database or training materials, located in a central location or on secure Internet sites, could recover from the loss of key personnel much quicker than groups without such a resource. Two distinct strategies emerge to attack knowledge networks: the first is to attack the nodes with either the highest cognitive load, a measurement of how much a specific node is involved in executing various tasks, and the second is to attack the node with the highest task exclusivity, meaning that the targeted node is the only one able to execute the task.[68] Since these two measurements are related, a hybrid approach that attempts to attack nodes with high task exclusivity and high cognitive load is more effective in destabilizing a terrorist network. The notion of cognitive load is important not only because it can predict key nodes within a given network, but it may also predict emergent leaders following the death or capture of existing leaders.[69] Cognitive load also shifts as agents are removed from the network, which may force remaining agents to make new connections in order to solve day-to-day problems. This is consistent with findings that routine problem solving is one of the defining features of real world organizations, enabled by a network structure.[70]

A more problematic and abstract form of attack is an attacks on belief networks. Since some form of ideology or belief system typically binds terrorist groups together, this can also be represented in the meta-network, especially in groups with beliefs not shared by the entire organization (such as the morality of suicide bombing or targeting co-religionists). The key difficulty with attacking a belief network is that it is tremendously challenging to assess effectiveness in these attacks. However, mapping beliefs onto a

[67] Carley, Reminga, and Kamneva, "Destabilizing Terrorist Networks," 2.

[68] Carley, Reminga and Kamneva, "Destabilizing Terrorist Networks," 4.

[69] Carley, "Estimating Vulnerabilities in Large Covert Networks," 14.

[70] Watts, *Linked*, 270.

meta-network does provide a potential framework for developing information operations as well as integrating intelligence reports of internal divisions into the overall network structure.

Advantages and Limitations of Dynamic Network Analysis

The key advantage in using dynamic network analysis tools on meta-networks is that these methods overcome the problems associated with viewing networks as static entities. Terrorist networks evolve regardless of whether intelligence officials are aware of the changes. As a result, intelligence analysts must have tools that reasonably project the most likely growth and structure of an organization over time. Tools such as *Analyst Notebook* do not have this ability, and as a result can only provide as much insight as is known directly and entered into the system. Dynamic network analysis also provides better tools for post-attack assessment by providing a likely network structure after a key attack by identifying emergent leaders. Using dynamic network analysis also provides better insights into knowledge gaps by inferring existing but unobserved network structure. If counterterrorism officials determine that the targeted terrorist network is performing to a degree that exceeds their observed capacity, they can use these tools to develop possible theories regarding the structure of portions of the networks not yet detected.

Despite these advantages, several limitations exist in research testing using dynamic network analysis. These limitations fall into broad categories based on agency and structure. In terms of agency, four limitations emerge. The most important and intuitively obvious limitation is that personality can have tremendous impact on the effectiveness of any organization. The different performance of identical military units throughout history is testament to this fact. Charismatic leadership or ineffective leadership can have a decisive impact on how any organization performs, and no structural analysis technique can account for this. As a result, counterterrorism officials must be fully cognizant of the fact that all leaders are essentially treated identically in any structural analysis and view results with this fact in mind.

The second agency-based limitation is that people react to the radicalization process differently, and radicalization itself takes time. In other words, people do not become terrorists overnight. British

intelligence officials recently estimated the time it took to radicalize a potential terrorist from a "harmless" civilian into someone willing to conduct attacks is approximately 18 months.[71] A third and related limitation is that radicalization can differ by location. Analysis of arrest rates when compared to the per-capita Muslim populations of Europe and the United States shows European Muslims have a radicalization rate up to six times higher than American Muslims.[72] Some possible explanations for this phenomenon are the embedded nature of American police forces into communities as compared to Europe, the American melting-pot mythos that facilitates assimilation as compared to the European emphasis on national essence, and the tendency of American Muslims to predominantly come from professional classes as compared to European Muslims who are typically in the working classes.[73] Additionally, some European nations have laws which limit the ability of foreign born minorities to integrate fully into society. As a result, analysts using these network models must acknowledge that these different radicalization rates affect the rate at which new agents can be added to a terrorist organization.

The fourth limitation based on agency is the fact that terrorists can mitigate discovery through the ability to avoid detection and mask the organization, which may lead to significant discrepancies between projected and actual organizational structure. Al Qai'da's four-tiered courier system developed following their expulsion from Afghanistan by U.S. forces is one such example, whereby the organization created several communication networks by compartmentalizing messages. The administrative network and operational network were separated by using different couriers. They also developed a media network charged with sending out their communications to the greater Muslim world through their propaganda group As Sahab. The most secure network consisted of memorized messages sent between key leaders.[74] Counterterrorist analysts tapping into any one of these networks would not be able to determine the entire scope of the network or the identities of the key nodes.

---

[71] Jones and Libicki, *How Terrorist Groups End*, 127.

[72] Sageman, Leaderless Jihad, 90.

[73] Sageman, *Leaderless Jihad*, 93-100.

[74] Jones and Libicki, *How Terrorist Groups End*, 129.

Aside from limitations based on agency, the primary structural disadvantage to using network analysis techniques, either static or dynamic, is that most terrorist networks (to include al Qa'ida) are not strictly organized as networks but instead combine networked and traditional hierarchical structures due to the existence of central leaders with centralized control of resources and training.[75] As a result, real terrorist networks do not necessarily fit into scale-free or other mathematical models since the leadership may not want a particular agent to be involved in given operation or task, and any terrorist network fitting a model could be a result of the collection process and not due to the network itself.[76]

The second structural disadvantage is that network analysis cannot account for the fact that individuals can make or break ties at will.[77] While this initially seems like a disadvantage based on agency, this is categorized as a structural disadvantage because the network structure itself is more malleable than even the most advanced techniques can project. For instance, linkage data gained from interrogations on captured terrorists may in fact reflect former connections that are no longer relevant to the existing organization due to losses of key personnel through death, capture, or defection. Even if the detainee is giving what they believe is accurate information, the data may be incorrect since agents can only describe what they believe is the existing structure, even if it has changed since they last learned of the information (much like corporate reorganizations). This data could describe the organization incorrectly and lead to wrong conclusions. These "stale" links are artifacts of the organizations' previous structure and not indicative of the current structure. There is no effective way to remove these stale links in the transactive knowledge of each agent unless every agent is aware of another agent's removal through defection, capture, or death. This leads to the notion of time as a parameter, since a shorter observation window yields considerably different results than a greater observation window. Analyzing al Qa'ida using links utilized in a given month provides a small dataset that eliminates those links that are

[75] Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," 7.

[76] Tsvetovat and Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," 76-77.

[77] Nobuyuki Hanaki, et al, "Cooperation in Evolving Social Networks," *Management Science*, Vol. 53, No. 7 (July 2007): 22.

active but infrequently used; analyzing the same organization over 20 years is equally fruitless, since the stale connections persist.

Applied Theory and Hypothesis

This leads to the primary question of this research, which is why do terrorist networks continue to survive despite persistent attacks by military and law enforcement officials? Based on the previous discussion of network dynamics and meta-networks, two potential answers emerge for testing. Since the ideology is difficult to attack, any terrorist network sustained by ideology will be able to continue to generate new membership for as long as the ideology is attractive. This is leads to the conclusion that an attractive ideology can maintain a high level of recruits even in light of devastating losses. The ability to recruit leads to the next key factor in sustaining the terrorist organization, which is that even the lowest recruit can work their way deeper into the organization over time as the network evolves. As a result, the generative ability of networks and ability of the network to evolve prevents purely kinetic solutions as long as the ideology is sustainable.

The issue of recruiting new members is at the heart of the problem in sustaining organizations. Despite the tendency to view them as separate societies, considerable evidence from counterterrorism operations suggests that terrorist networks are not wholly isolated from their societies since they typically require support from these societies,[78] and as a result could be described as open systems. A terrorist network can originate from existing networks within a given society (such as a group of friends) and is not entirely isolated.[79] Additionally, in contrast to Erickson's work suggesting centralized recruiting in secret societies,[80] control over recruiting in modern terrorist organizations appears to be locally implemented and not centrally implemented. Using Sageman's models of jihad as a social endeavor leads

[78] Jones and Libicki, *How Terrorist Groups End* , 25.

[79] Bonnie H. Erickson, "Secret Societies and Social Structure," *Social Forces*, Vol. 60, No. 1 (September 1981): 196-197.

[80] Erickson, "Secret Societies and Social Structure," 197.

to the conclusion that although established networks can serve as the basis for secret societies as stated by Erickson,[81] the notion that central leaders make a conscious decision to integrate these networks into the larger networks and completely remove them from the larger society is inconsistent with present experience and research. As a result, terrorist networks may be better viewed as a smaller system embedded within a larger system, which is the society as a whole.[82]

This leads to one testable hypothesis and a null hypothesis:

> H_1: Terrorist organizations that sustain their core ideology will survive as long as some number of recruits linked to the core ideology advance within the organization.
>
> $H_{0:}$ Terrorist organizations will have a hard time surviving even if they sustain their core ideology if they cannot retain a critical number of recruits at all times.

[81] Erickson, "Secret Societies and Social Structure," 196.

[82] Vito Latora and Massimo Marchiori, "Efficient Behavior of Small-World Networks**,"** *Physical Review Letters* Vol. 87, No. 19 (November 5, 2001): 4.

MODEL CONSTRUCTION

Since the interactions and decisions of individuals are the basis of social networking, using a multi-agent model to test social and meta-networking theories is entirely appropriate. Developing a successful multi-agent model requires the translation of concepts and theories into individual decisions by agents. This in turn allows researchers to identify emergent behavior and provides the ability to manipulate decision thresholds for insight into the conditions required for phase transitions from one state to another. Model construction and use is not an attempt to develop a "terrorist simulator" that analyzes and predicts group behavior. The model is instead a starting point for developing more refined inquiries by demonstrating some of a terrorist organization's possible choices based on existing theory and research. Like education, the purpose of modeling is not to provide answers but to trigger better questions.

The first step in model construction begins with the agents themselves. Researchers can describe nodes within a network as individual agents with certain properties such as a list of neighbors, types of knowledge, assigned tasks, and so on. This enables the model to capture many of the properties of the meta-network as properties of the agents. The other categories of nodes serve to capture those properties of the meta-network not covered by agents in order to maintain the multi-parite and multi-plex properties of the meta-networks. Each node category in the meta-network translates into a node in the multi-agent model. However, only the agents themselves have the ability to manipulate connectivity of other nodes, whereas the remaining node classes are essentially static.

The agents in this research are drawn from the 2006 edition of the 1998 Tanzania Bombing Dataset (version 3) developed by CASOS.[83] This data set is a meta-network consisting of eight node classes and seventeen networks, to include an Agent-to-Agent network (the social network), an Agent-to-Knowledge network (the knowledge network), and an Agent-to-Resource network (the resource network).

[83] *Tanzania Embassy Bombing Data Set*. Carnegie Mellon University CASOS, 2006. (http://www.casos.cs.cmu.edu/computational_tools/datasets/internal/embassy_2006/index2.html)

Since several of the networks and node classes are not required for this research, the actual testing dataset is a reduced version of the original dataset. Whereas Tanzania $_{2006\text{-}3}$ contains eight node classes, Tanzania $_{Henke}$ contains just five (Agent, Belief, Knowledge, Resource, and Tasks). Additionally, the author removed several non-critical individual nodes within the node classes to simplify the data computation. For instance, while there are 35 different nodes in the Task node class, Tanzania $_{Henke}$ contains only 18 nodes. Figure 4 provides a full description of the meta-network and Figure 5 lists the characteristics of each type of node.

Node Classes	# Nodes		Networks
Agent	27	Agent to Agent	Knowledge to Belief
Belief	2	Agent to Belief	Knowledge to Task
Knowledge	14	Agent to Knowledge	Resource to Resource
Resource	11	Agent to Resource	Resource to Task
Task	18	Agent to Task	Task to Task
		Belief to Task	

Figure 4: Properties of the Tanzania $_{Henke}$ dataset meta-network.

Agent Properties
- Neighbors (List of Agent nodes)
- Beliefs (List of Belief nodes)
- Knowledge (List of Knowledge nodes)
- Resources (List of Resource nodes)
- Tasks (List of Task nodes)
- Time in Network (Single variable)
- Radicalization (Single variable)

Belief Properties
- Tasks (List of Task nodes)

Knowledge Properties
- Beliefs (List of Belief nodes)
- Tasks (List of Task nodes)
- Connected Agents (List of Agent Nodes

Resource Properties
- Resources (List of Resource nodes)
- Tasks (List of Task nodes)
- Connected Agents (List of Agent Nodes

Task Properties
- Tasks (List of Task nodes)

Figure 5: Tanzania $_{Henke}$ dataset node properties.

One crucial note on this dataset is that many of the connections are one-way in order to indicate either a hierarchy or relationships of a more directive nature. For instance, Osama bin Laden's driver probably has a one-way relationship with bin Laden in that he merely takes directions (possibly literally, in the case of a driver). As a result, a list of an agent's neighbors may not reflect who is directing him if

the initiative for contact is with the other agent. However, graphical depictions of the networks, such as the social network in Figure 6, do not indicate the direction of the relationship for ease of viewing.

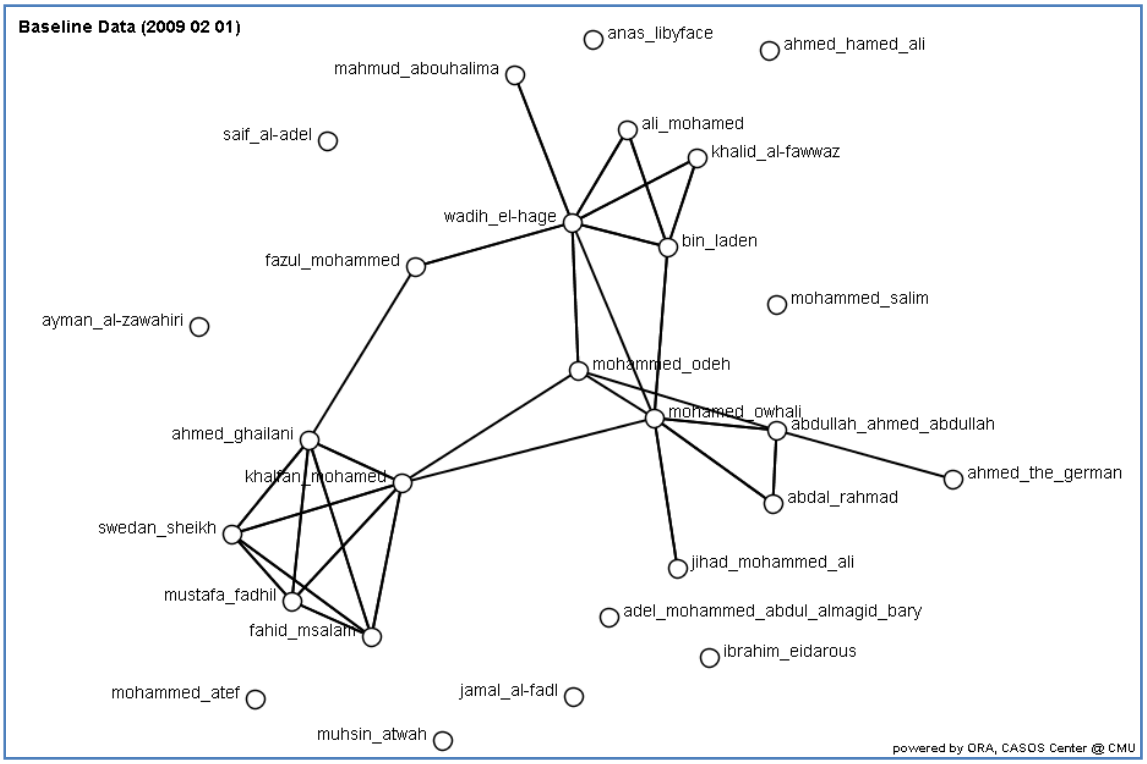

Figure 6: Tanzania $_{\text{Henke}}$ Agent-to-Agent network

The proposed model leverages Sageman's work on the radicalization process, which posits that radicalization is a process of time based on network embeddedness.[84] To operationalize this notion, one must view radicalization specifically as a function of time within the network, connectedness in the network, and the intensity of beliefs.[85] For the time being, the following function expresses radicalization:

$$Radicalization = f(Agent_{Time}, Agent_{K}, Agent_{Belief},)$$

The second principle of the proposed model is that resources and knowledge must have some level of redundancy. Despite the finding that small-world and scale-free networks cannot increase

[84] Sageman, Understanding Terror Networks, 120 and 135.

[85] This monograph uses the term "operationalize" in the academic sense, which is to turn a concept into a compact expression, usually in the form of a variable or equation. This work will explicitly state those instances when it uses "operationalize" in the military sense, meaning to translate concepts into some sort of capability.

redundancy without compromising security,[86] some level of redundancy is required to keep the network operational in the face of active attrition. Therefore, one of the rules of the model is that each resource and knowledge node must be accessible by at least two agents, and that the agents themselves with access to the knowledge or resource will seek to link neighbors to the knowledge or resource. Although some real-world organizations sometimes exhibit the exact opposite behavior by restricting knowledge or hoarding resources, these organizations tend to be easier to disrupt for that very reason. Since terrorist networks seek survival over time, one assumption of this research is that they will act in such a way to preserve any hard-fought gains in knowledge and resources.

By operationalizing both radicalization and knowledge/resource redundancy, a basic rule set for each agent in the form of an algorithm emerges. At the start of each iteration, *Agent* advances its time stamp, *Agent* $_{Time}$, and resets key tracking variables. *Agent* then executes the radicalization process, a process addressed shortly. After the radicalization process is complete, *Agent* looks at each neighbor (called *Neighbor*) and determines whether to link *Neighbor* to another neighbor under the principle of triadic closure. *Agent* and *Neighbor* must meet several conditions before the agent adds the link. For starters, *Agent* can only make one agent-to-agent link per turn and *Neighbor* can only gain one link (agent, knowledge, or resources) per round. Secondly, *Neighbor* $_{RadIndex}$ level must meet a globally defined constant, called *RadThresh,* but cannot exceed *Agent* $_{RadIndex}$. If *Agent* and *Neighbor* meet these conditions, *Agent* links *Neighbor* to its neighbor with the highest radicalization score. If *Agent* has the highest score, then *Agent* adds a two-way connection between itself and *Neighbor*. Using *RadThresh* as a global constant allows for comparative experimentation at varying levels of radicalization. Appendix 1: Multi-Agent Model) provides a full expression of the agent behavior algorithm.

[86] Henke, Glenn A. "Small-World Topology Networks: Predicting the Balance Between Resiliency and Security." Kansas State University Security Studies Master's Degree Terminal Paper (unpublished, 2008).

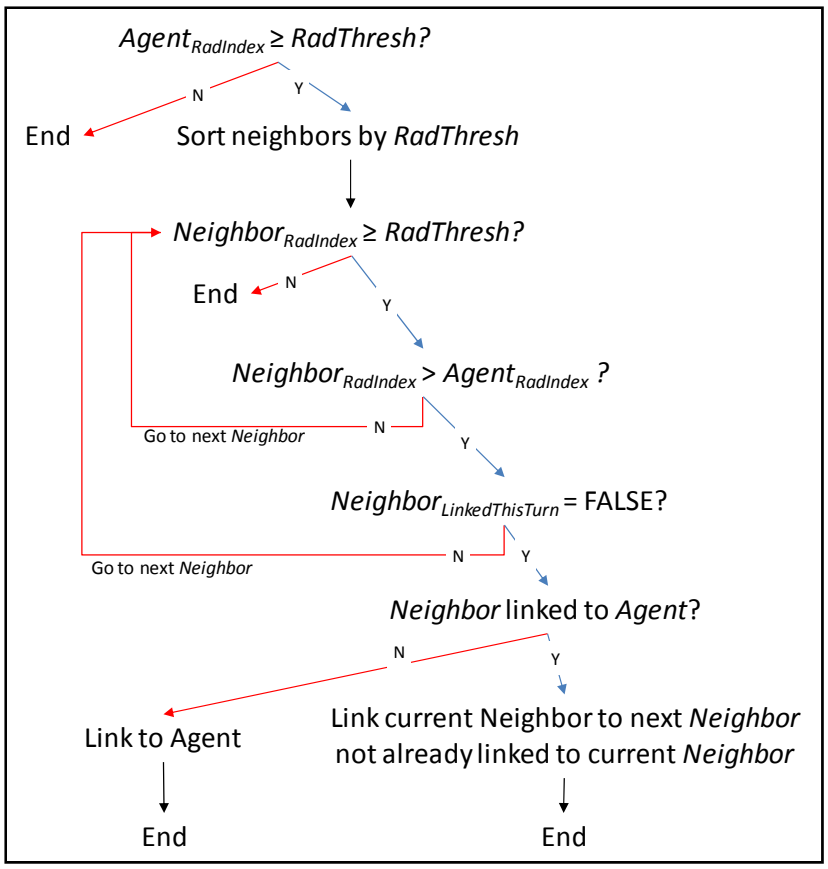

Figure 7: Agent Decision Tree

After completing the social network linking, the next *Agent* conducts the same procedure until all eligible agents have completed the process. The knowledge and resource redundancy processes begin in the same order, starting with the most radicalized agent first. Each *Agent* looks to see if the knowledge and resource accessed by *Agent* have some measure of redundancy. First, *Agent* looks at its own knowledge and sees if any neighbors also have this knowledge. If so, *Agent* does nothing. If not, *Agent* adds the neighbor with the highest radicalization score less than $Agent_{Radicalization}$ not yet linked to any other nodes this round. *Agent* then executes essentially the same for resources.

Now back to the radicalization process itself. As previously stated, radicalization is a function of time in the network, the intensity of the beliefs, and the agents connectivity within the network. Of these variables, time in the network is constantly increasing as long as the agent survives. This positively influences the agents' commitment to the group, although there is probably an upper limit to this effect.

Connectivity within the network is dictated by the interplay of losing members, recruitment of new members, and the increasing connectivity of the network over time. For experimentation purposes, all existing members of the dataset need an initial time stamp. Since terrorism is also a social endeavor, the more connected a member the more radical that member may become over time. Belief intensity can be variable or fixed, but is also a function of radicalization itself. This cyclical relationship is somewhat problematic, and future research must account for this. One way is to make beliefs fixed over the course of the experimentation, while another is to recalculate belief intensity after each round. This leads to our new formula for radicalization but also establishes a need to develop a formula for belief intensity adjustments over time:

$$Radicalization = \log 2(Agent_{Time} + 1) + Agent_{Belief} \times Agent_{K}$$

METHODOLOGY

The research question of how terrorist groups survive requires analysis and testing of an actual terrorist network incorporating the social, knowledge, and task networks associated with that terrorist organization. In addition to establishing a baseline with network analysis metrics, the data must have the opportunity to change over time according to an established model, both before and after attacks simulated by removing nodes. The primary visualization tool for this research is the Organizational Risk Analyzer (ORA) from the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. The primary analysis tool is the multi-agent model described in **Error! Reference source not found.**.

The actual conduct of the experimentation proceeds in a multi-step iterative process and follows a similar methodology utilized by Najara and Anderson.[87] First, the experimentation group is "baselined" in its initial organizational structure and analyzed using the ORA analysis and report generating tools in order to compare the organization to future evolutions. The baseline meta-network then runs through an iterative series of evolution, attack, and adaptation simulations. During the evolution phase, the dataset "evolves" using the multi-agent model to advance the organization over three time simulations, resulting in a new network based on the current network structure. Upon completion of this evolution phase, the social network (Agent-to-Agent) is "attacked" using a degree-centrality attack instead of a random attack in order to simulate kinetic and non-kinetic counterterrorism operations. A degree-centrality attack targets the node or agent with the most links (known as the degree *K* of a node), whereas random attacks target any node. The attack removes the two lowest degree *K* nodes from the network, effectively destroying them. Additionally, the node with the third highest degree *K* is also destroyed in order to simulate high-value targeting. The choice of eliminating the third highest degree node may appear arbitrary but is based on the assumption that the most connected node in a terrorist network is not typically exposed due to task

[87] Nagaraja and Anderson, "The Topology of Covert Conflict," 7.

saturation (meaning that they are too busy coordinating operations to be out in the open), as is the second-most connected node. Despite the ability of the network to evolve, it is possible that targeting either the first or second highest degree nodes (as opposed to the third highest) will cause discernible changes in the results. However, this is not likely to alter the overall conduct of the experiment after the initial attack rounds since the most connected node is not static due to the evolution process. Following the attack phase, the social network (Agent-to-Agent network) is allowed to add the number of nodes equal to the number of nodes lost, connected to the second lowest degree node to simulate recruiting.

This assumption of attack and replenishment as a zero-sum game is intended to simulate the real-world observations of terrorist group replenishment with the understanding that recruits start at the bottom and work their way "deeper" into the organization over time based on survival and trust. Each of the new recruits is linked to the secondary belief (Belief number 1: Bombing is a legitimate act) and one of the three is linked to the core Belief in the Agent-to-Belief network (Belief number 2: The United States is the Enemy). This selective use of "believers" is intended to allow for some members of an insurgency or terrorist group to be "opportunists" more interested in gaining advantage but allows for radicalization over time. Upon completion of the replenishment phase, the entire process is repeated for a number of iterations to be determined or until the network collapses. While this may seem to be a methodological "cheat" in order to extend the experimentation, the inverse of this is counterproductive. The notion that the network can be destroyed if the attacking forces can kill more terrorists than can be added to the network goes without saying. As a result, any methodology that degrades faster than it replicates is guaranteed to destroy the network eventually. Since this experimentation is primarily focused on the evolution of the network and the effect of the overall structure in light of attacks, the one-for-one growth is essential to get at the heart of the research question. Subsequent research should experiment with higher rates of recruiting once a general principle of organizational replication under attack is inferred from this research.

ANALYSIS

"No Evolution" Testing

In order to establish a point of departure for results, the first testing set did not employ the multi-agent model algorithm. Instead, this "No Evolution" round of testing only used the established test procedure described in the Methodology section. After sorting the nodes by greatest value *K*, the two lowest degree nodes and third highest degree nodes were eliminated. Three new nodes were inserted into the network, one onto each second lowest *K* value nodes as a two-way connection.

As expected, the inability to evolve the network led to a rapid degradation in the connectivity and performance of the network. The network lost agent access to numerous Knowledge and Resource nodes by Round 4, and the network effectively collapsed by Round 5. These results are hardly surprising given the static nature of the network, which did not allow for continued growth within the network amongst members. Any organizations mimicking the behavior of the "No Evolution" test procedures should expect rapid disruption to the point that the organization is no longer functioning. Rapid agent attrition in a compressed timeline, such as a series of simultaneous attacks on the organization, would likely mimic these testing results.

Static Belief Iteration

This iteration of testing employed both the established testing procedure and the multi-agent model algorithm. Each testing round consisted of three evolution rounds whereby the meta-network calculated the current radicalization index for each agent, evolved the agent-to-agent network, and then ran the knowledge and resource redundancy procedures. Upon completion, the test "killed" the two agents with the lowest value *K* and agent with the third highest value *K*, just as the "No Evolution" testing iteration. Based on the ability of the network to consistently generate new connections based on the radicalization threshold, the expected result of this testing would be a sustained but changing network structure. This iteration ran for ten rounds with 30 complete network evolution procedures.

Unlike the first iteration of testing, the meta-network in this iteration maintained the overall network structure for the entire testing run. By Round 10, the network suffered from minimal Knowledge and Resource losses. Additionally, the network successfully integratied new members into the structure to the degree that an agent added to the original dataset had exceeded the radicalization threshold and was eligible to generate new links. Because of the tendency for the most radicalized members to associate with each other as their other neighbors "died," the agents eligible for radicalization formed an internal network cluster that began to resemble an all-channel cluster as testing persisted. One side effect of this was the tendency for Knowledge and Resources to also cluster within these agents who could only pass link their Knowledge and Resources to each other or new agents linked to them, which had detrimental effects to the organization over the long term. As testing eliminated agents within the cluster, Knowledge became increasingly concentrated because the cluster invariably contained the most connected agents within the network. By the end of the Attack phase of Round 10, one agent became a single point of failure for several knowledge and resources. Had the testing persisted beyond Round 10, one could expect the meta-network to lose access to several Knowledge and Resource nodes, thereby disrupting the network's functionality.

The clustering of Knowledge and Resources also implies an increasingly centralized command structure due to the fact that only a few key nodes had the access required for operations. This clustering is directly attributable to the designated radicalization threshold *RadThresh*. In the interest of balancing the need for data with the burden of manipulating the network manually, *RadThresh* was set to a higher value (*RadThresh* = 6 for all testing iterations) in order to provide for a restrictive case. A lower *RadThresh* would have allowed several more agents to make additional links in each round, thereby increasing the interconnectivity and resilience of the network. While a real-world organization can decide to change its own notion of "how radical is radical enough?" in light of counterterrorist operations, this model used a fixed value for the entire testing run. The inability to expand the number of links based on the radicalization threshold explains for cluster formation with a monopoly on Knowledge and Resources.

Belief Intensification Iteration

The second iteration of testing utilizing the multi-agent model modified the test procedure in order to test the effect of changing belief intensity. Since radicalization is a process based on time, connectivity, and belief intensity, each round of testing modifies the radicalization index of each agent. Since duration in the network always positively impacts the radicalization index over time, the radicalization trends are entirely predictable when belief intensity and connectivity are fixed. However, connectivity is the one factor within this experimentation that changes almost continuously. As a result, an agent's radicalization index may wax and wane based on their connectedness at any given moment. This is all well and good until one moves the testing out of the abstraction of data and into the reality of what agent removal means. If the loss of an agent has any impact on their neighbors' belief intensity, the original testing procedure does not account for this. As a result, a testing procedure that allows for a change in belief intensity could be instructive on the impact of counterterrorism on the remaining members.

This iteration of testing modified the test procedure to change the belief intensity based on losses. For each neighbor killed in a given attack round, an agent's belief intensity for Belief 2 (The United States is the Enemy) increased by a value of 0.05 with a maximum value of 1.0. This assumes that the affected agent is more likely to harden their beliefs as neighboring agents die off. While the overall radicalization of an agent may drop in the short term since his connectivity K diminishes, belief intensity increases which allows for greater radicalization in the long term. Under this testing regime, one would expect the overall radicalization of the network to be higher than in the static belief testing iteration. This in turn should lead to more agents meeting the global radicalization threshold in earlier testing rounds.

The results of the data manipulation challenged the notion that new agents would radicalize more quickly than under a static belief system. Since new agents only have one connection, the loss of a neighbor may intensify their beliefs but also completely disconnects them from the network and causes their elimination in the next attack round. The only way for a newer agent to gain connections is for them

to be the second lowest value *K* node during the agent recruiting phase, which is possible when several agents with *K*=0 exist in the network after the attack phase. The belief intensity of the existing agents within the network with multiple connections did increase as their neighbors died, and the overall radicalization factor of the network (defined simply as the sum of each agent's radicalization index) was 6% greater than the radicalization factor of the static belief testing iteration.

Since this iteration did not greatly increase the ability of new agents to meet or exceed *RadThresh*, the overall results of this testing iteration were similar to the static belief iteration with regards to network connectivity. The meta-network suffered several Knowledge and Resource node access losses by the end of Round 10, and continued network attacks would likely collapse the system. The fact that no new agent ever met the radicalization threshold is in part attributable to the fact that when more than two nodes had the second lowest value of K, selecting which agent to connect the new agent was random.

Cluster Growth Iteration

During the process of data manipulation, one aspect of terrorist recruitment not accounted for was the fact that terrorists tend to join in groups as opposed to individuals.[88] All testing iterations up to this point ignored this option. To account for this, a new testing iteration that recruits clusters of individuals was required. Under this test procedure, one node attaches to the second-lowest value *K* node while two other nodes already connected to each other are *both* linked to the next second-lowest value *K* node. This should have the effect of radicalizing the "recruiter" of the cluster faster than the single-node recruiter, as well as allowing the new nodes to radicalize faster than their non-clustered peers. Beliefs were also adjusted based on agent loss as described in the previous testing iteration.

After the second round of testing, a surprising trend emerged in that the "recruiters" of the newer clusters were typically agents contained within a cluster added during the previous round. This was due

[88] Sageman, Understanding Terror Networks, 107.

to the fact that they had only two links and were therefore the second lowest value *K* nodes. In a real-world scenario, a terrorist group might be reluctant to allow its newest members to recruit, but these members may in fact be the agents with the most access to outside agents as the group membership becomes more exclusive of the outside world. One possible variation on this routine is to forbid a member from recruiting for a given amount of time, but this research made the selection at random. On subsequent rounds, the most recently added agents typically recruited the next generation. Ironically, the original membership (while it survived) began to lose access to the newer members since they were never the second-lowest value *K* nodes, suggesting the group as a whole may diffuse into a new organization over time. However, the core group maintained access to many key Knowledge and Resource nodes. Since they were unable to add new connections, they were unable to transfer access to these nodes to new members, causing a much earlier loss of several Knowledge and Resource nodes (by Round 3). The lower-ranking members in the original data set preserved the surviving Knowledge and Resources and thereby became the "new core" of the group. Despite the loss of Knowledge and Resources, new Agent nodes met *RadThresh* by Round 8 (although the first agent to do so died in the next attack phase).

Data Trends Analysis

The testing conducted in the control iteration and three experimentation iterations confirms the notion that models are best suited to trigger better questions, as opposed to finding answers. None of the experimentation duplicates perfectly what a real-world terrorist organization might do in similar circumstances, but the experimentation does trigger new questions as well as reinforce earlier notions. For those concepts reinforced by the model, the model provides a helpful way of simulating the behavior in future research, so long as the limitations of the model are explicitly acknowledged and challenged.

First, the testing iterations using the radicalization process demonstrated a workable model of the "echo-chamber" effect, whereby groups become more radical through interconnection and duration in the cluster. For all experimentation runs, the radical core tended to become more radical with increased interaction. Closely linked to this is the idea that increasing radicalization increases connectivity within the most extreme elements.

The model also confirms the idea that terrorist groups under attack must continuously work to protect and generate knowledge and resources. While the model does not provide for the introduction of new resources, it does demonstrate that an organization under attack must constantly spread knowledge and prevent so-called single points of failure whose removal cripples the network. Additionally, the model effectively simulates the phenomenon whereby clusters become isolated from the main meta-network. Since the loss of these Knowledge or Agent clusters poses an organizational dilemma, counterterrorist officials should pay special attention to any opportunity to isolate portions of the organization from the main organization. Although certain clusters may be able to operate effectively without the main organization, especially those clusters operating in a cellular network structure, the continued effectiveness of a cluster after isolation may give helpful clues into the overall structure of the main network.

As useful as the confirmations just discussed may be to counterterrorist officials, the questions generated by the model are more interesting and provide insight into future research. The most important question is the notion of a threshold for radicalization. At what point does a terrorist organization think a member is trustworthy enough to bring new people into the organization, gain greater responsibility, or access critical knowledge and resources? As shown in the testing, a higher value *RadThresh* limits the meta-network's ability to evolve over time, whereas a lower value allows considerably more flexibility. Variations on this testing could also lower the threshold under times of effective disruption by counterterrorism officials or even assign each member their own notion of *RadThresh* when assessing possible links. Like the model itself, this exercise will in no way duplicate a real-world organization's behavior but it could provide trends or insights into crossover points when the organization transforms into a new structure.

Another source of questions is the operationalization of radicalization. The equation used for radicalization should trigger heated debate and further research, and an optimal outcome of any discussions stemming from this present research is a refined operationalization. Whatever form this operationalization takes, it should account for time, belief intensity, and network connectedness. No one

factor by itself can dominate the process of radicalization completely. The positive effect of time diminishes the longer the Agent is in the network, as demonstrated by Table 1. Simply adjusting beliefs or adjusting links by themselves does not radicalize as quickly as when these factors are adjusted simultaneously. The belief intensity still has the most significant influence on radicalization, but it still needs time and connectivity (although higher belief intensity diminishes the importance of connectivity). In experimentation, Agent 7 (Osama bin Laden) was rarely the most connected agent but was consistently within the top three for radicalization due to belief intensity. In the Static Belief testing iteration, the fact that he was typically the second or fourth highest degree *K* agent probably contributed to his long term survival.

Table 1: Radicalization by Time, Connectivity (K) and Belief Intensity

	Radicalization by *Time*									
Time	1	4	7	10	13	16	19	22	25	28
K	4	4	4	4	4	4	4	4	4	4
Belief	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Radicalization	0.4	2.4	3.2	3.7	4.1	4.4	4.6	4.9	5	5.2

	Radicalization by *K*									
Time	8	8	8	8	8	8	8	8	8	8
K	2	3	4	5	6	7	8	9	10	11
Belief	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Radicalization	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	4	4.1

	Radicalization by *Belief*									
Time	8	8	8	8	8	8	8	8	8	8
K	4	4	4	4	4	4	4	4	4	4
Belief	0.1	0.2	0.2	0.3	0.3	0.4	0.4	0.5	0.5	0.6
Radicalization	3.4	3.6	3.8	4	4.2	4.4	4.6	4.8	5	5.2

The notion that losing neighbors intensifies beliefs is another source of questions. The Dynamic Belief testing iteration increased belief intensity whenever an Agent lost a neighbor in order to simulate

the increased anger and resentment stemming from such a loss in real-world counterterrorism operations. Since this testing used an arbitrary value of 0.05 for every single member, the results must be viewed with the notion that a larger impact on beliefs increases radicalization at a much higher rate. The level of belief intensification likely varies from person to person based on their familiarity with the neighbor and frequency of interaction based on shared tasks, resources, and common interests. Ultimately, this may be impossible to quantify, especially if the agent killed is a family or close relation.

The final question generated by the testing results gets to the heart of the original research question of "How to terrorist groups survive?" In the final testing iteration, the core group became increasingly isolated from the emerging organization. This suggests that the core retains vitality by linking to newer members or by bringing agents meeting *RadThresh* into the core. The Cluster Growth iteration model of testing suggests that this process is more difficult when clusters join the group. Since real-world counterterrorist operations do not routinely capture or kill top-tier agents such as bin Laden or al-Zawahiri, the core in these groups probably does not keep losing members and is therefore able to survive long enough to make those connections. However, in the event of high attrition of senior members in the manner described in the testing procedures, the organization seems to shift rapidly towards a newer core group. The cluster growth iteration is the youngest data set, measured by the combined time factors of each agent, shown in Figure 8. This trend may duplicate itself in real-world terrorist organizations undergoing sustained attrition levels. However, the cluster growth iteration also demonstrates a consistent inability to link the older members of the organization to the newer members and also demonstrates a gradual decline in capabilities over time, suggesting that groups showing this pattern may be vulnerable to schism or targeted isolation.

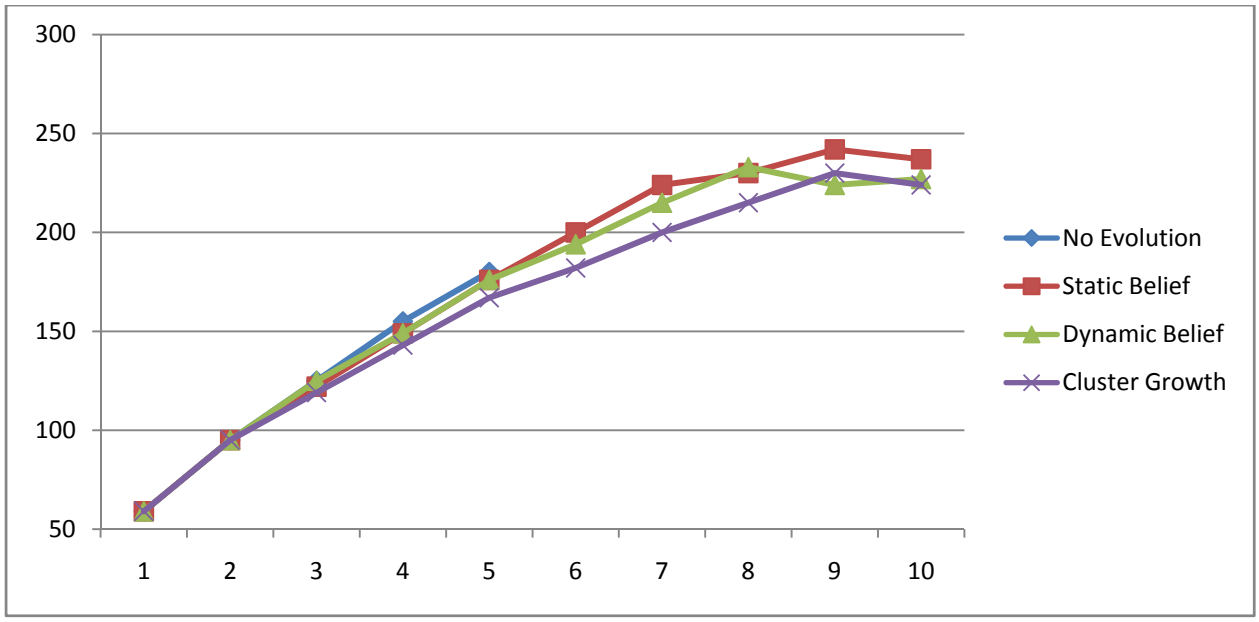

Figure 8: Age by Round

FUTURE RESEARCH

As discussed in both the methodology and theory chapters, this experimentation does not provide a complete understanding of the dynamics in terrorist organizational evolution. Future experimentation may challenge several of the findings. Therefore, the author recommends four additional research programs below in order to provide a more complete understanding of the dynamics of terrorist meta-networks. Each of these research programs flow from previous theoretical discussions as well as the implications and potential of multi-agent modeling. While the ideal research program simultaneously integrates and tests all of these research programs, each program requires individual testing first in order to establish baseline performance.

New Tasks

Real-world organizations routinely acquire or execute new tasks for a variety of reasons. Executing new tasks is also a major rationale for organizational change since these tasks typically dictate new knowledge, resource, and agent requirements. Since this current research did not change the tasks the network sought to accomplish, it does not capture the dynamics of task-based organizational change. While the core hypothesis tested in this research monograph would likely remain valid, studying the organizational evolution of gaining new tasks would likely provide more robust findings as well as highlight opportunities of organizational weakness for counterterrorism exploitation.

New Locations

In addition to conducting new tasks, real-world organizations routinely acquire new locations: al Qa'ida was already a global entity prior to the Tanzania bombing and continues to operate in locations across the globe, as required. Adding new locations also drives the acquisition of new resources and new knowledge. Future testing using the methodology in this research should add new locations in two separate simulation iterations. The first iteration should study a single agent as a "recruiter" in the new location, and the second iteration should analyze the effects of sending a fully formed cell to a new

location. Much like the potential findings of adding new tasks, this new research would likely expand on the findings of this monograph and provide some insight into organizational vulnerabilities while organizations expand geographically. This testing could also test the hypothesis that organizations such as al Qa'ida need to move into new locations in order to survive.

Mergers and Combined Action

If the history of al Qa'ida is any indication, terrorist organizations routinely combine forces or merge, such as Ayman al Zawahiri's merger of Egyptian Islamic Jihad into al Qa'ida in the 1990s. This merger had profound impact on al Qa'ida, most notably in the form of al Zawahiri emerging as bin Laden's most visible lieutenant, and eventually resulted in a wholly new organization. Another form of organizational change is the addition of so-called al Qa'ida affiliates, such as al Qa'ida in the Maghreb (AQM), which are existing terrorist organizations that join al Qa'ida as a whole in return for global legitimacy, training, guidance, and resources.[89] Studying the effect of mergers could lead to a deeper understanding of the organizational dynamics of how one organization dominates another in such mergers. A more interesting research question revolves around whether there are conditions in meta-networks that preclude such a merger. Although not a terrorist or covert organization, examining the failure of the Daimler-Chrysler merger using meta-networks could provide several insights into this question. This research program might challenge some of the findings in this monograph if the organizational ideology is not binding to the degree that it can overcome the inevitable friction of combining organizational cultures, in which case the ideology may be more specific.

Robust Financial Networks

One shortcoming of this current research is the short shrift given to financial resources. Since financial networks are networks in their own right, researchers should leverage existing information from financial counterterrorism operations to study the impact of the evolution of these networks over time on

[89] Jones and Libicki, *How Terrorist Groups End,* 115.

the larger meta-network. This research could provide valuable insights for future financial interdiction as well as the social network evolution that follows from shifting financial resources from one particular mode to another. The Taliban's growing reliance on poppy production offers one example.

Multi-Agent Modeling Software

The findings presented in this research are based on the multi-agent model proposed in the modeling chapter. While this algorithm could be easily programmed to execute the required data manipulation, the author manipulated the data in a series of Microsoft Excel spreadsheets. The primary reason behind this decision was a need to avoid programming delays, since as all computer programmers can tell you, all software projects spend 50% of their time being 90% complete. Multi-agent modeling software such as *NetLogo* or *Repast Symphony* abound on the Internet, but time and training necessitated a time-expedient solution. Therefore, future research should run this exact same data experimentation (with multiple repetitions to gain statistical insight) with a fully automated version of the original algorithm and various test procedures in order to verify the manual work presented here. This automated model should contain the tunable parameters presented in the experimentation. Additionally, the model must move from the current linear algorithmic approach to a true multi-agent model. The version presented is similar to game-theoretic approaches. How best to go about translating a game-theoretic approach into a truly independent multi-agent model is up for debate.

Datasets

A major limitation of most counterterrorism research is the dearth of datasets. While several datasets have gained in sophistication and depth since 2001, many are insufficient for the research programs described in this section. As such, terrorism researchers and government counterterrorism officials should work closely to declassify more terrorist data and convert this information into meta-networks as described in the theory section of this monograph. Fortunately, this data does not necessarily need to be on contemporary terrorists groups such as al Qa'ida. A group that has effectively ceased to

operate could provide an ideal dataset, as long as the data reflects the changes over time. Data on organized crime may also work in this regards since these groups share many similarities with covert groups.[90]

[90] Erickson, "Secret Societies and Social Structure," 189.

CONCLUSION AND RECOMMENDATIONS

Conclusion

At this point, one must return to the original hypothesis of this research to determine whether this endeavor was fruitful. The hypothesis established in the Theory section states the following: *Terrorist organizations that sustain their core ideology will survive as long as some number of recruits linked to the core ideology advance within the organization.* To prove the hypothesis, we first must show that terrorist groups can sustain themselves as long as new members are able to advance within the network to the degree that the network structure is sustainable. In those testing iterations using the multi-agent model, the terrorist groups did not collapse during the observed data runs. However, each of these networks would likely collapse in subsequent rounds. Under the model presented in this research, agents must meet a certain radicalization threshold *RadThresh* in order to begin adding links to the organization. This value is global and arbitrary, meaning that a lower level would have sustained the network for a longer time. Therefore, the hypothesis holds for a radicalization index that enables new connections and is therefore not an unconditional statement.

The opposite case should also hold true for the hypothesis to be true, in that if the beliefs are not maintained then the group will eventually collapse. The agent's radicalization index also serves as a form of internal ranking within the organization. Radicalization is a function of time (which always increases), connectedness measured by *K* (which is variable based on properties of the network itself), and belief intensity (which is variable based on external data or internal network structure changes in some experimentation instances). Radicalization therefore increases when all variables increase, and decreases when *K* and belief intensity decrease. Since terrorists not linked to any other agents are of minor concern to security officials, belief intensity changes are central to the durability of terrorist organizations. Table 2 and Figure 9 show the effect of decreasing beliefs on the *RadIndex* over time with a fixed value *K*. In each time stamp, *Belief* decreases by 0.05. The *RadIndex* increases up to *Time* = 20 and then declines

gradually. Depending on the global value of *RadThresh*, this agent would likely be unable or increasingly unable to make new links, thereby preventing network growth in the face of continued attrition.

Table 2: Radicalization over time with fixed *K* and decreasing Belief Intensity

	Decreasing Beliefs Over Time																				
Time	1	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
K	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Belief	1	0.95	0.9	0.85	0.8	0.75	0.7	0.65	0.6	0.55	0.5	0.45	0.4	0.35	0.3	0.25	0.2	0.15	0.1	0.05	0
Radicalization	3	3.85	4.7	5.13	5.4	5.57	5.68	5.76	5.8	5.82	5.82	5.81	5.78	5.75	5.71	5.66	5.6	5.54	5.47	5.4	5.32

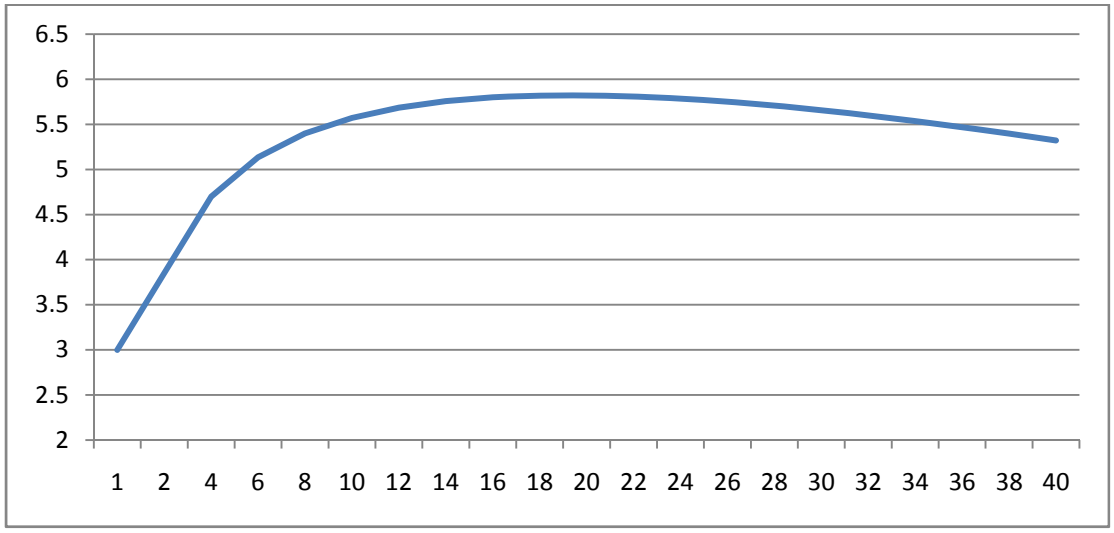

Figure 9: Radicalization over time with fixed *K* and decreasing Belief Intensity

A caveat remains with this statement. Even if belief intensity is set to zero, the effects of time and connectivity eventually will increase radicalization again. Figure 10 shows the same data extended 50% longer. This suggests a certain measure of path dependency for terrorist organizations committed to fighting more than their cause, assuming they survive the period where the agents fail to make new connections. Galula reminds us that cause diminishes over time,[91] and groups such as FARC give credence to this notion. At this crossover point it may be prudent to reassess the group's actual core beliefs as opposed to their professed beliefs. However, this also gets to the attractiveness of the ideology.

[91] David Galula, *Counterinsurgency Theory and Practice*, (St. Petersburg, FL: Hailer Publishing, 1964): 25.

If the members of a group no longer believe in the stated ideology, then it is likely to be difficult to recruit using that ideology.

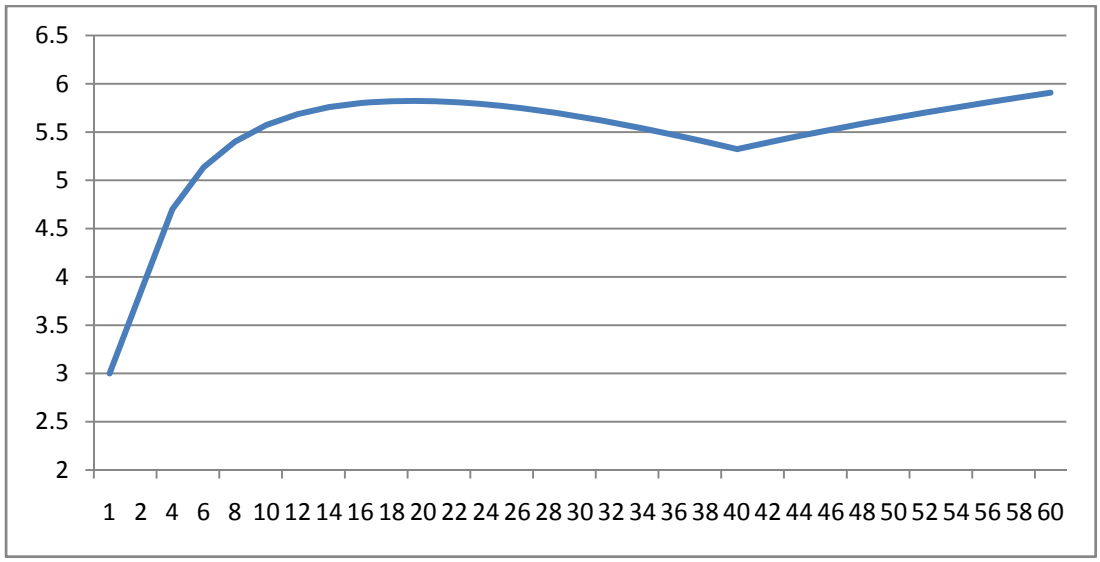

Figure 10: Sustained Radicalization over time with fixed K and decreasing Belief Intensity

Therefore, since the data testing demonstrates that terrorist groups can sustain themselves as long as new members join (since they will eventually integrate into the network) and the properties of the Radicalization demonstrate that decreasing belief intensity lowers radicalization, the hypothesis holds.

Recommendations

While research of this nature works extraordinarily well in the mathematical sense and helps build better models, counterterrorism research must offer something back to the community of practice. As such, several recommendations emerge from the results. These recommendations fall into the vague categories of things for counterterrorist officials to look for and things for them to do.

The first aspect to examine is the emergence of a new organization following massive attacks. The dynamic nature of modern terrorism lends itself towards rapid reorganization and reconstitution following catastrophic losses. The fact that al Qa'ida in Iraq persists shows the durability of these organizations. Al Qa'ida in Iraq and the al Qa'ida Central Core also show an interesting dynamic of how

a new organization may eventually dominate the existing organization. One could argue that al Zawahiri's intercepted rebuke of al Zarqawi was also intended to prevent him from becoming the most visible face of the al Qa'ida brand.

In terrorist organizations built around an increasingly isolated core group, the difficulty in passing access to knowledge and resources disrupts operations. Since the testing in the final run indicates that these groups maintain vitality by linking to newer network clusters, we can expect them to assert control over these network additions. Therefore, intelligence officials should study how a targeted group is passing access to knowledge and resources to agents in the field. Since this isolation of the group with access to resources and knowledge leads to centralization of command and control, counterterrorist officials should expect an increase in communications attempts between isolated cells. If the agents in the field suddenly gain new capabilities, it could serve as an indicator that the group either has managed to pass resources effectively or is generating new resources.

This research indicates the importance of new recruiters in sustaining the organization. While recruiting in modern terrorism is rarely a "top-down" affair, counterterrorism officials may be able to exploit or disrupt an organization by focusing targeting efforts on low-level potential recruiters in order to slow overall recruiting and weaken the organization, especially after attacks by counterterrorism forces. These low-level recruiters may also become the seeds of "spin-out" organizations from the main group.

Aside from intelligence opportunities, some concrete steps against terrorist groups emerge from this research. The first and most critical is to militarily operationalize radicalization. While the equations used in this research are probably not entirely appropriate and too mechanistic for real-world use, a methodology for determining agent radicalization would likely benefit intelligence analysts focused on specific terrorist networks. This leads to the next recommendation, which is to update current doctrine to militarily operationalize meta-networks for targeting and assessment. While some aspects of networks based on the PMESII construct should inform these meta-networks, intelligence operatives cannot rely exclusively on PMESII due to the lack of emphasis on dynamics and the vague nature of the categories themselves. These networks should include not only the Agent-to-Agent network but the Agent-to-

Knowledge, Agent-to-Resources, Agent-to-Tasks, and Agent-to-Beliefs. Beliefs mapping onto a meta-network provides a logical framework for information operations development and effectiveness assessments. Additionally, although funding is a type of resource, intelligence analysts should treat financial networks as a separate meta-network linked to the main terrorist network due to the intricacy and interconnectivity of the global and Islamic banking systems.

The research results also imply some doctrinal adjustments for joint and Army doctrine, mostly in terms of approach. Current doctrine emphasizes network structure instead of dynamics and processes; by analyzing measures such as closeness and betweeness, intelligence prediction is based on artifacts and consequences of enemy dynamics. Targeting highly connected nodes does not necessarily lead to network collapse without an understanding of the nature and dynamics the links are meant to represent. A network analysis on a U.S. Army infantry battalion would likely show the battalion chaplain as the most connected node due to his or her ability to interact with every soldier in the unit. However, the loss of the chaplain is not likely to disrupt operations for that battalion. The irony of the structural approach in doctrine is that network analysis is supposed to be embedded in Joint Intelligence Preparation of the Operational Environment (JIPOE), a process which also focuses on what an enemy is supposed to do. By building analysis around static networks with no regard of the dynamics, decision makers are left without an understanding of the functionality of the organization represented by the network. Networks are merely abstractions of real organizations that actually perform actions. Joint doctrine is especially prone to this error due to the incorporation of System of Systems Analysis approaches into recent operations and intelligence doctrine.[92] Predictive intelligence based on a structural approach to networks is a fallacy destined to lead to failure.

Finally, the testing demonstrates that targeting high-payoff targets has value but that this value must not be overstated. In those organizations where control of certain resources and knowledge is

[92] Joint Concept Development and Experimentation Directorate, *Commander's Handbook for an Effects-Based Approach to Operations*, (Joint Warfighting Center, 2006), II-2. The diagram depicted in figure II-1 demonstrates a remarkable similarity to Figure III-2 in JP 5-0.

centralized, attacking key individuals has tremendous effect in disrupting the organization. Conducting these attacks simultaneously or in rapid succession has the potential to destroy the network by breaking agent links, disrupting the radicalizing effect of the “echo chamber”, and denying access to resources and knowledge. These attacks remain the “gold standard” of modern counterterrorism, but the difficulty in conducting these attacks against multiple agents at the same time means that they cannot be relied upon in the day-to-day fight. As long as a group is growing internally and attracting new members based on the attractiveness of their ideology, then the group will likely survive. As a result, the ultimate solution in counterterrorism still lies in coordinating kinetic attacks against irreconcilable agents while simultaneously attacking the specific belief structure that serves as the core of the radicalization process.

BIBLIOGRAPHY

Books

Arquilla, John, David Ronfeldt, and Michell Zanini. "Networks, Netwar, and Information Age Terrorism." *In Countering the New Terrorism*, eds. Ian O. Lesser et al., 39-84. Santa Monica, CA: RAND Corporation, 1999.

Barabási, Albert-Lásló. Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life. New York: Plume, 2003.

Jones, Seth G., Martin C. Libicki. *How Terrorist Groups End: Lessons for Countering Al Qa'ida*. Santa Monica, CA: RAND Corporation, 2008.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. St. Petersburg, FL: Hailer Publishing, 1964.

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

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Watts, Duncan J. *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton and Co., 2003.

Periodicals and Articles

Albert, Réka and Albert-Lásló Barabási. "Statistical Mechanics of Complex Networks." *Reviews of Modern Physics*. Vol. 74 (January 2002): 47-97.

Albert, Réka, Hawoong Jeong, and Albert-Lásló Barabási. "Error and Attack Tolerance of Complex Networks." *Nature 406*, No. 6794 (July 27, 2000): 378-382.

Carley, Kathleen M. "Inhibiting Adaptation." *Proceedings of the 2002 Command and Control Research and Technology Symposium*. Monterey, CA: Naval Postgraduate School, 2002.

Carley, Kathleen M. "Estimating Vulnerabilities in Large Covert Networks." *Proceedings of the 8th International Command and Control Research and Technology Symposium Conference.* Washington DC: National Defense War College, 2003.

Carley, Kathleen M. "Destabilization of Covert Networks." *Computational and Mathematical Organization Theory 12*, No. 1 (April 2006): 51-66.

Carley, Kathleen M., Jeffrey Reminga, and Natasha Kamneva. "Destabilizing Terrorist Networks." *Proceedings of the 8th International Command and Control Research and Technology Symposium*. Washington DC: National Defense War College, 2003.

Crucitti, Paolo, Vito Latora, Massimo Marchiori, Andrea Rapisarda. "Error Tolerance of Complex Networks." *Physica A*. No. 340, (2004): 388-394.

Dodds, Peter Sheridan, Roby Muhamad, and Duncan J. Watts. "An Experimental Study of Search in Global Social Networks." *Science*, Vol. 30 (August 18, 2003): 827-829.

Dodds, Peter Sheridan, Duncan J. Watts, and Charles F. Sabel. "Information Exchange and the Robustness of Organizational Networks." *Proceedings of the National Academy of Science of the United States of America*, Vol. 100, No. 2 (October 14, 2003): 1-19.

Erickson, Bonnie H. “Secret Societies and Social Structure.” *Social Forces*, Vol. 60, No. 1 (September 1981): 188-210.

Hanaki, Nobuyuki, Alexander Peterhansl, Peter S. Dodds, and Duncan J. Watts. “Cooperation in Evolving Social Networks.” *Management Science*, Vol. 53, No. 7 (July 2007): 1036-1050.

Holme, Petter, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. “Attack Vulnerability of Complex Networks.” *Physical Review E*, Vol. 65, Issue 5, (May 7, 2002), 1-15.

Latora, Vito, and Massimo Marchiori. “Efficient Behavior of Small-World Networks**.”** *Physical Review Letters*, Vol. 87, No. 19 (November 5, 2001): 1-4.

Mitchell, Melanie. “Complex Systems: Network Thinking.” *Artificial Intelligence*, Vol. 170, Issue 18 (December 2006): 1194-1212.

Moon, Il-Chul, Kathleen M. Carley. “Locating Optimal Destabilization Strategies.” *Proceedings of ICCRTS. Newport, RI (Jun 19-21, 2007).*

Moon, Il-Chul, Kathleen M. Carley. “Modeling and Simulating Terrorist Networks in Social and Geospatial Dimensions.” *IEEE Intelligent Systems 22*, No. 5 (September/October 2007): 40-49.

Moon, Il-Chul, Kathleen M. Carley, and Alexander Levis. “Vulnerability Assessment on Adversarial Organization: Unifying Command and Control Structure Analysis and Social Network Analysis.” *Proceedings of the SIAM International Conference on Data Mining, Workshop on Link Analysis, Counterterrorism and Security*. Atlanta, GA: April 26, 2008.

Nagaraja, Shishir, and Ross Anderson. “The Topology of Covert Conflict.” *University of Cambridge Computer Laboratory Technical Report*, No. 637 (July 2005).

Newman, M. E. J. “The Structure and Function of Complex Networks.” *SIAM Review*, Vol. 45, No. 2 (June 2003): 167-256.

Reed, Brian. A Social Network Approach to Understanding an Insurgency. *Parameters: U.S. Army War College Quarterly*, Vol. 37, No. 2 (Summer 2007): 19-30.

Ressler, Steve. “Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research.” *Homeland Security Affairs*. Vol. 2, No. 2 (July, 2006): 1-10.

Strogatz, Steven H. “Exploring Complex Networks.” *Nature 410*, No. 6825 (March 8, 2001): 268-276.

Tsvetovat, Maksim. and Kathleen M. Carley. “Bouncing Back: Recovery Mechanisms of Covert Networks.” *Proceedings of the 2003 North American Association of Computational Social and Organization Science*. Pittsburgh, PA: Carnegie Mellon University, 2003.

Tsvetovat, Maksim, Kathleen M. Carley. “On Effectiveness of Wiretap Programs in Mapping Social Networks.” *Computational and Mathematical Organization Theory 13*, No. 1 (March 2007): 63-87.

Watts, Duncan J., Peter Sheridan Dodds, and M. E. J. Newman. “Identity and Search in Social Networks.” *Science*, Vol. 296, No. 5571 (May 17, 2002): 1302-1305.

Watts, Duncan J., Steven H. Strogatz. "Collective Dynamics of 'Small-World Networks." *Nature*, Vol. 393 (June 4, 1998): 440-442.

Government Documents

Combating Terrorism Center at West Point Harmony Database. “Summary of Zawahiri’s Letter to Zarqawi.” United States Military Academy. http://ctc.usma.edu/aq/pdf/Zawahiri-Letter-Summary.pdf, (accessed January 15, 2009).

Joint Concept Development and Experimentation Directorate. *Commander’s Handbook for an Effects-Based Approach to Operations*. Joint Warfighting Center, 2006.

Joint Publication 5-0, *Joint Operation Planning*. Washington, DC: Government Printing Office, 2006.

Joint Publication 3-24, *Counterinsurgency Operations* (Revision First Draft), 2008.

U.S. Army Field Manual 3-24, *Counterinsurgency*. Washington, DC: Government Printing Office, 2006.

Theses, Monographs, and Unpublished Works

Henke, Glenn A. “Small-World Topology Networks: Predicting the Balance Between Resiliency and Security.” Kansas State University Security Studies Master’s Degree Terminal Paper (Unpublished, 2008).

Software

Organizational Risk Analyzer, version 1.9.5.3.3. Kathleen M. Carley, Carnegie Mellon University CASOS, January 2009. (http://www.casos.cs.cmu.edu/projects/ora/)

Tanzania Embassy Bombing Data Set. Carnegie Mellon University CASOS, 2006. (http://www.casos.cs.cmu.edu/computational_tools/datasets/internal/embassy_2006/index2.html)

Appendix 1: Multi-Agent Model

```
// Initialize this round of evolution //

    // Radicalize Agents and sort Agent list by RadIndex, with most radical agent first //
    FOR each Agent DO
        Radicalize (Agent)
    END
    {Sort Agent list (Max to Min Radicalization Factor)}

    // Advance the Agent's time stamp by 1 step and reset variables //
        Agent Time = Agent Time + 1          // Advances Agent's time in system one step //
        Agent Linked Agent = FALSE           //Tracks when Agent creates link between Neighbors//
        Agent Linked Knowledge = FALSE       //Tracks when Agent creates Knowledge link with Neighbor//
        Agent Linked Resource = FALSE        //Tracks when Agent creates Resource link with Neighbor//
        Agent Linked This Turn = FALSE       //Tracks if Agent has been linked to anything this turn//

//Have the agent link neighbors to each other as appropriate. Start with most radical first.//
    FOR each Agent DO
        {Sort Agent Neighbor list (Max to Min Radicalization factor)}
        FOR each Agent Neighbor DO
            IF (Neighbor Linked This Turn = FALSE ) AND (Agent Linked Agent = FALSE)
            AND (Agent Radicalization ≥ Neighbor Radicalization ≥ Threshold Radicalization ) THEN
                {Link Neighbor in question to neighbor with highest radicalization score,
                including self if not already linked(making it a 2 way connection)}
                {If no other neighbors, then do nothing.}
                Agent Linked Agent = TRUE
                Neighbor Linked this Turn = TRUE
        END
    END

//Have the Agent ensure Knowledge redundancy //
    FOR each Agent DO
        FOR each Agent Knowledge DO
            IF (Neighbor Linked This Turn = FALSE) AND (Knowledge Connected Agents < 2)
            AND (Agent Linked Knowledge = FALSE ) THEN
                {Link Neighbor with highest RadIndex less than Agent's RadIndex to Knowledge node,
                as long as that Neighbor has not been linked this turn}
                Agent Linked Knowledge = TRUE
                Neighbor Linked this Turn = TRUE
        END
    END

//Have the agent ensure resource redundancy //
        FOR each Agent Resource DO
            IF (Neighbor Linked This Turn = FALSE) AND (Resource Connected Agents < 2)
            AND (Agent Linked Resource = FALSE ) THEN
                {Link Neighbor with highest RadIndex less than Agent's RadIndex to Resource node,
                as long as that Neighbor has not been linked this turn}
                Agent Linked Resource = TRUE
                Neighbor Linked this Turn = TRUE
        END
    END
```