Graph Theory, Social Networks and Counter Terrorism

Adelaide Hopkins
Advisor: Dana Fine
Department of Mathematics
University of Massachusetts Dartmouth
May 19, 2010

INTRODUCTION

On September 10, 2001 most Americans had never heard of a clandestine group of Islamic fundamentalists called al-Qaeda, nor did they know that they were about to embark on a seemingly endless war against a whole new kind of enemy; one that would require an entirely new approach to war. John Arquilla and David Ronfeldt's book published not soon after 9/11, *Networks and Netwars,* discusses how modern warfare has evolved into a netwar, "a lower-intensity battle by terrorists, criminals, and extremists with a networked organizational structure," one which is often leaderless and thus able to act more quickly (Ressler, 2006). In the subsequent days of the World Trade Center attacks, as information gradually came into public knowledge about the hijackers, who they operated for and under and their relationships to each other, a new term came into the American vocabulary: terrorist network.

Networks are the underlying structural basis of many natural events, organizations, and social processes, and a social network is a result of the patterns of connections between agents or actors in a network (Ressler, 2006, p. 2). Social networks are visually represented in mathematical literature by a graph made up of points, called nodes or vertices, with connecting lines, called edges, which represent an association between the nodes. Graphs may be directed or undirected. Undirected graphs can show interpersonal relationships between actors in a social network and can be represented by a symmetric adjacency matrix **A** with elements:

$$A_{ij} = \begin{cases} 1 & \text{edge (i, j) exists} \\ 0 & \text{no edge} \end{cases}$$

Directed graphs can show flow of money or ideas and are be represented by an asymmetric matrix in which $A_{ij} = 1$ implies the existence of an edge pointing from $j\ to\ i$ which will, in general, be independent of the existence of the edge from $i\ to\ j$ (2Newman, 2006). Weighted graphs can be directed or undirected and be represented by an adjacency matrix in which the non-zero values indicate connections of varying strengths.

In a social network the nodes may represent individual people or groups of individuals with the links showing relationships or flows of information, money, or ideas between the nodes. Social network analysis is grounded in the intuitive notion that the patterns of social ties in which the actors are embedded has important consequences for those actors (Freeman, 2004, p. 2). It is

then the task of a network analyst to use mathematical properties inherent in the graphical structure to seek and uncover differing patterns in the network to determine the conditions under which the networks operate and may best be exploited.

It is clear that the structure of a social network can have a strong influence over the patterns of economic transactions, flow of information, spread of diseases and ideas and nearly every other type of social interaction amongst the human beings it represents (2Newman, 2006). Indeed, the network structure of an organization like al-Qaeda will "directly affect its ability to access new ideas, recruit new individuals, and achieve sustainability" (Ressler, 2006). The new challenges in warfare that al-Qaeda and groups like it present have stimulated a resurgent interest in the application of social network analysis to counterterrorism. However, rampant inaccuracies in data imply that mathematicians and administrations alike must exercise caution before too much stake is put into such a new and inexact science, and these inaccuracies are taken into account in the analysis of the sample network presented here. Errors stem from incompleteness and fuzzy boundaries in the data as a result of the inevitability of missing nodes and the fact that data may be subject to self-reported bias. Data may also be biased toward leaders and members captured or identified in an attack. As well, accurate and specific information on covert and terrorist networks are not readily available to the public, or at least not easily found, and the ever-changing landscape of these networks makes keeping current graphical models accurate very difficult.

Though despite these challenges and through increasingly extensive research, social network analysis has arisen as an effective way of tracking, understanding, and possibly dismantling the structures of these clandestine cells by providing both a visual and a mathematical analysis of human relationships in which the structure of the network and relationships and ties with others in the network are more important than the individual actors in the network (Ressler, 2006).

With continuous discovery and research beginning in the 1930s, social network analysis has evolved through adopting mathematical techniques and applying them to sociological events and has applications in organizational psychology, sociology and anthropology. Social network analysis provides an avenue for analyzing and comparing formal and informal information and

ideological flows in an organization as well as it aids in identifying potential weaknesses in a terrorist network and uncovering acts of terrorism before they occur.

SOCIAL NETWORK ANALYSIS: DISAMBIGUATION

Social network analysis focuses on the kind of research that examines the links among the objects of study (in this case people). This approach is based on a structural analysis that has extensive relevance throughout academia. Anthropologists and those working in communications use structural analysis to investigate the spread of information in communities as well as to analyze human interaction and predict behaviors. Politics and organization studies, social psychology and diffusion research, and biological and molecular research all incorporate some form of structural analysis in their studies. Astrophysicists use structural analysis to study the gravitational influence of each planet in our solar system over the others in order to account for planetary orbits, while electrical engineers observe how the interactions of various electronic components will influence the flow of a current through a circuit (Wasserman, 1994).

According to Linton C. Freeman, there are four elements that define social network analysis:

(1) Motivation by a structural intuition based on ties linking social actors

(2) Research based on systematic, empirical data

(3) Utilization of graphic imagery

(4) Employment of mathematical and/or computational models to predict future behavior (Freeman, 2004)

The method of social network analysis itself consists of three essential parts: (a) the conducting of empirical studies which investigate network structure using a variety of techniques such as interviews, direct observation, archival records, or methods like “snowball sampling” or “ego-centered” studies, (b) the use of mathematical or statistical methods to answer questions about the community, and (c) the creation of mathematical or computer models to replicate the processes taking place in networked systems. Empirical studies are represented by a graph consisting of multi-edges (repeated edges between the same pair of vertices), self-edges (edges connecting a vertex to itself), and hyper-edges (edges that connect more than two vertices together) which then connect the network into mathematically measurable groups of clusters and connected components.

When taken together, graphs and mathematical properties of those graphs are used in an attempt to answer questions about the network such as: Who are the most central members of a network and who are the most peripheral? Which people have most influence over others? Does the community break down into smaller groups and if so what are they? and Which connections are most crucial to the functioning of a group? The final result is a visual representation of the connections between individuals in the network, and because possible connections between people vary, studies may be designed appropriately to measure the particular connections of interest to the experimenter (2Newman, 2006). These methods can provide important information on the unique characteristics of terrorist organizations such as network recruitment, network evolution, and the diffusion of radical ideas through topological analysis focusing on the statistical characteristics of the network structure.

PROPERTIES OF GRAPHS

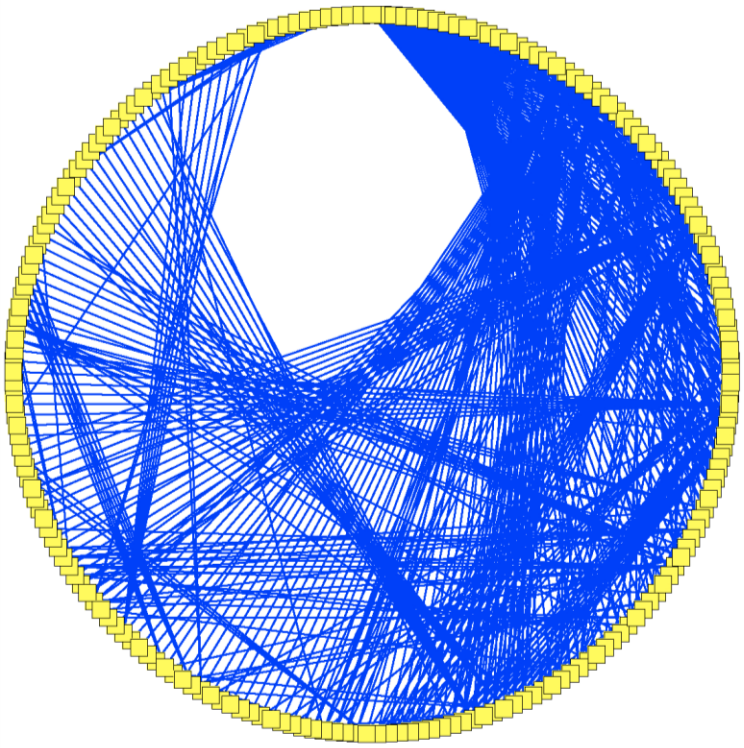
As previously stated, a graph is made up of nodes or vertices connected by edges. A node's *degree* is the number of edges incident on that vertex and is a highly effective measure of the influence or importance of a node (Newman, 2003). Other properties of graphs used in social network analysis may include the measure of a *path* which is a sequence of vertices included by following connected edges across the network, or more specifically, the identification of a *geodesic path* which is the shortest path, in terms of number of edges traversed, between a specified pair of vertices, or the mean geodesic distance between a vertex and all other connected vertices, called *closeness* (Newman, 2003). Two paths which connect the same pair of vertices are said to be *node-independent* if they have no common vertices other than their starting and ending points. "The number of node-independent paths between vertices i and j in a graph is equal to the minimum number of vertices that need to be removed from the graph in order to disconnect i and j from one another. Thus, this number is in a sense a measure of the robustness of the network to deletion of nodes." (Girvan 2001) A vertex may be identified as a *bridge,* a node through which pass many shortest paths (high "betweenness"), or a *hub*, a node with high degree. Other properties include kinship structure, distribution of structural properties such as vertex degree or geodesic paths, connectors, mavens, leaders, bridges, and isolates, boundary spanners, and peripheral players all of which can be analyzed to gain deeper insight into the

network.

ANALYZING THE TOPOLOGY OF NETWORKS WITH A SAMPLE APPLICATION

Network analysis uses a number of statistical properties to analyze the topology of a given network. The purpose of this paper was to follow a similar formula to that used by Jennifer Xu and Hsinchuen Chen in their article, *The Topology of Dark Networks*, in which they compared the topological features of three different kinds of covert or "dark" networks including the Global Salafi Jihad, methamphetamine traffickers, gang-related criminals, and a terrorist website network.

Graph 1



Maple 13 was used to generate visual representations of the al-Qaeda network using a hand-drawn adjacency matrix imported from Excel as a .csv file. Data for the structure of this network was mined from GlobalSecurity.org and cross-referenced with recent news articles, history books, and government publications when available. The pinwheel structure of this circle graph is an incidental result of the "snowball sampling" method used to gather and enter the data. To ascertain if the sample al-Qaeda network is small world or follows the expected formula for a dark network the average path lengths, clustering coefficients and global efficiency must be calculated. (Xu 61)

Types of Networks

Network analysis often deals with the distribution of structural properties such as vertex degree. When analyzing the vertex degree distribution of random graphs the fraction pk of vertices having degree k is given by the binomial distribution, which becomes Poisson in the limit of

large n:

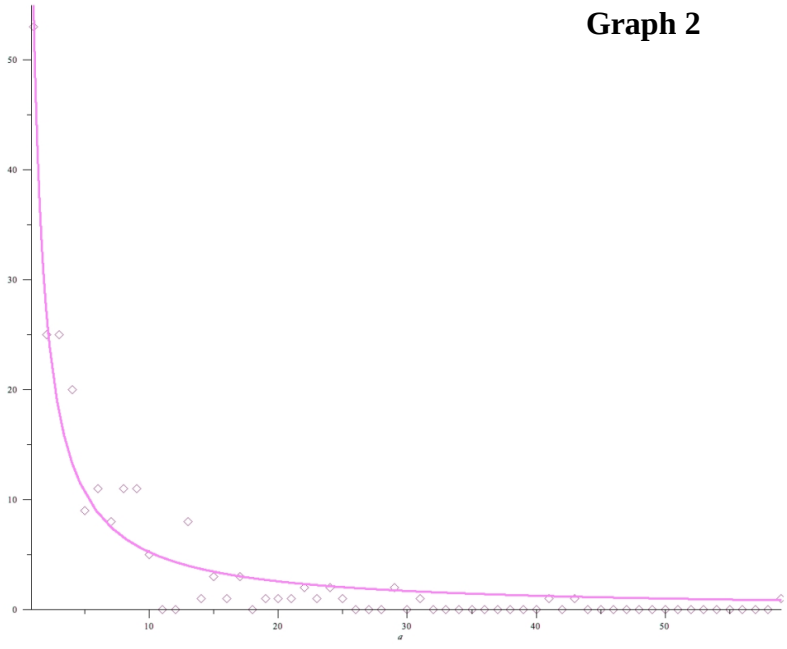
$$p_k = \binom{n-1}{k} p^k (1-p)^{n-1-k} \cong \frac{z^j e^{-z}}{k!}$$

where $z = (n - 1)p$ is the mean degree. However, when analyzing graphs of real networks (social and otherwise) empirical observation has found that most have highly non-Poisson distributions of degree, often heavily right-skewed with a fat tail of vertices having unusually high degree. It is those vertices found in these fat tails that may have a substantial effect on the behavior of a networked system (2Newman, 2006).

Large complex networks such as terrorist or criminal networks can be categorized into three types: random, small-world, and scale-free. A number of statistics have been developed to study their topology including average path length, average clustering coefficient, and degree distribution (Xu, 2008). The topological analysis of the sample network represented in Graph 1 can be seen in Table 1.

Random networks have a small average path length,l, with small clustering coefficient, C, and a bell-shaped Poisson degree distribution. Comparatively, *small-world* networks are characterized by a significantly larger clustering coefficient than random networks while maintaining a relatively small average path length and are vulnerable to bridge attacks. *Scale-free* networks are characterized by a power-law degree distribution where a large percentage of nodes in the network have just a few links and a small percentage of nodes have a large number of links (Graph 2). Growth and preferential attachment play a key role in the emergence of the power-law distribution, and

Graph 2



networks with scale-free properties are highly robust against random failure and errors but notably vulnerable to targeted attacks (Xu, 2008, 58 – 60). Most complex systems are not random but present both small-world and scale-free properties. Measures such as *link density*, the ratio of existing edges *m* to all possible edges *n*, and global average shortest path length can help to determine which of these categories a network falls into. Link density is calculated as

$$d = \frac{2m}{n(n-1)}$$

and the Maple code used to calculate the average shortest path length may be found in Appendix A.

Table 1: TOPOLOGICAL ANALYSIS

Number of Nodes, *n*	209
Number of Links, *m*	662
Average Degree, <*k*>	42.05126345
Maximum Degree	59
Link Density, *d*	0.03045638572
Degree Assortativity, *r*	-.3250012
Power-Law Distribution Exponent, γ	1.02308154
Goodness of Fit, R^2	0.9142475
Clustering Coefficient, *C*	0.7186465

Clustering

Transitivity, also called the degree of clustering, is the tendency for triangles of connections to appear frequently in networks (socially: "the friend of my friend is also my friend"). The *clustering coefficient* of the entire network is the average density:

$$C = \langle \frac{2E_i}{k_i(k_i - 1)} \rangle$$

(Ebel, 2003) and was calculated for the sample data using a code written in Maple which may be found in Appendix A. A similar, but not equivalent, definition for the clustering coefficient is provided by the fraction of fully connected "triples" with a triple being a connected subgraph containing three nodes

$$C_{\Delta} = \frac{3 * (\text{number of fully connected triples})}{\text{number of triples}}.$$

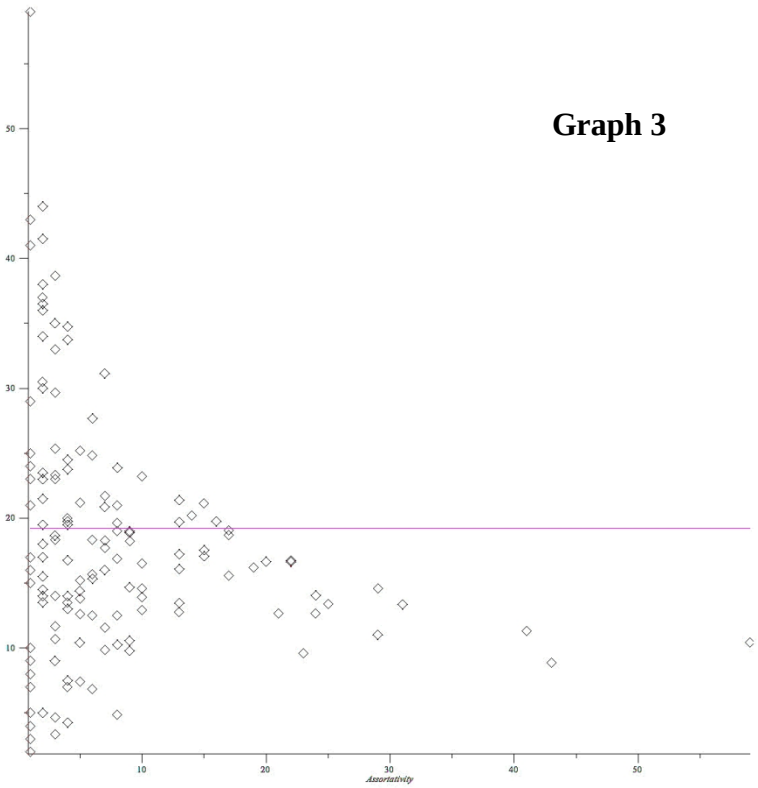
In social networks, it is safe to assume that the central mechanism for the dynamics of creation of new acquaintance networks is that people are introduced to each other by a common acquaintance (transitive linking). (Ebel, 2003)

Assortativity

Inferences can also be made about the significance of those vertices which fall in the core and periphery of the graph as well as their *similarity*, meaning the extent to which two given vertices do or do not occupy similar positions in the network; boundary spanners, for example, are defined as actors who link distinct clusters or groups of members within the network (Hanson, 2008). Similarly, a cut-point is a node whose removal would increase the number of connected components by dividing the sub-graph into two or more separate sub-graphs between which there are no connections and can be viewed as a kind of local centrality can operate as pivotal points of articulation between the agents that make up the network (Sabater, 2002).

Social networks have non-trivial clustering of network transitivity, and they show positive correlations, also called assortative mixing, between the degrees of adjacent vertices. (2Newman, 2003) Assortativity reflects the tendency for nodes to connect with others that are similarly popular in terms of any easily compared graphical statistic, such as degree or betweenness. For example, the degrees of adjacent vertices in networks are positively correlated in social networks but negatively correlated in most other networks, and the level of clustering seem in many non-social networks is no greater that one would expect by chance, given the observed degree distribution. For social networks however, clustering appears to be far greater that would

Graph 3



be expected by chance. (2Newman, 2003) Almost all networks seem to be disassortatively mixed, i.e., have negative values of the assortativity coefficient r, except for social networks, which are normally assortative. Degree correlation arises because individuals who belong to small groups tend to have low degree and are connected to others in the same group who also have low degree. Similarly, large groups tend to have higher degree and are also connected to one another. (2Newman, 2003) Positive degree assortativity, which was attempted to be replicated here, means that popular members tend to connect with other popular members, and if each individual knows all others in their group, then $p = 1$ and we have perfect assortativity. (2Newman, 2003) "In positively assortative networks, high-degree nodes tend to cluster together as core groups, a phenomenon evident in the GSJ network in which bin Laden and his closest cohorts form the core of the network and issue commands to other parts of the network." (Xu, 2008, 61)

Degree correlation arises since individuals who belong to small groups tend to have low degree and connect to others in the same group, who also have low degree while large group members tend to have a higher degree and are also connected to one another. Graph 3 would indicate a disassortative relationship in the sample data however, much of the error can be attributed to incomplete or inaccurate data because the disassociation is small.

Topological Analysis of Covert and Terrorist Networks

A covert network's efficiency in terms of communication, information flow and commands can be tied to their small-world structures, which are characterized by short average path length and a high clustering coefficient. Terrorists are able to connect with any other member in a network through only a few mediators; the networks are sparse, with very low link density which help to lower the risk of detection and enhance efficiency of communication. The high clustering coefficient contributes to the local efficiency. (Xu, 2008, 62) Dark networks present scale-free properties with power-law degree distributions in the form of $p(k) \sim k^{-\gamma}$ where $p(k)$ is defined as the probability that an arbitrary node has at least k links. (Xu, 2008, 62) Two mechanisms have been proposed to account for the emergence of two-regime power-law degree distributions during the evolution of a network. First, new links may emerge between existing network members. This emergence implies that criminals or terrorists who were not related previously

could become related over time. (Xu, 2008, 62)

However, network models may have missing links that can cause the networks to appear to be less efficient; there may actually be hidden "shortcuts" connecting distant parts of the networks. Second, the presence of coincidental "fake" links might cause the elicited networks to be more efficient than they would otherwise be since these links are not communication channels. (Xu, 2008, 63) Understanding topology yields greater insight into the nature of clandestine organizations and could help develop effective disruptive strategies. Comparatively, terrorist networks are more sensitive to attacks targeting bridges than to those targeting hubs whereas pure scale-free networks are vulnerable to both hub and bridge attacks. Small-world networks are more vulnerable to bridge attacks.

Centrality Measures

Measures such as *network centralization* and individual network centralities provide insight into an individual's location in the network, where the relationship between the centralities of all nodes can reveal much about the overall network structure. For example, a very centralized network is dominated by one or a few very central nodes where, if removed or damaged, the network would quickly fragment into unconnected sub-networks. A highly central node can become a single point of failure. A network centralized around a well-connected node with high degree and betweenness centrality, called a *hub*, can fail abruptly if that hub is disabled or removed (orgnet.com). Conversely, a less centralized network has no single points of failure and is resilient in the face of many intentional attacks or random failures. In this case many nodes or links can fail while allowing the remaining nodes to still reach each other over other network paths. Networks of low centralization "fail gracefully" and are more indicative of those seen when attempting to map al-Qaeda. (orgnet.com) Centrality measures require the computation or enumeration of shortest paths between all pairs of nodes in the graph. (Carpenter 1) By utilizing some or all of these measures, analysts then create computer models, which allow predictions to be made about the behavior of a community as a function of the given parameters affecting the system (2Newman, 2006).

Graphs have certain individual centrality measures that are highly useful in topological analysis.

A centrality measure attempts to answer the question, "Who is the most important or central person in this network?" However, centrality measures are often very sensitive to minute changes in nodes and/or links. As well, the meanings of "most important" or "central" nodes can change with the type of information a researcher is seeking. For example, *degree centrality* (degree) is a measure of the number of direct connections a node has and is usually an effective measure of the influence or importance of a node where the degree k_i of vertex i is

$$k_i = \sum_{j=1}^{n} A_{ij} \quad (2\text{Newman}, 2006)$$

Nevertheless, sometimes what really matters is where those connections lead and how they connect the otherwise unconnected (orgnet.com). *Eigenvector centrality*, conversely, acknowledges that not all connections are equal and that a vertex's connections to people, who are they themselves influential, will lend that vertex more influence than connections to less influential people where the centrality x_i is

$$x_i = \frac{1}{\lambda} \sum_{j=1}^{n} A_{ij}\, x_j,$$

where λ is constant (2Newman, 2006). However, having a large number of connections still counts for something, but a vertex with a smaller number of high-quality contacts may outrank one with a larger number of mediocre contacts.

Another centrality measure is concerned with the idea of the *betweenness* of nodes. The idea of *betweenness-based centrality* is concerned with whether or not a point in a communication network is central to the extent that it falls on the shortest path between pairs of other points; that is, the fraction of geodesic paths between other vertices that vertex *i* falls on (Freeman, 1977). It is a measure of the influence of a node over the flow of information between other nodes, especially in cases where information flow over a network primarily follows the shortest available path. (Girvan 3)

Betweenness is calculated by first finding the shortest path (or paths) between every pair of vertices, and then determining on what fraction of those paths *i* lies.

$$B(v) = \sum_{s \neq t \neq v \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \text{ where } \sigma_{st} \text{ is the number of shortest paths between } s \text{ and } t \text{ in } G.$$

(Carpenter 2) What results is a crude measure of the control *i* exerts over the flow of information between others in the network and measures the fraction of information that will flow through *i* on its way to its destination. Other measures of this type are referred to as "flow betweenness" or "random walk betweenness" which may account for the fact that the flow of information does not always flow along geodesic paths. A vertex with high betweenness will exert substantially more influence over others by virtue not of being in the middle of the network but of lying "between" other vertices in this way. A subset centrality measure of betweenness is the random-walk betweenness of a vertex which is equal to the number of times that a random walk starting at *s* and ending at *t* passes through *i* along the way, averaged over all *s* and *t* (Newman, 2003).

There is much debate about information flow in a network and how to determine along which paths an idea or message is most likely to travel. Information centrality weighs all paths between a pair of nodes, thinking all paths carry information and may be "very well-suited to analyzing terrorist networks where deliberate efforts are made to obfuscate communication" (Carpenter 5). Conversely, *closeness centrality* is determined by calculating the mean geodesic distance from a vertex to every other reachable vertex.

$$C(v) = \frac{1}{\sum_{t \in V} d(v,t)} \text{ where } d(v,t) \text{is the shortest distance between } s \text{ and } t \text{ in } G.$$

(Carpenter 2). Closeness is thus lower for vertices that are more central within the network in the sense that they have a shorter distance to travel to other vertices. One of the most important factors of social networks that seem to be emerging is that of network reach. Research by Noah Friedkin, Ron Burt and others indicates that the shorter paths in the network are more important and that these networks have horizons over which we cannot see, nor influence. They propose that "the key paths in networks are 1 and 2 steps and on rare occasions, three steps." (orgnet.com) The 'small world' that Milgram made famous is not one of six degrees of separation but of direct and indirect connections less than three steps away. Therefore, it is important to know: who is in your network neighborhood? Who are you aware of, and who can you reach? Uncertainty in the data will be reflected in inaccuracies in shortest path computations. Thus, not only is the length of the shortest path between a pair of nodes somewhat uncertain, but

the path itself may change dramatically with relatively small changes in the data which maybe especially problematic for measures like betweenness that depend on knowing the precise identity of nodes in geodesic paths. (Carpenter 4)

SOCIAL NETWORK ANALYSIS AS APPLIED TO TERRORIST NETWORKS

> "Bin Laden is the leader of a movement that doesn't necessarily need a leader to function and be effective… [al-Qaeda] is such a diffuse structure that it can survive without him." (Rothenberg, 2002, p. 37)

After the attacks of 9/11, academia, the government, and even mainstream media began to discuss the importance of social network analysis in fighting terrorism. Media outlets such as the *Washington Post* and the *Dallas Morning News* all ran articles lauding the potential benefits of network science. Authors of popular books on networks were interviewed extensively on television and radio programs on how the knowledge of social networks could be used to fight terrorism, however they repeatedly used words like amorphous, invisible, resilient, dispersed and other terms that made it difficult to visualize what the structure really looked like (Krebs, 2002). Then, in 2006 when the National Security Agency's controversial eavesdropping program hit the newswires, the importance of social network analysis in fighting terrorism reemerged in a *New York Times* article discussing the ability of network analysis to map and potentially make meaning out of the millions of communications NSA would intercept daily between individuals under surveillance (Ressler, 2006).

One may be mislead about the popular notion of the hierarchical structure of al-Qaeda with bin Laden as the *emir*, or leader, surrounded by a council of roughly one dozen advisors called the *shura*, and numerous subsequent committees responsible for the execution and maintenance of the essentials of any revolutionary force such as military operations, religious affairs, finances, and the production of false travel and identity documents (Rothenberg, 2002). In fact the larger more deadly aspect of the network, and what makes al-Qaeda so resilient to attack, is that it consists mainly of "small, multi-potential groups with considerable internal discipline and local decision making power all held together by the adherence to a common cause" which stems from

their religious fanaticism (Rothenberg, 2002). Few direct contacts, but a sense of connection to a larger whole and purpose, supports an unshakable belief structure that has shown itself capable of performing multiple tasks with agility, audacity, and devastating lethality (Rothenberg, 2002). While the hierarchical leadership structure of al-Qaeda is more familiar to the American public and may be important for the larger efforts of recruiting members or spreading ideologies, it is not critical for the perpetuation of terrorist activity and terrorism as a whole (Rothenberg, 2002).

Social network analysis has been shown to provide important information on the unique characteristics of terrorist organizations ranging from issues of network recruitment, network evolution and the diffusion of radical ideas. As network analysis of terrorist organizations continues to grow, its researchers can be classified in two groups: the data collectors and the modelers (Ressler, 2006). Data collectors are those researchers who focus primarily on data collection and then analyze the information through description and straightforward modeling. Modelers create complex models that offer insight on theoretical terrorist networks such as "how to model the shape of a covert network when little information is known," or how to estimate a terrorist network's vulnerabilities to destabilize it (Ressler, 2006, p. 5).

In the 2001 post-9/11 edition of *Connections,* an International Network for Social Network Analysis (INSNA) journal that publishes “original empirical, theoretical, and methodological articles, as well as critical reviews dealing with applications of social network analysis,” Valdis E. Krebs (2002) attempted to construct his own graph of al Qaeda using data sources and publicly released information reported in major newspapers such as the New York Times, the Wall Street Journal, the Washington Post, and the Los Angeles Times. (insna.com, Krebs, 2002) Once investigators knew who to look at, connections were quickly made amongst the hijackers. He mapped the links between the 19 hijackers using varying lengths representing the length of time two terrorists had spent together. Those living together, attending the same school or classes or training would have the strongest ties. Those travelling together and participating in meetings together would have ties of moderate strength and medium thickness. Finally, those who were recorded as having a financial transaction or an occasional meeting and no other ties were sorted into the dormant tie category and were shown with the thinnest links in the network (Krebs, 2002). When varying centrality measures are taken of Kreb's graph, Mohammed Atta (one of the

pilots on 9/11) scores the highest on degrees and closeness but not betweenness. This would indicate that, while he has contact with the most hijackers, he was not their commander and did not exercise the most influence over the group (Krebs, 2002).

Krebs' research led him to the conclusion that deep-trusted ties not easily visible to outsiders held al-Qaeda together (Krebs, 2002). He observed that many pairs of team members where beyond the horizon of observation and that many on the same flight were more than two steps away from each other. This indicated that the purpose of keeping cell members distant from each other, and from other cells, was to minimize the damage to the network if a cell member was captured or otherwise compromised (Krebs, 2002). The hijacker's network displayed a very long mean path length, 4.75 for a network of less than 20 nodes, clearly indicating al-Qaeda's preference for secrecy over efficiency (Krebs, 2002). However, when consideration is given to various operational meetings to coordinate tasks and report progress, the connections that arise present shortcuts to distant parts of the network. These connections drop the mean path length in the network by over 40% thus improving the information flow in the network (Krebs, 2002). However, after the coordination is accomplished and the members disperse, these cross-ties go dormant until the need for their activity arises again and are subsequently nearly invincible (Krebs, 2002).

Network structure is a modern organizational structure, the strength of which is built upon the idea of disintermediation or "removing the middle man" where individuals can directly connect to each other. This is especially facilitated with the advancements of modern telecommunications and the internet. Individuals are able to join al-Qaeda through weak ties and plan attacks through loose connections while still wreaking as must destruction as possible (Ressler, 2006). It is easier to kill a man than to change his mind, and terrorist organizations present a unique challenge in that they are united by a specific ideology. On the local level, the network is small and dynamic and consists of formidable barriers to entry and exit (Rothenberg, 2002). It values secrecy above communication and its structure tends to be more cellular and distributed than a normal social network (Carley, 2003, Rothenberg, 2002). The hijacker's network had a hidden strength in its massive redundancy through established prior contacts and it was the ties forged in school, through kinship, and training and fighting in Afghanistan that made the network very resilient

(Krebs, 2002). However, when analyzing al-Qaeda, one realizes that its entire global network is a connected component held together by its fundamentalist ideas, so that the loss of a unit or actor will not be deleterious to al-Qaeda's overarching mission, and may in fact serve to accelerate it (Rothenberg, 2002).

The federal government has been using link analysis to counteract terrorism, yet social network analysis improves upon link analysis by moving from single variable analysis to multivariate analysis, allowing the individual to control for many factors at once (Ressler, 2006). This transition from single to multivariable analysis indicates exceptional progress when researching terrorism because terrorism is affected by a number of different factors. For example, the propensity for one to participate in terrorist activity might not be strongly affected by the single variable of being related to a terrorist member but the combination of multiple variables such as poverty, type of government, combined with the link to a terrorist member may cause a person to participate in a terrorist activity (Ressler, 2006). Where traditional social network analysis is limited in that it only considers the linkage among people, is concerned with non-adaptive systems, and most measures have been tested only for small (less than 300 node) networks, multi-agent modeling uses very simple unrealistic agents who, although they adapt, move about only on a grid and don't take actual networks in to account (Carley, 2003). Social network analysis allows researchers to control for one variable while still taking others into account and thus may be used to anticipate and counteract terrorist cells while still attempting to address the underlying causes of terrorism (Ressler, 2006). Peter Klerks makes an excellent argument for targeting those nodes in the network that have unique skills and thus may have unique ties within the network. Klerks methodology centers on identifying the "task and trust ties" between conspirators to locate possible suspects and then, via snowball sampling, map their ego networks to see where they lead and overlap (Krebs, 2002).

One of the areas in which social network analysis presents a disadvantage is in the acquisition of data. Many researchers are limited to open source information which is usually incomplete, scattered, and prone to errors. Consequently, if the analyst is unable to find sufficient information on a specific terrorist, they must assume that that node does not exist and thus, the data analysis can be misleading (Ressler, 2006). Terrorists also generally try to keep a low profile before

carrying out an attack, which makes detection and acquiring current, relevant information unreliable and difficult. Often models are created data-free or without complete data and do not fully consider human and data limitations which can result in potentially misleading results as they cannot take into account behavioral and contextual issues that might affect the network structure and activity (Ressler, 2006). Modelers are often mathematicians or sociologists who do not have a foundation in terrorist studies nor do they always work with top counter-terrorism experts. All of these factors make it difficult to turn numbers and graphic models into interpretable results that not only make sense in the context of the vast literature on terrorism, but are applicable as well. Hence, knowledge of the appropriate people and cultures can provide a context for the network data created by the modelers, including the historical and political trends exhibited in terrorism, reasons people join terrorist groups, and the psychology of terrorist attack tactics, including suicide terrorism (Ressler, 2006).

Kathleen Carley (2003) of Carnegie Mellon University has made many great advances toward the applications of network analysis to counterterrorism through her research into network text analysis which is used to "define and model the relationships between words in a text to turn raw text related to Mideast covert networks into a pictorial network representation of the social and organizational structure of a covert network." (Ressler, 2006, p. 8) Her main contribution has been with the concept of dynamic network analysis made possible due to three key advances: (1) the meta-matrix connecting various entities such as agents, knowledge and events, (2) treating ties as "variable" and so having a weight and/or probability, and (3) combining social networks with cognitive science and multi-agent systems to endow the agents with the ability to adapt (Carley, 2003). In a *meta-matrix perspective* a set of networks are combined to describe and predict system behavior. In *variable tie perspective*, connections between entities are seen as ranging in their likelihood, strength, and direction rather than as being simple binary connections indicating exclusively whether or not there is a connection. Finally, the utilization of multi-agent network models enables researchers to project inferences about the dynamics of complex adaptive systems. In particular, these computational models "combine our understanding of human cognition, biology, knowledge management, artificial intelligence, organization theory and geographical factors into a comprehensive system for reasoning about the complexities of social behavior." (Carley, 2003, p. 3) Carley (2003) has outlined seven methods to assess

destabilization tactics of terrorist networks:

1. Identify key entities and the connections among them.
2. Identify key processes by which entities or connections are added or dropped, or in the case of connections, changed in their strength.
3. Collect data on the system (covert network).
4. Determine performance characteristic of existing system.
5. Determine performance characteristics of possible optimal system.
6. Locate vulnerabilities and select destabilization strategies.
7. Determine performance characteristics in the short and long term after a destabilization strategy has been applied.

CONCLUSION

An emerging emphasis on counter-operations outside of face-to-face combat has given light to the application of social network analysis to counterterrorism as well as intelligence and data analysis. While our military might dwarfs our enemies, our network is no match. Terrorists networks are loosely structured, can move quickly and be adaptive because they do not need to go through layers of bureaucracy while the bureaucratic networks that are tasked with executing counteractions to terrorism are unlikely to have the capacity to deal with al-Qaeda in their current network configuration (Ressler, 2006). Covert networks often don't behave like normal social networks and the conspirators don't often form many new ties outside of the network while minimizing the activation of existing ties inside the network. Strong ties, which were frequently formed years ago in school and training camps, keep the cells interconnected, yet unlike normal social networks, these strong ties remain largely dormant and therefore hidden. They are only activated when absolutely necessary. Weak ties were almost non-existent between members of the hijacker network and outside contacts. It was often reported that the hijackers kept to themselves. They would rarely interact with outsiders, and then often one of them would speak for the whole group. A minimum of weak ties reduces the visibility into the network, and chance of leaks out of the network (Krebs, 2002). With a normal social network, strong ties reveal the cluster of network players, and thus it is easy to see who is in the group and who is not. In a covert network, because of their low frequency of activation, strong ties may appear to

be weak ties, or may not appear at all (Krebs, 2002). Social network analysis has brought together sociologists, anthropologists, mathematicians, economists, political scientists, psychologists, communication scientists, statisticians, ethologists, epidemiologists, computer scientists, organizational behavior and market specialists from business schools and recently, physicists all under the umbrella of structural analysis. Social network analysis focuses on the value of the network structure rather than the characteristics of the individual provides a structural analysis while still leaving room for individual effort (Freeman, 2004, Ressler, 2006).

References

Bonacich, P. (1972). Factoring and weighting approaches to status scores and clique identification. *Journal of Mathematical Sociology 1972(2),* 113 – 120.

Carley, K. M., & Reminga, J., & Kamneva, N. (2003). Destabilizing terrorist networks. *NAACSOS conference proceedings.* Pittsburgh, PA.

Carpenter, T., & Karakostas, G., & Shallcross, D. (2002). Practical issues and algorithms for analyzing terrorist networks. *Telcordia Technologies, Inc.* Morristown, NJ.

Ebel, H., & Davidsen, J., & Bornholdt, S. (2003). Dynamics of social networks. Kiel, Germany, & Toronto, Canada, & Leipzig, Germany. Retrieved from http://arxiv.org/PS_cache/cond-mat/pdf/0301/0301260v1.pdf

Freeman, L. C. (1977). A set of measures of centrality based upon betweenness. *Sociometry, 40(1),* 35-41.

Freeman, L. C. (2004). *The Development of social network analysis: A study in the sociology of science*. North Charleston, SC: BookSurge, LLC.

Girvan, M., & Newman, M. E. J. (2001). Community structure in social and biological networks. *Santa Fe Institute*, Santa Fe, NM, *& Department of Physics*, Ithaca, NY.

Hanson, W. R. (2008). Complexity leadership dynamics: Leader network awareness. *Clemson University*. Retrieved from http://www.netscience.usma.edu/NSW3/Program/Papers/hanson/hanson_08.pdf

Krebs, V. (2002). Mapping networks of terrorist cells. *Connections, 24(3),* 43-52.

1Newman, M. E. J. (2006). Finding community structure in networks using the eigenvectors of matrices. *Department of Physics and Center for the Study of Complex Systems.* Ann Arbor, MI. Retrieved from http://www-personal.umich.edu/~mejn/pubs.html

2Newman, M. E. J. (2006). The mathematics of networks. *Center for the Study of Complex Systems, University of Michigan.* Retrieved from http://www-personal.umich.edu/~mejn/papers/palgrave.pdf

1Newman, M. E. J. (2003). A measure of betweenness centrality based on random walks. *Department of Physics and Center for the Study of Complex Systems.* Ann Arbor, MI. Retrieved from http://www-personal.umich.edu/~mejn/pubs.html

2Newman, M. E. J., & Park, J. (2003). Why social networks are different from other types of networks. *Department of Physics and Center for the Study of Complex Systems.* Ann

Arbor, MI. Retrieved from http://www-personal.umich.edu/~mejn/pubs.html

Ressler, S. (2006). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs, 2(2).* Retrieved from www.hsaj.org/pages/volume2/issue2/pdfs/2.2.8.pdf

Rothenberg, R. (2002). From whole cloth: Making up the terrorist network. *Connections 24*(3), 36-42.

Sabater, J., & Sierra, C. (2002). Reputation and social network analysis in multi-agent systems. *Proc. First Internat. Joint Conf. Autonomous Agents and Multiagent Systems.* Association for Computing Machinery, Bologna, Italy. Retrieved from http://ccs.mit.edu/dell/reputation/SocialRegret.pdf

Wasserman, S. & Faust, K. (1994). *Social network analysis in the social sciences.* Cambridge, UK: Cambridge University Press.

Xu, J., & Chen, H. (2008). The topology of dark networks. *Communications of the ACM 51(10),* 58 – 65. New York, NY. Retrieved from http://ai.arizona.edu/intranet/papers/Xu-SNA-2008.pdf