Original Article

Social Network Analysis: A case study of the Islamist terrorist network

Richard M. Medina
Assistant Professor, Department of Geography and GeoInformation Science, George Mason University, 4400 University Drive, MS 6C3, Fairfax, VA 22030-4444, United States.
E-mail: rmedina3@gmu.edu

Abstract Social Network Analysis is a compilation of methods used to identify and analyze patterns in social network systems. This article serves as a primer on foundational social network concepts and analyses and builds a case study on the global Islamist terrorist network to illustrate the use and usefulness of these methods. The Islamist terrorist network is a system composed of multiple terrorist organizations that are socially connected and work toward the same goals. This research utilizes traditional social network, as well as small-world, and scale-free analyses to characterize this system on individual, network and systemic levels. Leaders in the network are identified based on their positions in the social network and the network structure is categorized. Finally, two vital nodes in the network are removed and this version of the network is compared with the previous version to make implications of strengths, weaknesses and vulnerabilities. The Islamist terrorist network structure is found to be a resilient and efficient structure, even with important social nodes removed. Implications for counterterrorism are given from the results of each analysis.
Security Journal (2014) **27,** 97–121. doi:10.1057/sj.2012.21; published online 28 May 2012

Keywords: social network analysis; terrorism; al-Qaeda; global network

Introduction

The al-Qaeda led global terrorist network began as a small guerilla organization in the 1980s that helped fend off Soviet occupation in Afghanistan. It has expanded into a global movement that comprises many organizations and individuals (with and without formal social connections). Al-Qaeda, affiliates or sympathizers are operating on every continent. With the great losses the terrorist network experienced in 2011, including the deaths of Osama bin Laden and Anwar al-Awlaki, there is question as to whether the organization can pose global threats on the scale of 9/11; however, with regrouping and restructuring, the potential to command attacks within the most secure countries in the world can be harnessed again. While multiple organizations are active in the system, al-Qaeda remains the core organization in the network and offers ideological, logistic and strategic assistance to other terrorists and organizations.

The global Islamist[1] terrorist network is constructed from many smaller networks, and operates on international, regional and local levels (Kilcullen, 2005). Family/friendship,

financial and virtual networks are utilized by different sized groups and individuals that are arranged in a networked manner. The core of the global network, al-Qaeda, is a conglomerate of multiple regional branches including al-Qaeda in Iraq (Tanzim Qaedat fi Bilad al-Rafidayn), al-Qaeda in the Islamic Maghreb (Tanzim Qaedat fi Bilad al-Maghreb al-Islami) and al-Qaeda Organization in the Malay archipelago, among others. The network also includes many affiliates including Jemaah Islamiyah, Lashkar-e-Toiba and Abu Sayyaf (International Centre for Political Violence and Terrorism Research (ICPVTR), 2008).

The Islamist network has, since its inception in the 1980s, generally grown in strength and numbers, until relatively recently with counterterrorist efforts. The network has persisted through time with what would in many other network cases be major setbacks. Following the attacks of September 11, 2001, US and coalition forces fought in the War on Terrorism in many different countries including Afghanistan and Iraq, at one point seeming to defeat of the Taliban (Armitage, 2002), who have since resurged. The Islamist network has lost many leaders and has rebuilt and restructured much of its network. On 2 May 2011, Osama bin Laden, the figure head of the Islamist network was killed and quickly replaced by the number two in the network, Ayman al-Zawahiri. The future of Islamist terrorism is uncertain, though up to this point has proven to be resilient and adaptive.

This article serves two purposes. First, it provides an introduction to Social Network Analysis (SNA) methods that can be used to characterize terrorist networks and identify properties of strength and weakness. Traditional SNA (Wasserman and Faust, 2007) and more recent small-world (Watts and Strogatz, 1998) and scale-free (Barabási and Albert, 1999) approaches are used to analyze terrorist network structure. This is illustrated through a case study on the Islamist terrorist network. Second, it serves to explore the timely issue of how the removal of leaders affects the structure and operations of the network. In this analysis, Osama bin Laden and Abu Mussab al-Zarqawi are removed from the network sample. Then SNA results are compared between the network with and without the leader nodes.

The rest of this article is structured as follows: Present day terrorist network structures are discussed to provide a background for the analysis. Then a brief history of the SNA approach is given followed by the data, methods and analysis of the global Islamist terrorist network. Implications of each analysis are included throughout. Finally, conclusions are discussed including successes and failures of SNA in this research and future directions. All equations and explanations can be found in the Appendix.

Terrorist Network Structures

Terrorist organizations are typically arranged in network structures where authoritative roles vary by structure type. Two general types of network organization are hierarchical and decentralized. Hierarchical networks have a well-defined leadership core, while in decentralized networks the leadership is spread throughout the network and is much more difficult to detect. The Islamist terrorist network is often conceptualized as a decentralized network; however, as an adaptive organization it may take the form of multiple structures, including some that are hierarchical, to perform varying operations and maintain security (Medina and Hepner, 2011).

There are three forms of systemic decentralization: structural, geographic and authoritative. Structurally, a social network is decentralized if the pattern of relationships between

nodes diverges from the core of the network, such that there is no identifiable core, or there are multiple cores. This type of decentralization is based on connectivity. In the extreme case, a structurally decentralized network is an all-channel network where every member is connected to all others (Arquilla and Ronfeldt, 2001).

Geographic decentralization occurs for a social network as entities geographically disperse from the network core. This can occur by movement of members or recruitment of members that already reside in distant places. Examples of this are seen with terrorist organizations, such as al-Qaeda that operate on a global scale as opposed to organizations that have remained relatively local to regional, such as the Provisional Irish Republican Army.

Authoritative decentralization occurs when the leadership of the network is distributed throughout the entire network. The network becomes more resilient as the organization cannot be destroyed by removing its head (Arquilla and Ronfeldt, 2001). For example, the death of Osama bin Laden in 2011 or the dismantlement of al-Qaeda will not necessarily result in the destruction of the global network. Another leader or organization that operates on a global level could potentially take the leadership role. In the case of al-Qaeda, Ayman al-Zawahiri is presently at the helm following the death of Osama bin Laden. Attacks on the network can lead to further decentralization and splintering. The cohesive future of the global terrorist system is based on its level of adaptation.

The SNA Approach

Social Network Analysis (SNA) is composed of methods and metrics used to characterize networks of connected people and the relationships between them. It has gained popularity in recent years, partially an effect of globalization, the information age and ubiquitous connectivity. It allows for research on systems of connected people and provides a new perspective for answering organizational questions based on relationships (Wasserman and Faust, 2007). Widely used approaches to SNA today include traditional analyses and more recent small-world (Milgram, 1967; Watts and Strogatz, 1998) and scale-free models (Barabási and Albert, 1999). Traditional SNA focuses on nodal network positions. It is often used to identify various roles within networks, such as brokerage and leadership, though there are many other applications. Small-world and scale-free models focus on the characterization of networks based on structures of connected nodes. Small-world networks are characterized by high clustering and relatively low numbers of intermediaries between people (Watts and Strogatz, 1998), while scale-free networks are dynamic in that they exhibit growth over time and include network hubs that gain connections in proportion to the number of connections they already have (Barabási and Albert, 1999).

Regularities and patterns identified through SNA define social structures and relationships in the networks that are not always explicitly apparent. On the basis of the patterns, implications can be made about organizational structure, diffusion, efficiency and resilience. SNA techniques exist for local (individual nodes) and global (entire network) analyses (Malm *et al*, 2009). This provides a better understanding of networks as systems and also social location and influence of individual actors.

SNA can help researchers uncloak strengths and weaknesses, leadership, and underlying structures of terrorist networks (Sparrow, 1991; Ressler, 2006). Though data are scarce, there have been multiple publications on the subject including those by Krebs (2002),

Sageman (2004), Koschade (2006), Magouirk *et al* (2008) and Xu *et al* (2009). Krebs was the first to apply SNA on the September 11th bomber network and analyze communication topologies (2002); Sageman published a large study of the Global Salafi Jihad network (2004); Koschade used SNA to analyze the Jemaah Islamiyah network (2005); Magouirk *et al* showcase the Global Transnational Terrorism Project, which builds a terrorist social network database (2008); and Xu *et al* analyze the growth pattern of the Global Salafi Jihad (2009). These and other authors have paved the way for further SNA analyses on terrorist networks.

SNA of the Global Islamist Terrorist Network

Data collection and processing

The dataset compiled for this research includes 381 individuals who are terrorists or actively support the goals of terrorist organizations and 690 undirected links that connect those individuals. The links include terror-based connections, such as being in the same terrorist cell, training at a camp and planning attacks, non-violent operational activities, such as knowingly financing and providing other forms of support and shelter, and radicalization activities, such as preaching violent Jihad and leading potential terrorists to active radicalization. For each of the links, a social interaction is required, which can include face-to-face meetings, phone calls and email messages, among other types of interactions. Because this is a preliminary study and detailed data in this area are scarce, there is no weighting to signify stronger or weaker relationships based on type or frequency of contact. In an ideal case, analyses with weighted links could provide a greater understanding of the usage and effectiveness of various information technologies; however, data with the necessary detail at this scale of analysis are not available in the open source.

The temporal range for the dataset begins in the 1980s, when al-Qaeda began its formation, and ends in 2008. Because of this long time span, the data set includes individuals that are alive, dead and imprisoned. The majority of individuals in the dataset are affiliated with one or more Islamist organizations, which include al-Qaeda, Jemaah Islamiyah, Abu Sayyaf, the Chechen insurgency and others.

Three open data sources were used to acquire the sample of terrorists and other supporting individuals: the International Centre for Political Violence and Terrorism Research (ICPVTR) at Nanyang Technological University in Singapore, the FMS Advanced Systems Group, and terrorist network literature from governmental and NGO reports, journals and websites. The ICPVTR houses one of the largest, most thorough terrorist network databases titled the *Global Pathfinder*. The *Global Pathfinder* includes profiles of many terrorist organizations, leaders and attacks all over the world. It also includes media reports and a comprehensive collection of documents linked to terrorist groups (International Centre for Political Violence and Terrorism Research (ICPVTR), 2008). These data were used to construct the foundational database for this research.

The second source, to build a more complete database for this research, is the FMS Advanced Systems Group. The *tracking the threat* website provides information on terrorists and other individuals affiliated with al-Qaeda (FMS Advanced Systems Group, 2008).[2] The information collected by FMS is open source from media, reports and other documents.

These data were extracted manually from the *tracking the threat* website and entered into the database.

The final source is a collection of journal articles, government publications and books on terrorist organizations. Terrorism information is widely available in the open source; however, time must be taken to sort through literature and format the data for specific usage. This information completed the database compilation.

Problems with terrorist network data

The main problems with open source terrorist network data are incompleteness of information, lacking representations of node dynamics and fuzzy boundaries between terrorists, supporters and innocent individuals (Sparrow, 1991; Krebs, 2002; Tsvetovat and Carley, 2002). The data used in this research provide no exception to these difficulties. Not all individuals involved with Islamist terrorism are included, nor would the collection of a comprehensive dataset be possible. The goal for data collection was to construct a database of sufficient size and detail to represent the terrorist network and provide meaningful research results. It is assumed that the 381 terrorists represented in the database are sufficient for this task.

It is difficult to determine who are terrorists and who are merely supporting the organization. This research defines Islamist terrorists as those that are members of Islamist terrorist organizations; however, it looks at Islamist terrorism as a system larger that the formal operational network of violent actors. Individuals who are actively supporting the Islamist network by providing financial, goods, haven and other support are also included in the database, as they are a part of the Islamist terrorist system.

Nodes in a terrorist network, and the connections between them, are dynamic in many ways. Changes over time that can affect topological properties, as can geographic movement, political boundaries and social structures within and between terrorist organizations. This research only includes social space analyses and does not consider types and strengths of relationships. Because of the spatiotemporally static nature of these terrorist data, and the lack of temporal detail related to activity, capture or death, the results gained from this research must be understood as a strictly social study with a best case network scenario (that is, a fully intact network without respect to time and space). The terrorists represented in this research existed as actors in the Islamist network system between its assumed beginnings in the 1980s to 2008. Not much can be said about specific operations or periods of time.

Traditional SNA methods to characterize network structure and connectivity

Traditional SNA methods include metrics of density, diameter and centrality. These metrics characterize network connectivity and structure and tend to focus on relationships within networks.

Density

Network density is calculated as the number of connections within the network compared to the total number of connections possible. Results are given as a proportion or a percentage

of the network that is connected. By calculating network density an analyst is provided with a general understanding of how well connected nodes within the network are. Networks that are relatively dense have greater flow potential. Nodes within them have more opportunities for transfer and are, in general, socially closer. Denser networks are more resilient in the sense that they are harder to dismantle. Removing a connection, in many cases, will not hinder the connectivity potential between people. For sparsely connected networks flows must follow few, specific paths. Sparse networks are less resilient, because the removal of nodes from poorly connected networks is more likely to be detrimental to overall connectivity and operations.

The density value for the Islamist terrorist network sample is 0.01, meaning that it is approximately 1 per cent connected. There are 690 total undirected links between nodes out of a total 144 780 possible. This network appears through SNA to be a relatively sparse social network, though many of the real network connections may not be accounted for in the dataset. Sparseness in this case is a judgment call, as density is typically used to compare networks. A good example of a much denser social network is illustrated with the online Facebook network, where Lewis *et al* (2008) have shown a population mean density of 22.4 per cent.

The sparseness of the Islamist terrorist network confirmed by this analysis may be due to a few factors. First, the SNA focuses on a small subset of the entire network. The dataset used for SNA is composed of entities that are logistically relevant. Many of the casual connections that would create a more socially dense Islamist environment are not included. Second, the network may be sparse for security purposes. In operational cells, there are cell members that are separated by multiple degrees[3] (Krebs, 2002). For example, agent handlers have been used by al-Qaeda logistically as intermediaries to minimize security threats (Gunaratna, 2002). In some covert networks there is a very small probability that two nodes are connected by chance (Tsvetovat and Carley, 2002). There is a clear advantage to sparseness of terrorist network connections. If any random member of a cell is captured, and s/he knows only few others, the entire operation is not at risk of being broken up. Third, the number of connections between nodes in the empirical network data may be underestimated. It is assumed that not all connections between terrorists are identified by the open sources used to compile the empirical data. Terrorists in the network may be more connected than the data illustrate. The Islamist network should be vulnerable to attacks if its sparseness resembles the results shown here, but it has proven, up to this point, to be quite resilient to the loss of members. It may be more resilient because of its successful covertness, size, and number of peripheral branches and affiliates, which with weakening of the core through the loss of leaders are presently gaining strength.

Diameter

The diameter of a network is reported as the longest geodesic path[4] between two nodes. If the longest geodesic is relatively short then any two nodes can reach each other by passing through few other nodes, thus, network diameter is a measure of reachability. If nodes can reach each other easily, material and non-material transfers through the network should be more efficient (Wasserman and Faust, 2007).

The diameter of the graph[5] representing the Islamist terrorist network is 12 with an average path length of 4, which is representative of a relatively compact social network. The diameter of 12 and other connections that require many degrees in the network may occur

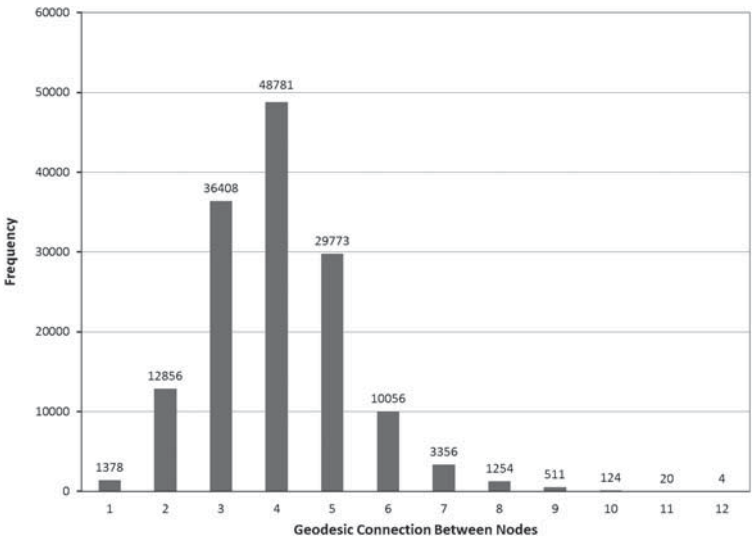

Figure 1: Distribution of geodesic connections.

because of the number of organizations involved. As a network of networks (for example, financial, friendship, operational, political, ideological counterparts), this system includes many organizations and members that are not in direct contact.

The distribution of geodesic connections is provided in Figure 1. The geodesic path that has the greatest frequency between two nodes is 4 degrees, keep in mind that a degree is a social connection from a target node. The largest geodesic of 12 is only counted for four of the connections between nodes in the network, although the connections that are registering above 6 degrees reflect the sparseness of the network at the peripheries. This network is much more well-connected at and surrounding the core.

The Islamist network, which crosses political and cultural lines, operates with al-Qaeda at the center and many other organizations and individuals on the periphery (International Centre for Political Violence and Terrorism Research (ICPVTR), 2008). These peripheral actors, in many cases, are not in direct contact, though they may have been at one time. For example, many terrorists in the network met previously in other Jihad arenas. The network has multiple branches in various locations that control local operations and work toward local goals. It is easy to conceptualize great social distances between people operating in the varying geographic regions. For example, members of al-Qaeda in the Islamic Maghreb might not be very connected with members in al-Qaeda in the Malay Archipelago. This type of sociospatial structure can generate longer geodesics (Medina and Hepner, 2011).

Results above suggest that the core of the organization is much denser than at the peripheries with the average path length and most occurring geodesic of 4. Geodesics greater than 7 occur relatively infrequently, so much of the network is connected quite efficiently. Disturbing the connectivity within this efficiently operating network can be detrimental to task and attack-based operations, though this may be difficult to do based on the connectivity structure.

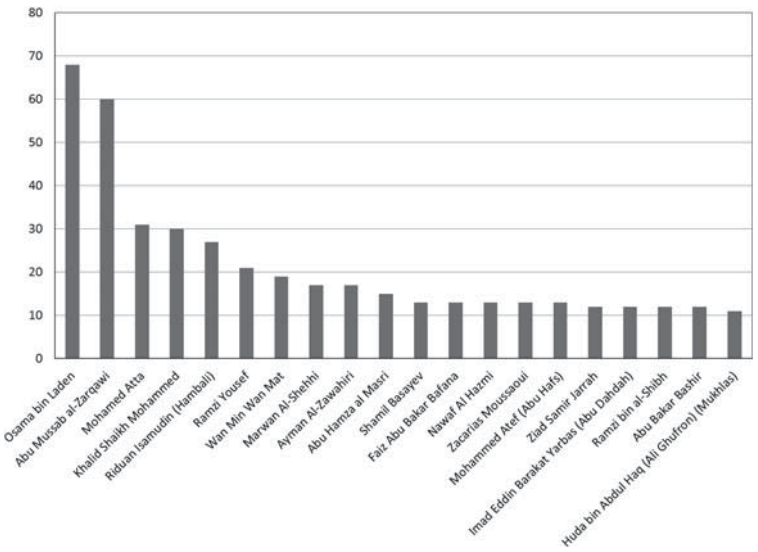

Figure 2: Nodes with more than 10 links.

Centrality

Centrality analyses are used to detect leadership roles in social networks. Central leaders have a greater influence than others over the network in many cases (Malm *et al*, 2008). There are three main centrality metrics: degree, closeness and betweenness. These metrics can be used in actor (that is, the analysis and comparison of individual nodes) or group (that is, the analysis of the entire network) form (Wasserman and Faust, 2007). All are discussed in the following subsections.

Degree centrality The degree centrality metric for individuals detects actors in a social network that are most socially active based on the number of people they are directly connected to. Those in a social network who know more people directly are more central in the network. The group degree centrality measures the tendency toward centralization for an entire network. The results of group degree centrality determine how structurally similar a network is to a star network structure based on first degree connections. The star network is fully centralized, such that the central node is connected to all other nodes directly, and all other nodes connect to each other through, and only through, the central node (Wasserman and Faust, 2007). The terrorists identified as degree central leaders are displayed in Figure 2. It is important to note that these leaders are affiliated with different organizations. This analysis identifies the core of Islamist terrorism as being largely al-Qaeda; however, with the inclusion of other organizations, a system of radical Islamist networks is delineated. It is also important to note that many of the core members have been captured or killed by counterterrorist forces, and that these results may not be a totally accurate representation of what the system has evolved into presently.

Figure 3 shows the overall trend of degree centrality for the entire network. The *y*-axis frequency is the number of nodes that have the specified number of adjacent[6] nodes on the *x*-axis. The majority of nodes have only one link. This is shown at the column labeled ‘1’ on

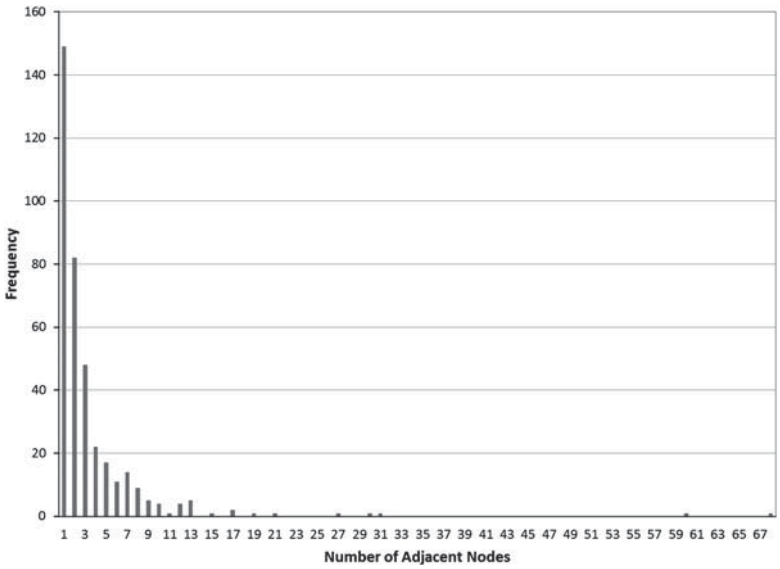

Figure 3: Degree centrality.

the *x*-axis. As the node frequency decreases, the number of links increases. The mean number of adjacent nodes is 3.62. As with the density analysis, this centrality analysis suggests that the network is relatively sparse as one might expect from a covert network, where little operational information is shared between members (Krebs, 2002). Most actors in the network have very few connections.

The group degree centralization is approximately 17per cent. As this representative network is only 17 per cent centralized, its structure is substantially different from a star network structure. There are few nodes with high connectivity; however, the connectivity for the remaining members is distributed through the entire system, which results in a decentralized network.

Closeness centrality Closeness centrality is a metric that measures how central a node is with respect to all other nodes in the network. The actor closeness centrality metric calculates the number of degrees for each node to reach all other nodes in the network. This is also referred to as the actor far-ness (Hanneman and Riddle, 2005). Closeness central nodes are leaders in the network based on their structural centrality in the system.

As group degree centrality is important in determining the centrality characteristics of a network, so is group closeness centrality; however, closeness centrality focuses on paths to all nodes in the network, not only neighbors. In the terrorist network, actors who are socially closer to all other actors in the network, not just those that are adjacent are structural leaders. This can be measured by closeness centrality. Actors who are 'close' to other actors in the network have great social reach and are located in efficient positions for transfers and diffusion in the network.

The terrorists identified to be closeness central leaders are shown in Figure 4.

The leadership of al-Qaeda and Jemaah Islamiyah are present, and many of those that have the most adjacent connections are also very central in the entire network. Osama bin

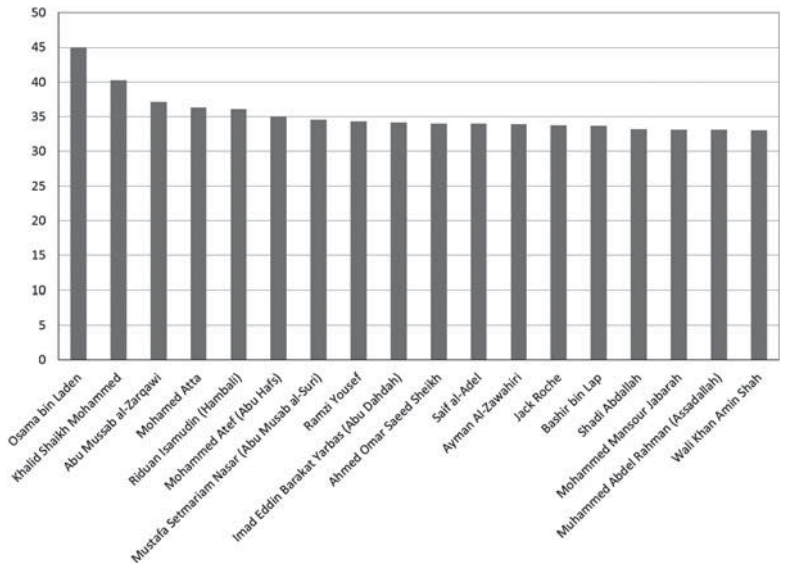

Figure 4: Leading closeness nodes.

Laden remains the most central actor in the Islamist terrorist network based on both degree and closeness values. With this second centrality analysis, a core of the network becomes more apparent.

For the entire terrorist network, the closeness centralization value is 39 per cent. This is a low level of centralization, although it is higher than the degree network centralization at 17 per cent. With this metric, the network still measures different than a star network structure, though it is more centralized when considering all degree connections.

Betweenness centrality Betweenness centrality reflects the 'betweenness' of a node, or the number of geodesics (that is, shortest paths between nodes) that traverse it. This metric can be used to identify brokers, or those controlling flows in the network. The group betweenness centrality calculates the betweenness for the entire network. Rather than considering adjacent connections, as with degree centrality, or connections to all nodes, as with closeness centrality, it focuses on the overall structure of geodesics. Similar to the other group centrality calculations the results can be used to compare multiple networks, though in this analysis the main concern of group centrality is in the number of connected nodes and social location in the system, so the group betweenness centrality is not calculated.

Terrorists that have relatively high betweenness centrality characteristics may be brokers[7]. They can be intermediaries that transfer goods or information, or can have key roles connecting leadership to those in the field, such as agent handlers. They can also be key players connecting organizations. Targeting nodes with relatively high betweenness values can help slow down or stop transfers of goods and information within the network.

Figure 5 displays the top betweenness central nodes. The similarities of betweenness results and the other two centrality metric results are evident. Osama bin Laden remains the most central actor in the network, while other al-Qaeda leadership nodes are also listed, as are agents of various organizations.

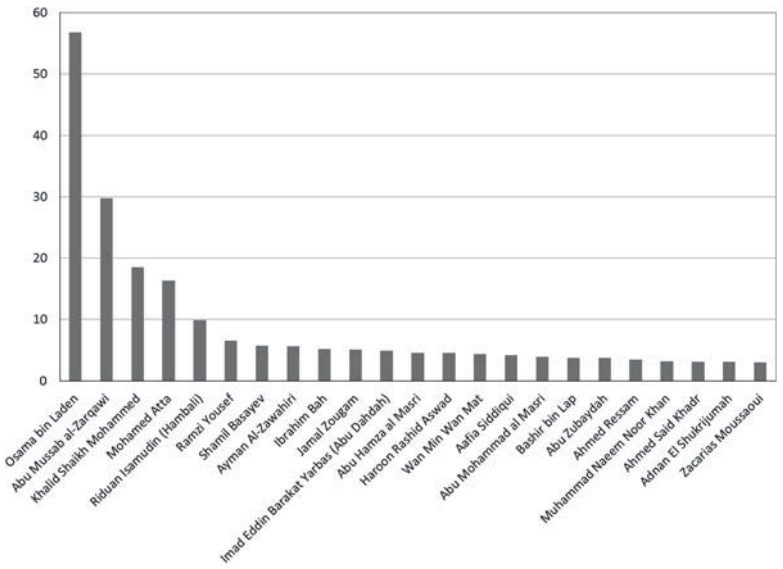

Figure 5: Leading betweenness nodes.

Implications of centrality analyses

The leadership core is defined by the results of the three centrality metrics, which are correlated at 0.00 significance. The core is well defined and composed of members from multiple groups including al-Qaeda, Jemaah Islamiyah and the Chechen Islamist insurgency. Riduan Isamudin (Hambali), Wan Min Wan Mat, Faiz Abu Bakar Bafana, Abu Bakar Bashir and Huda Bin Abdul Haq (Ali Ghufron) are members of Jemaah Islamiyah, while Shamil Basayev led the Islamist insurgence in Chechnya. Osama bin Laden, the one-time leader of al-Qaeda, is directly connected to members of Jemaah Islamiyah, Abu Sayaaf and the Chechen insurgency, among other groups such as Hizballah (Bergen, 2001). More data may reflect that the core includes members of other organizations, as many of them are connected and share activities, such as attacks and attendance at training camps (International Centre for Political Violence and Terrorism Research (ICPVTR), 2008).

Considering the top 20 nodes for each of the centrality results, eight of the same nodes are found in all three: Osama bin Laden, Khalid Shaikh Mohammed, Abu Mussab al-Zarqawi, Mohammed Atta, Riduan Isamudin, Ramzi Yousef, Imad Eddin Barakat Yarbas and Ayman al-Zawahiri. These eight terrorists have had key roles in the Islamist terrorist network that are either ideological, logistic or attack based. Seven of these eight have been captured or killed, as have many other members of the system core. The network has been substantially weakened since 9/11 (Gunaratna, 2004). However, up to this point removing well connected terrorists from the network has not been enough to dismantle it, which speaks for its resiliency.

Some of the most central nodes in this network are directly connected to large terrorist attacks. For example, Ramzi Yousef is connected to the World Trade Center attack (1993), Mohamed Atta is connected to the World Trade Center attack (2001) and Riduan Isamudin

(Hambali) is connected to the Bali Bombings (2002). This may be representative of the resources and social capital necessary to carry out large coordinated attacks.

The Islamist terrorist network is much bigger than al-Qaeda. Multiple organizations are operationally, logistically and ideologically linked. One of the major strengths of the Islamist terrorist network is in its complex, cooperative leadership and interconnectivity of organizations.

Characterizing network structure with small-world and scale-free analyses

Small-world and scale-free network models tend to focus on the identification of network classes based on structure. Small-world network theory has recently become popular, and is often recognized by the widely publicized term 'six degrees of separation', which refers to the short average social distances between people in a social network. This network model has been used to characterize networks of Hollywood actors, academics and terrorist networks. Scale-free network theory has also experienced popularity in the information age. Rather than assume that connections between people in social networks are random (such as assumed by Erdős and Rényi, 1959), this model builds a framework around network growth that incorporates individual properties and time.

Terrorist networks and sub-networks have previously been shown to exhibit small-world and scale-free characteristics (Krebs, 2002; Sageman, 2004; Medina and Hepner, 2008); however, quantitative evidence is often missing. In this section small-world and scale-free diagnostics will be applied to determine if the Islamist terrorist network can be classified as neither, either or both.

Small-world analysis

Small-world networks have structural connectivity characteristics between regular networks (that is, each node has the same number of connections and a pattern of connection is easily identified) and random networks (that is, the number and direction of connections between nodes are drawn randomly) (Erdős and Rényi, 1959). By taking a regular network and randomly rewiring it, a small-world structure will be reached. Small-world networks are characterized as having a short average degree distance between nodes, and high clustering (Watts and Strogatz, 1998).

To classify a network as a small-world, calculations of the characteristic path length (average path length) and clustering coefficient are required. The characteristic path length is a measure of the closeness of nodes in the network. It is calculated as the average social distance, by degree of geodesics, for all nodes reach to all other nodes in the network. The clustering coefficient is a measure of the connectivity of each node's neighborhood, which consists of all adjacent nodes. It can be reported in individual or group form. An individual's clustering coefficient determines the connectivity of her/his adjacent connections (for example, how many of a person's friends are connected?).

The global clustering coefficient is calculated by taking the average of all individual clustering coefficients. This statistic determines the overall neighborhood clustering for the network and can be used to compare connectivity characteristics between networks.

Table 1: Results of small-world validation test

	Actual characteristic path length	*Random characteristic path length*	*Actual clustering coefficient*	*Random clustering coefficient*
Terrorist network	4.00	4.64	0.49	0.01

The short average path length experienced by small-world networks is beneficial for efficient material and non-material flows in the network, as is the redundancy of connections between people, which is a property of high clustering. If one path is broken in the network, it is likely that there will be another path available with equal efficiency. This redundancy of connections also adds to the resilience of the network structure. The removal of links in the network will most likely not affect its flow potential. When social organizations are aware of the enhanced connectivity of this structure, its utility can be maximized.

To determine if the Islamist terrorist network conforms to a small-world structure, the characteristic path length and clustering coefficient values are compared with a random network representation that is built using the averaged characteristic path length and clustering coefficient results of 10 random networks, which are defined with the same number of nodes and connections as the terrorist network representation. Table 1 shows the results of the comparison. The clustering coefficient is much higher in the terrorist network than the random network, and the characteristic path length in the terrorist network is comparatively low. Theoretically, higher clustering should result in longer path length. This terrorist network resembles the clustering characteristics of a more regular network, while its path length characteristics resemble a random network. It does not satisfy the small-world network requirements provided by Watts and Strogatz (1998), that the characteristic path length in the network should be larger than or equal to that of a random network of the same number of nodes and connections and the clustering coefficient should be much larger than that of a random network, again with the same characteristics.

The Islamist terrorist network does not classify as a small-world, but because of its relatively short characteristic path length, it is deemed more efficient than a small-world with respect to the closeness of actors. There is some property, yet to be determined, that gives this network structure its efficiency. This could be the result of planning in the network structure formation stage. If more thought is given to structure to enhance reachability and flows, it is possible to affect the connectivity in this way. This would be evidence of a more top down authoritative structure rather than one of a decentralized, self-organizing system. It could also be the result of inherent characteristics of culture structure in certain regions of the world, such as those in developing countries, which tend to have greater respect for hierarchical social structures and tight connections within sects (Mousseau, 2002/2003).

Scale-free analysis

Scale-free networks grow by preferential attachment (that is, connections to nodes that are more ‘attractive’ will grow faster than connections to those that are less ‘attractive’). In a social network, attractiveness can be obtained in many ways. For example, individuals can attract social interactions through economic means (for example, those offering money or

resources may be contacted more in certain situations), social location (for example, in organizations, some individuals may be placed in a social location where more interaction is required), or as a personality trait (for example, some people are just more pleasant to be around). As a scale-free network grows by preferential attachment the probability for a node to gain a connection is directly proportional to the number of connections that node already has. Over time, this leads to a structure where highly connected hubs dominate network connectivity (Barabási, 2003). Many real world networks have been shown to possess scale-free properties, such as the network of actors, the World Wide Web, and the power grid of the western United States (Barabási and Albert, 1999; Goh *et al*, 2002).

To classify networks as scale-free, a power law distribution is determined through use of a log-log plot. A linear relationship between the log of the number of connections each node has and the log of the frequency (that is, the number of nodes that have that specific number of connections) determines a tendency toward preferential attachment within the network (Barabási and Albert, 1999).

The preferential attachment properties of social networks create hubs in networks because (1) some individuals are more attractive, and (2) individuals that have been members of the system longer have a greater opportunity to make more connections. Hubs have been referred to as super spreaders in epidemiological research, but have other implications. Super spreaders can be used to efficiently and effectively spread information, resources or other goods in a social network. Because of their attractiveness, they may also be used in an organization for recruitment or leadership purposes. The scale-free network structure tends to be resilient, because an attack on a network must be directed at its hubs to maximize damage. Random attacks will most likely not find a hub (Sageman, 2004).

Terrorist networks have been theorized to grow by preferential attachment in many cases, and thus are classified as scale-free networks (Medina and Hepner, 2008). There are nodes within the al-Qaeda network that are charismatic and successful in recruiting and other tasks (Sageman, 2004). The temporal characteristics of preferential attachment would also explain the high connectivity of the al-Qaeda leadership. Those that have been in the network the longest should be hubs in the network, as the scale-free model is time dependent.

To determine if the Islamist terrorist network conforms to a scale-free structure, a log-log plot is drawn with the log of the number of connections on the *y*-axis and the log of the frequency, or the number of actors that register the specified number of connections, on the *x*-axis. The scale-free structure of the Islamist terrorist network is verified by the linear pattern of log-log connectivity in Figure 6.

In spite of the small sample of terrorists (381 network nodes), the scale-free properties of the network are still approximated by the power law distribution. The majority of nodes in this network have relatively few connections. For example, the point (0,2.2) in the log-log plot is representative of all nodes that are only connected to the network by one link. There are 149 nodes that have only one connection, which comprises 39 per cent of the network.

Random attacks on the Islamist terrorist network will most likely have minimal effects, but directed attacks can be very damaging. Directed attacks have weakened the network to its present state, although the network has shown reorganization and strengthening in the FATA, Yemen and Somalia (U.S. Committee on Foreign Relations, 2010). Directed attacks must be numerous and successful to be effective, because the terrorist network is quick to repair itself, as shown when Abu Mussab al-Zarqawi was replaced with Abu Ayyub al-Masri in Iraq in 2006, and Osama bin Laden was replaced with Ayman al-Zawahiri in

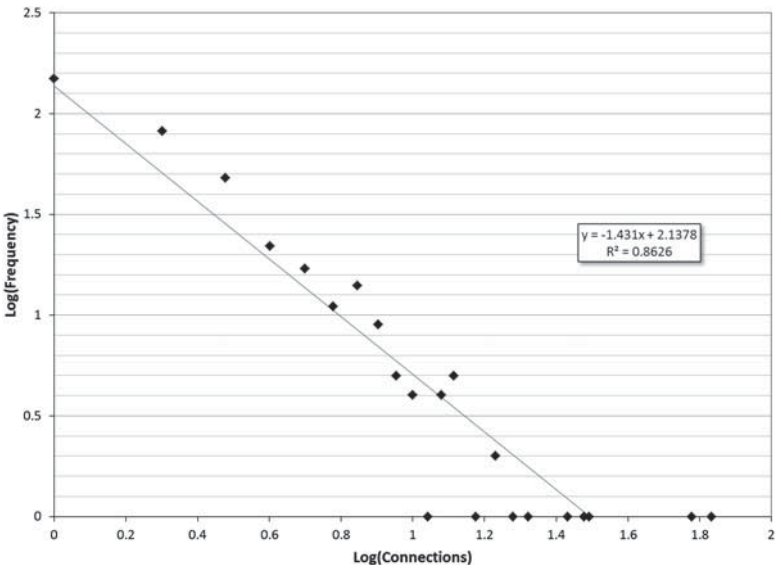

Figure 6: Log-log plot of terrorist network connectivity.

2011. The resilience of network structure based on effectiveness and efficiency of hubs is a main characteristic of scale-free networks. Non-directed and random attacks will most likely not target the hubs in the network who are responsible for much of the total connectivity.

The hubs in the network are strategic/logistic leaders, ideological/religious leaders and leaders of large attacks. This is apparent through a review of terrorist activities of these specific members (International Centre for Political Violence and Terrorism Research (ICPVTR), 2008). These nodes are somehow more attractive than other nodes in the network and are able to connect socially with more people. It is also apparent that some of these nodes have been involved with Islamist terrorist for approximately 30 years. This has given them more opportunity to gain social capital.

Osama bin Laden is the most connected hub in this representation of the network. He was the founder of al-Qaeda and acted as an ideological and strategic leader. The size, strength and staying power of al-Qaeda are testaments to bin Laden's social attractiveness. Much of his popularity in the Islamist word is due to his efforts in Afghanistan against the Soviet Union that included activities of conflict, as well as facilitation of travel and training for incoming Jihadists and monetary support. He is also given praise by Islamists for his renouncement of a potentially easy life, as he was born into a rich family, in turn for a highly devotional existence of violent Jihad (Bergen, 2001; Sageman, 2004). He is the dominant hub in the network, which in a scale-free sense can be attributed to his attractiveness and length of time in the network.

An analysis of important nodes and the resilience of the network

One of the most valuable applications of SNA is focused on targeting agents within the terrorist or other criminal networks. In a broader sense, this application is utilized to detect

Table 2: Summary of SNA results with and without Osama bin Laden and Abu Mussab al-Zarqawi

SNA metric	*With all nodes*	*Without OBL and al-Zarqawi*
Main component *n*	381	293
Density	0.01	0.01
Diameter	12	12
Mean degree centrality	3.62	3.63
Median degree centrality	2	2
Group degree centralization	0.17	0.09
Mean closeness centrality	25.85	21.83
Median closeness centrality	25.78	22.12
Group closeness centralization	0.39	0.27
Mean betweenness centrality	0.79	1.29
Median betweenness centrality	0	0
Log-log fit	0.86	0.92
Clustering coefficient	0.49	0.45
Characteristic path length	4	4.75

vulnerabilities and weaknesses in a network based on its structure and connectivity. It has been used to identify vulnerabilities of static networks, such as critical infrastructures (Grubesic and Murray, 2006), and can be applied to terrorist networks.

The Islamist network sample connectivity is dominated by two nodes in the network, Osama bin Laden and Abu Mussab al-Zarqawi (see Figures 2–5). To test the resilience of the network structure to losses of highly connected nodes, the network is analyzed with these two hubs removed and the results are compared to the results compiled for the entire network. This is a reasonable test since al-Zarqawi was killed in Iraq in 2006 (Perry *et al*, 2006) and bin-Laden was killed in Pakistan in 2011 (Baker *et al*, 2011). Al-Zarqawi was quickly replaced by Abu Ayyub al-Masri, but al-Masri did not experience the media popularity that al-Zarqawi had. Al-Masri was also killed in 2010 (CNN, 2010). Bin Laden was quickly replaced by Ayman al-Zawahiri (Sheridan, 2011).

Table 2 shows the SNA results for the Islamist terrorist network with and without bin Laden and al-Zarqawi. On the basis of these results it can be determined that the network is resilient, although the removal of the dominant nodes should not be understated.

The resilience of the terrorist system is illustrated with the comparison of statistics for the main component, group centralization, log-log fit, clustering coefficient and the characteristic path length. With Osama bin Laden and Abu Mussab al-Zarqawi removed, the connected network loses 88 nodes. It becomes a smaller network with 293 nodes, and also a slightly more dense network; however, it is still sparse with a density of 0.01 (that is, 1 per cent of the possible connections are made). The network diameter remains 12, so the network shrinks in size, but does not become more compact. The degree centrality average values remain very similar; however, the central authority of bin Laden and al-Zarqawi is apparent with the drop in closeness average values and degree and closeness group centrality values. The closeness mean and median drop from 25.85 to 21.83 and 25.78 to 22.12, respectively. Group degree centralization without bin Laden and al-Zarqawi, 0.09, is about half of the centralization for the entire network of 0.17 and the group closeness centralization drops from 0.39 to 0.27. This is expected as the two dominant hubs in the network command a large part of interaction. The network is less of a star network structure with the two nodes removed.

Table 3: Results of small-world validation test with Osama bin Laden and Abu Mussab al-Zarqawi removed

	Actual characteristic path length	*Random characteristic path length*	*Actual clustering coefficient*	*Random clustering coefficient*
Terrorist network	4.75	4.46	0.45	0.01

Although decentralized structures are often referred to as more effective for terrorist organizations, this case highlights a manifestation of decentralization (that is, a network that is both decentralized at the peripheries, but maintains a core of leadership), whereby the loss of key organizational members, which may prove to be detrimental to the system. The loss of well connected terrorists over time will work to further decentralize the Islamist terrorist system. Leaders must work to maintain communications, whether they be virtually based or face-to-face. Without these communications, the fathers of the global Jihad will lose control of the movement. Processes of decentralization are very sensitive and control can be lost quickly.

The small-world analysis was also repeated without bin Laden and al-Zarqawi. The clustering coefficient without the two nodes is 0.45 and the characteristic path length is 4.75. Table 3 shows the comparison between the clustering coefficient and the characteristic path length and the clustering coefficient from the network without the two hubs and the random representation. By meeting the requirements of a small-world network (the characteristic path length in the network should be larger than or equal to that of a random network of the same number of nodes and connections and the clustering coefficient should be much larger than that of a random network, again with the same characteristics) the network without the two dominant nodes is classified as a small-world.

For the scale-free network analysis, the goodness of fit (R^2) test[8] gives better results without bin Laden and al-Zarqawi. The least squares trend of the log-log plot is a better fit at 0.92 versus 0.86 (Figure 7). This is the case because the two nodes dominate the connectivity such that they become outliers. The network is determined to be scale-free with or without the two hubs. The resilience of the network is demonstrated through the many counter terrorism strikes that have weakened the network, but not been sufficient to dismantle it. Many of the organizational leaders have been captured or killed. The removal of terrorists such as Khalid Shaikh Mohammed in 2003 (Williams, 2010), who are integral in operations and demonstrate the scale-free hub phenomenon, have resulted in a noticeable weakening of the terrorist system. These members are responsible for connectivity, as well as planning, recruitment, diffusion and gatekeeping.

The small-world and scale-free analyses with bin Laden and al-Zawahiri removed did not produce results much different than with the two nodes. In fact, the removal of nodes transforms the network, such that it is classifiable as a small-world/scale-free network. These results speak for the resilience and efficiency of the terrorist network structure. The log-log fit and the clustering coefficient change only slightly, which is expected as these are measures of the entire structure and removing two nodes, albeit structurally important nodes, does not affect the structure of the entire network much, though this does not speak for often times immeasurable factors such as leadership skills.

The characteristic path length, before and after the removal of the two nodes, seems to be, along with the change in the main component, one of the most affected metrics, though this can be misleading. There is almost one additional degree separating nodes in the network on average. The change makes the network as structurally efficient as a small-world. Recall

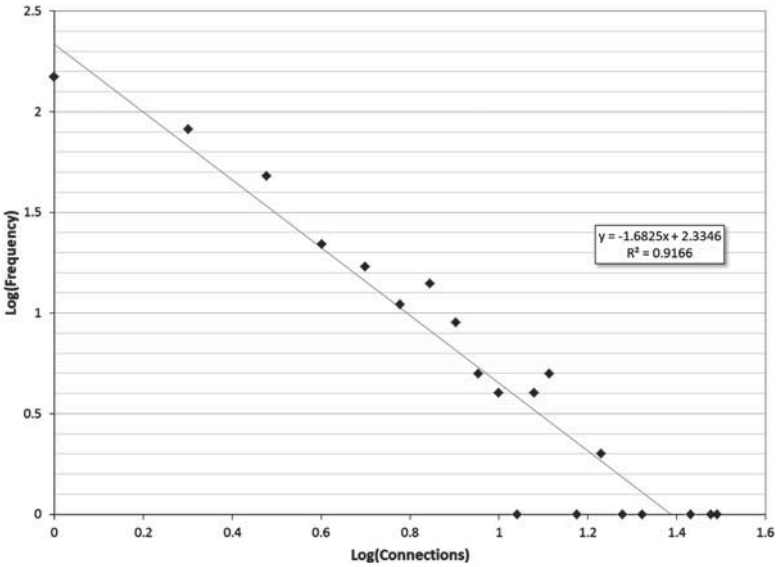

Figure 7: Log-log plot of terrorist network connectivity with Osama bin Laden and Abu Mussab al-Zarqawi removed.

that previously the network was more efficient than a small-world. So bringing the network back to the small-world structure range is not very damaging to the system.

There are no structural reasons that the Islamist network cannot operate with some of the hubs removed. The SNA results here show that removing two hubs from the network does not severely damage the network structure and with respect to some metrics, does no damage at all. The network becomes more decentralized, albeit potentially more volatile, which is expected with hubs removed. It also becomes more dense, but the diameter does not change. The network becomes a small-world and its scale-free properties are more apparent. It seems that the network has not lost much efficiency and resilience; however, there are leadership qualities that SNA does not account for. The presence of Osama bin Laden in the Islamist network may have been much more important than reflected in these analyses, which do not take into consideration leadership properties of motivation. With bin Laden removed from the network, much of the motivation to continue for some, at least on the same path, may have left with him. In this case, more nodes than expected from these results will be disconnected and fewer may join the network in the future.

The removal of nodes does not imply that the disconnected nodes will no longer be terrorists or remain active in terrorist support activities. Terrorists can find other connections to the network, or there may already be redundant connections not represented in these data. Removing highly connected nodes in the network will cause some damage, but the damage will only be maximized if redundant connections do not exist and time is not allowed for rebuilding social structures. In the case of the Islamist terrorist network, much of the organizational activity is still possible without the two nodes.

The removal of nodes and connections from the network can lead to splintering. Splintering can be an outcome with any attacks that disassemble parts of the network. The

nodes disconnected from the network can act individually, form new organizations, or if already members of other organizations, they can continue without connections to the network. Disconnections from the network can also lead some individuals to stop their terrorist activities. Influences from terrorist network connections may drive activities and capabilities, and the removal of connections to the network, for some individuals, can greatly inhibit them from continuing with terrorist operations. Connections to terrorist networks bring benefits of resources, training and the potential for adherence to ideologies that are often not available without being connected. Of course, individuals with proper training and motivation may not be hindered at all. For them operations can continue with connectivity at a minimum or even non-existent.

Abu al-Zarqawi seemed to be an effective leader of terrorism in Iraq, and while the decline in terrorist activity in Iraq after 2006 cannot be attributed wholly to his death (Medina *et al*, 2011) the loss of effective leadership may have played a role. Al-Zarqawi was quickly replaced by another member the Iraqi organization and disciple of Ayman al-Zawahiri, Abu Ayyub al-Masri (Bakier, 2010).

Al-Qaeda leadership realizes the benefits of decentralization in terrorist operations (Lia, 2008), though they must also maintain control to guide the movement. This requires the quick replacement of lost nodes in the network and communications through media as well as face-to-face interactions. In Iraq, the formation of the Islamic State of Iraq may have been an attempt, not only to strengthen terrorist forces, but also to unite multiple organizations under the same umbrella for the purpose of controlling actions and direction (Khalil, 2010). The direction of the global Jihad is much more uncertain without Osama bin Laden as a head figure, but its potential, based on the remaining social structure as illustrated through SNA, remains intact.

Conclusions

This article introduces concepts and methods of SNA that are meaningfully applied as a case study of the global Islamist terrorist network. Results from the case study analyses characterize the terrorist network structure and give insights into its strengths, weaknesses and vulnerabilities. Specifically, traditional SNA is used to delineate the overall structure of the Islamist terrorist network, as well as to identifying multiple types of leaders. Small-world and scale-free approaches are used to categorize the network and make inferences based on the categorizations. By redrawing the network without the two most connected nodes the structural resilience of the system is shown.

SNA in this case has provided valuable information on the Islamist terrorist system; however, there remains reason to be cautious of implications drawn from the results. Three main considerations are that (1) the 381 terrorists in the dataset may not be representative of the actual al-Qaeda-led terror network; (2) the data are crude in that social dynamics are not accounted for. In reality, connections and strength of connections can change over time. The data cover a long time period and do not consider the temporal aspects and changes of the network and (3) SNA does not account for social factors such as the motivation to become a terrorist or the ability to effectively radicalize potential terrorists. Social factors may be responsible for network properties that can affect operations and logistics.

Much research on the topic of terrorist and insurgent systems remains to be explored. Organizational operations for networked groups have changed owing to the increasing

field of communications technologies in the information age. Although many of the classic social network and organizational science concepts and theories still apply, new approaches and methods are required in some cases to characterize today's organizational systems. Future terrorist network research will attempt to include temporal and spatial dynamics of the system, social dynamics (that is, weighted links), and more advanced SNA techniques to overcome setbacks of data unavailability and lack of sufficient detail. There should also be more efforts made to compile the detailed data necessary for these types of studies.

Through further social network analyses weaknesses in the terrorist network may be identified, which can assist in not only breaking up the networks, but also by limiting recruitment and radicalization. It may be beneficial for researchers to take a systems approach, and conceptualize terrorist networks as open systems that evolve with and adapt to their environments. The Islamist terrorist system is constructed as a network of networks that interact with political, social and economic systems. Thus, a next step is to analyze each network in the system separately to characterize activities and identify specific weaknesses.

Terrorism research focused on terrorist organizational structures and their strengths and weaknesses can be helpful in informing policymakers on topics of global security. Many terrorist operations, such as attacks, radicalization and recruitment, and economic ventures are dependent on organizational structures and interactions with other terrorists and with non-terrorists.

This article should serve as an introduction to SNA for terrorism research, as well as an informative case study on the Islamist terrorist network for policymakers. It has provided ideas and tools for further SNA and will hopefully influence more analyses on the research topic. It is hoped that SNA here can be seen as a valuable tool, combined with larger literatures on Islamist terror, in understanding the phenomenon and ways it can be confronted.

Notes

1 The term Islamist is used here and throughout the article to describe terrorists who operate on fundamental or radical Islamic ideologies, which often includes a literal and harsh interpretation of the Quran. The end goal of Islamist terrorism has been stated by some actors to be the establishment of the global caliphate.
2 This information is no longer available by the FMS Advanced Systems Group at www.trackingthethreat.com.
3 Degrees can be defined as consecutive connections through nodes in the network.
4 A geodesic path in a social network is the shortest path, counted by number of intermediate connections, between any two nodes.
5 A graph can be conceptualized here as a quantitative representation of a real network used for visualization and analysis.
6 Adjacent is used to describe closeness n social space and represents direct social connections.
7 Brokers in social networks can be conceptualized as those who are socially located between groups or individuals that have the potential to control flows (Burt, 1992).
8 Goodness of fit (R^2) tests are used to determine how well the data fit a statistical model. In this case, the test measures the fit of the terrorist connection and frequency data against the linear log/log plot.

References

Armitage, R.L. (2002) Modification of description of 'territory of Afghanistan controlled by the Taliban' in executive order 13129, A notice by the State Department. *The Federal Register* 29 January,

http://www.federalregister.gov/articles/2002/01/29/02-2244/modification-of-description-of-territory-of-afghanistan-controlled-by-the-taliban-in-executive-order.
Arquilla, J. and Ronfeldt, D. (2001) The advent of netwar (Revisited). In: J. Arquilla and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy: Rand Report MR-1382*. Santa Monica, CA: Rand Corporation, pp. 1–25.
Baker, P., Cooper, H. and Mazzetti, M. (2011) Bin Laden is dead, Obama says. *The New York Times* 1 May, http://www.nytimes.com/2011/05/02/world/asia/osama-bin-laden-is-killed.html.
Bakier, A.H. (2010) A profile of al-Qaeda's new leader in Iraq: Abu Ayyub al-Masri. In: R. Mardini (ed.) *Volatile Landscape: Iraq and Its Insurgent Movements*. Washington DC: The Jamestown Foundation, pp. 112–114.
Barabási, A.-L. (2003) *Linked: How Everything Is Connected to Everything Else and What It Means*. New York: The Penguin Group.
Barabási, A.-L. and Albert, R. (1999) Emergence of scaling in random networks. *Science* 286(5439): 509–512.
Bergen, P.L. (2001) *Holy War Inc*. New York: The Free Press.
Burt, R.S. (1992) *Structural Holes: The Social Structure of Competition*. Cambridge, MA. Harvard University Press.
CNN. (2010) Al Qaeda confirms death of 2 top leaders. CNN, 25 April, http://articles.cnn.com/2010-04-25/world/iraq.militant.leaders.killed_1_al-qaeda-abu-ayyub-al-masri?_s=PM:WORLD.
Erdös, P. and Rényi, A. (1959) On random graphs. *Publications Mathematicae* 6: 290–297.
FMS Advanced Systems Group. (2008) Network navigator, www.trackingthethreat.com, accessed 15 April 2008.
Freeman, L.C. (1979) Centrality in social networks: Conceptual clarification. *Social Networks* 1(3): 215–239.
Goh, K-I., Oh, E., Jeong, H., Kahng, B. and Kim, D. (2002) Classification of scale-free networks. *Proceedings of the National Academy of Sciences* 99(20): 12583–12588.
Grubesic, T. and Murray, A.T. (2006) Vital nodes, interconnected infrastructures, and the geographies of network survivability. *Annals of the Association of American Geographers* 96(1): 64–83.
Gunaratna, R. (2002) *Inside al Qaeda: Global Network of Terror*. New York: The Berkley Publishing Group.
Gunaratna, R. (2004) The post-Madrid face of Al Qaeda. *The Washington Quarterly* 27(3): 91–100.
Hanneman, R. and Riddle, M. (2005) *Introduction to Social Network Methods*. Riverside, CA: University of California.
International Centre for Political Violence and Terrorism Research (ICPVTR). (2008) Global Pathfinder Database, http://www.icpvtrdatabase.org/pls/icpvtr/InterQuest, accessed 20 June 2008.
Khalil, L. (2010) Evolving trends and insurgent groups. In: R. Mardini (ed.) *Volatile Landscape: Iraq and Its Insurgent Movements*. Washington DC: The Jamestown Foundation, pp. 36–39.
Kilcullen, D. (2005) Countering global insurgency. *The Journal of Strategic Studies* 28(4): 597–617.
Koschade, S. (2006) A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism* 29(6): 559–575.
Krebs, V.E. (2002) Mapping networks of terrorist cells. *Connections* 24(3): 43–52.
Lia, B. (2008) *Architect of Global Jihad: The Life of al-Qaida Strategist Abu Mus'ab al-Suri*. New York: Columbia University Press.
Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A. and Christakis, N. (2008) Tastes, ties, and time: A new social network dataset using facebook.com. *Social Networks* 30(4): 330–342.
Magouirk, J., Atran, S. and Sageman, M. (2008) Connecting terrorist networks. *Studies in Conflict & Terrorism* 31(1): 1–16.
Malm, A., Kinney, J.B. and Pollard, N.R. (2008) Social network and distance correlates of criminal associates involved in illicit drug production. *Security Journal* 21(1): 77–94.
Malm, A., Bichler, G. and Walle, S.V.D. (2009) Comparing the ties that bind criminal networks: Is blood thicker than water? *Security Journal* 23(1): 52–74.
Medina, R. and Hepner, G. (2008) Geospatial analysis of dynamic terrorist networks. In: I. Karawan, W. McCormack and S.E. Reynolds (eds.) *Values and Violence: Intangible Aspects of Terrorism*. Berlin: Springer, pp. 151–167.
Medina, R.M. and Hepner, G.F. (2011) Advancing the understanding of sociospatial dependencies in terrorist networks. *Transactions in GIS* 15(5): 577–597.
Medina, R.M., Siebeneck, L.K. and Hepner, G.F. (2011) A geographic information systems (GIS) analysis of spatiotemporal patterns of terrorist incidents in Iraq 2004–2009. *Studies in Conflict and Terrorism* 34(11): 862–882.
Milgram, S. (1967) The small-world problem. *Psychology Today* 1(1): 61–67.

Mousseau, M. (2002/2003) Market civilization and its clash with terror. *International Security* 27(3): 5–29.
Perry, C., McIntyre, J., Starr, B., Schuster, H. and Habib, R. (2006) Autopsy performed on al-Zarqawi: U.S. military: Cell phone helped track terrorist leader. CNN, 11 June, http://www.cnn.com/2006/WORLD/meast/06/10/iraq.al.zarqawi/index.html.
Ressler, S. (2006) Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs* 2(2).
Sageman, M. (2004) *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press.
Sheridan, M.B. (2011) Zawahiri named new al-Qaeda leader. *The Washington Post* 16 June, http://www.washingtonpost.com/world/al-zawahiri-named-new-al-qaeda-leader/2011/06/16/AGNk87WH_story.html.
Sparrow, M.K. (1991) The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13(3): 251–274.
Tsvetovat, M. and Carley, K.M. (2002) Knowing the enemy: A simulation of terrorist organizations and counter-terrorism strategies. Paper presented at the CASOS Conference; 23 June, Pittsburgh, PA.
U.S. Committee on Foreign Relations. (2010) Al Qaeda in Yemen and Somalia: A ticking time bomb. One Hundred Eleventh Congress, Second Session, 21 January, Washington DC, http://foreign.senate.gov/imo/media/doc/Yemen.pdf.
Wasserman, S. and Faust, K. (2007) *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press.
Watts, D. and Strogatz, S.H. (1998) Collective dynamics of 'small-world' networks. *Nature* 393(6684): 440–442.
Williams, M. (2010) Khalid Shaikh Mohammed. *The New York Times*, 29 January, http://topics.nytimes.com/topics/reference/timestopics/people/m/khalid_shaikh_mohammed/index.html..
Xu, J., Hu, D. and Chen, H. (2009) The dynamics of terrorist networks: Understanding the survival mechanisms of Global Salafi Jihad. *Journal of Homeland Security and Emergency Management* 6(1): 1–15.

Appendix

Formula to calculate network density:

$$\Delta = \frac{2L}{g(g-1)} \tag{1}$$

where Δ is the network density, L is the number of observed links and g is the total number of nodes in the network. The denominator, $g(g-1)$, gives the total number of links possible in a directed graph. L is multiplied by 2 in the case of an undirected graph (that is, a graph where links between nodes represent a connection and interactions are non-directional). A fully connected network will have a density of 1, while a network with no links will have a density of 0 (Wasserman and Faust, 2007).

The formula to calculate degree centrality:

$$C_D(n_i) = d(n_i) \tag{2}$$

where $C_d(n_i)$ is the degree for each node i and $d(n_i)$ is the number of adjacent connections for node i Centrality values can standardized, as the interpretation of results may be dependent on the number of nodes in the network. Standardized results are reported on an index between 0 and The standardized degree centrality equation can be written as:

$$C'_D(n_i) = \frac{d(n_i)}{g-1} \tag{3}$$

where $C'_D(n_i)$ is the standardized degree centrality value for node i in the network, g is the number of nodes in the network and the denominator, $g-1$, represents all potential connections in the network for node i. Upon calculating the degree centrality for all nodes in a network, the values can be arranged, such that the list includes all network actors in order of their extent of social interaction based on their connections.

The formula to calculate the group degree centrality:

$$C_D = \frac{\sum_{i=1}^{g}[C_D(n*) - C_D(n_i)]}{[(g-1)(g-2)]} \tag{4}$$

where $C_D(n^*)$ is the largest observed centrality value and $C_D(n_i)$ is the degree centrality value for each node i. The denominator is the maximum possible of the sum of differences between the largest degree observed index value and the actor degree indices (Freeman, 1979; Wasserman and Faust, 2007). This metric reports network cenralization results between 0, which reflects a graph where all degrees are equal, such as a circle graph (that is, a graph conceptualized as nodes arranged in a circular formation and connected only to their neighbors), and 1, which reflects a graph completely centralized, such as a star graph (Wasserman and Faust, 2007).

The formula to calculate closeness centrality:

$$C_C(n_i) = \sum_{j=1}^{g} d(n_i, n_j) \tag{5}$$

where $C_C(n_i)$ is the closeness centrality for node i and $\Sigma_{j=1}^{g}\, d(n_i, n_j)$ is the sum of path distances by degree from node i to all other nodes j. In a standardized form, closeness can be written as:

$$C'_C(n_i) = \frac{g-1}{\left[\sum_{j=1}^{g} d(n_i, n_j)\right]} \tag{6}$$

where $C'_C(n_i)$ the standardized closeness for node i, given by the inverse of the summation of the number of degrees in all geodesics from the target node to every other node in the network (shown in the denominator). The numerator in the equation, $g-1$, is the network size by number of nodes (g) minus one, which represents the potential connections of the target node (Wasserman and Faust, 2007).

The formula to calculate the closeness centrality for the entire network:

$$C_C = \frac{\sum_{i=1}^{g}[C'_C(n*) - C'_C(n_i)]}{[(g-2)(g-1)]/(2g-3)} \tag{7}$$

where C_C is the group closeness centrality, $C'_C(n^*)$ is the maximum observed standardized closeness centrality, which is found by calculating the actor closeness centrality for all nodes, $C'_C(n_i)$ is the standardized closeness centrality for each node i in the network, and the

denominator represents the maximum possible value for the numerator and assures the results are between 0 and 1. Similar to degree centrality, 0 results in a network where the number of connections for each node is equal, and 1 results in a star graph where the network is completely centralized (Wasserman and Faust, 2007).

The formula to calculate actor betweenness centrality:

$$C_B(n_i) = \sum_{j<k} g_{jk}(n_i) \tag{8}$$

Where $C_B(n_i)$ is the betweenness centrality for node i, and $\Sigma_{j<k} g_{jk}(n_i)$ is the sum of all geodesics that transverse node i (Hanneman and Riddle, 2005). If multiple geodesics between two nodes and through varying nodes exist, the value of the geodesic is split, such that each between node takes its proportion of the value. For example, given three nodes that are all on separate but equal geodesic paths between a pair of nodes; each of the 'between' nodes is given 1/3 of the betweenness value, $g_{jk}(n_i)$ (Freeman, 1979).

This calculation can be normalized by the total number of geodesics in the network as:

$$normC_B(n_i) = \frac{\sum_{j<k} g_{jk}(n_i)}{g_{jk}}, \tag{9}$$

where g_{jk} is the total number of geodesics between node pairs. This metric can be further standardized to report results on an index from 0 to 1 in the form:

$$C'_B(n_i) = normC_B(n_i) / \left[\frac{(g-1)(g-2)}{2} \right] \tag{10}$$

where $C'_B(n_i)$ is the standardized betweenness centrality for node i and the maximum of $C_B(n_i)$ is given by $(g-1)(g-2)/2$.

The formula to calculate group betweenness centrality:

$$C_B = \frac{\sum_{i=1}^{g} [C'_B(n^*) - C'_B(n_i)]}{(g-1)}, \tag{11}$$

where C_B is the group betweenness centrality, $C'_B(n^*)$ is the maximum observed standardized betweenness centrality and $C'_B(n_i)$ is the standardized betweenness centrality for each node i in the network. In the range of results, a 0 occurs if all nodes have the same betweenness value and a 1 occurs in the case of a star graph (Wasserman and Faust, 2007).

The formula to calculate the characteristic path length, $L(p)$:

$$L(p) = \frac{D_g}{N_p}, \tag{12}$$

where D_g is the sum of degree values for all geodesics between node pairs, and N_p is the total number of node pairings.

The formula to calculate the clustering coefficient, $C(p)$:

$$C(p) = \frac{N_c}{N_t}, \tag{13}$$

where N_c is the number of connections between neighbors, and N_t is the total number of connections possible between individuals in a neighborhood. The target node is used only to define the neighborhood and is not included in the $C(p)$ calculation (Watts and Strogatz, 1998).