Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research

Steve Ressler

INTRODUCTION

The greatest security threat facing the United States is not from formal states, but from terrorist organizations that attack informally, using terror at any time and place, with the goal of undermining confidence in U.S. institutions and the American way of life. No longer a structured battle that can be fought with military power, the war against terrorism will be won with superior knowledge.

Due to the changing nature of homeland security issues, a new type of intelligence is needed by homeland security: social network analysis (SNA). The basis of social network analysis (also known as network science or network sociology) is that individual nodes (which, depending on the type of network, can be people, events, etc.) are connected by complex yet understandable relationships that form networks.[1] These networks are ubiquitous, with an underlying order and simple laws. Networks form the structural basis of many natural events, organizations, and social processes.

Terrorist organizations are well-suited to study using social network analysis, as they consist of networks of individuals that span countries, continents, and economic status, and form around specific ideology. Terrorist organizations are different from hierarchical, state-sponsored appointments in characteristics such as leadership and organizational structure. Social network analysis can provide important information on the unique characteristics of terrorist organizations, ranging from issues of network recruitment, network evolution, and the diffusion of radical ideas. Specifically, social network analysis can be used to understand terrorist networks, inform U.S. homeland security policy, and form the basis of a more effective counter-measure to net war.

SOCIAL NETWORK ANALYSIS

The origin of contemporary social network analysis can be traced back to the work of Stanley Milgram.[2] In his famous 1967 experiment, Milgram conducted a test to understand how people are connected to others by asking random people to forward a package to any of their acquaintances who they thought might be able to reach the specific target individual.[3] In his research, Milgram found that most people were connected by six acquaintances. This research led to the famous phrase “six degrees of separation,” which is still widely used in popular culture.

Another important step in the development of social network analysis was the work of Mark Granovetter on network structures. In his widely-cited 1973 article “The Strength of Weak Ties,” Granovetter argues that “weak ties” – your relationships with acquaintances – are more important than “strong ties” – your relationships with family and close friends – when trying to find employment.[4] Granovetter's article and subsequent research extended this argument by positing that more disperse, non-redundant, open networks have greater access to information and power than smaller,

denser, and more interconnected networks because they supply more diversity of knowledge and information.

D.J. Watts' small world hypothesis builds upon both Milgram's "six degrees of separation" concept and Granovetter's "weak ties" argument by stating that most networks in the natural and man-made world are highly clustered yet far-reaching.[5] These networks have a "clustered" center, where most nodes are neighbors, tightly interconnected. In addition, each has weak ties that can connect it to any node in the network in a few short connections. For example, if a node represents a person, a person's friendship network is generally tightly connected, with common friends, similar backgrounds, and overlaps. However, despite this "clustered" inner core, as shown with Milgram's "six degrees of separation," a person can reach a stranger in the world through only a few small steps/connections. Watts' small world argument has been extended by numerous researchers to help understand the structure and behavior of various networks, including the spread of AIDS, the collapse of financial markets, and the spread of information.[6]

The value of social network theory versus other political science and sociological approaches is its focus on the value of the network structure rather than the characteristics of the individual. While social network analysis leaves room for individuals to affect their fate, it argues that the structure of the network and relationships and ties with others in the network are more important. The network structure of an organization (in this case a terrorist organization) will affect its ability to access new ideas, recruit new individuals, and achieve sustainability. Network analysis seems to work because it provides a structural analysis while still leaving room for individual effort. In a sense, network analysis builds upon many organizational theories, since networks are just another organizational structure. As Charles Perrow discusses in his work *Complex Organizations*, many organizational theories have evolved over time in an attempt to explain the organization structures of the related era.[7] Network structure is a modern organizational structure, whose power may be built upon the idea of disintermediation. Disintermediation is the removal of the intermediary role in a process or supply chain, a proverbial "cutting out the middleman." Modern social networks are building upon this idea of disintermediation as individuals can directly connect to each other especially with the advancements of modern telecommunications and the Internet. The power of loosely structured networks is that they can move quickly and be adaptive, as they do not need to go through layers of a hierarchical chain. Disintermediation is important for terrorist networks as they have cut out layers of bureaucracy; individuals can join a network through weak ties and plan attacks through loose connections.

While social network analysis has been present in some form for decades, the concept entered popular culture in the beginning of the twenty-first century. Malcolm Gladwell's bestseller *The Tipping Point* uses basic network ideology to describe how real-world social epidemics occur, such as the popularity of Airwalk shoes and the decline of crime in New York City.[8] Gladwell describes the importance of three types of people: connectors, mavens, and salesman. Gladwell builds upon Watts' research as he describes connectors – those with wide social circles – as the hubs of the human social network and responsible for the small world phenomenon.

The use of social network analysis in the mainstream has increased with the growth of a number of new online Internet sites based on social network principles. For

example, MySpace, Friendster, and Facebook are three websites that allow users to connect with friends and friends of friends to share photos, blogs, user profiles, and messages. Especially important in teenager culture, these sites map out each user's network of friends and acquaintances. According to Alexa.com, a web trafficking service, as of April 2006, MySpace is the third most popular website in the U.S. and the sixth most popular in the world ("Top 500 Sites"). Further, similar websites have been created in the employment field. Sites such as LinkedIn allow members to map their professional connections and allow employers and employees to use their associations as references in job matching.

SOCIAL NETWORK ANALYSIS AND TERRORISM

The importance of SNA in fighting the war on terrorism was recognized even before the attacks of September 11, 2001. John Arquilla and David Ronfeldt's work *Networks and Netwars,* which was released in 2001 before the terrorist attacks, describes the increased network principles in modern criminal organizations.[9] The premise of the book is that war is no longer a head-to-head battle of two powers. There is no formal hierarchical-based enemy like the U.S.S.R. during the Cold War. Modern war is *netwar*, a lower-intensity battle by terrorists, criminals, and extremists with a networked organizational structure. These networked structures are often leaderless and able to attack more quickly. Novel, asymmetric approaches are needed to combat a network-based criminal organization.

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. Mainstream media outlets such as the *Washington Post* and the *Dallas Morning News* ran articles describing the potential benefits of network science.[10] Authors of popular press network books, such as Antonio-Laszlo Barabasi (*Linked*), were interviewed extensively, on television and radio programs, on how we could use the knowledge of social networks to fight terrorism. Further, when the National Security Agency's warrant-less eavesdropping program hit the news in 2006, 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 intercepts daily between individuals.[11]

Academic Activities

After 9/11, social network experts in academia began to look explicitly at the use of network methodology in understanding and countering terrorism. The listserv associated with the leading social network organization, International Network for Social Network Analysis (INSNA), was inundated with questions, comments, and concerns over the role of social network analysis in the fight against terrorism. In the winter of 2001, *Connections*, the social network journal affiliated with INSNA, devoted an issue to social network analysis and terrorism. In this issue, Valdis Krebs begins to map the Al-Qaeda network by collecting public available data on the Al-Qaeda hijackers and running basic network principles through computer software.[12] The rest of the articles in this issue are more or less data-free. Kathleen Carley and others describe the potential uses of social network analysis and multi-agent modeling to destabilize

terrorist networks.[13] Richard Rothenberg conjectures on the structure of the al Qaeda terrorist network based on newspaper articles and radio commentary.[14]

Since the winter of 2001, the academic world has increased the attention paid to the social network analysis of terrorism as a result of public interest and new grant money.[15] Network analysis of terrorist organizations continues to grow and can be divided into two groups: the data collectors and the modelers.

Data Collectors

Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. Valdis Krebs was one of the first to collect data using public sources with his 2001 article in *Connections*. In this work, Krebs creates a pictorial representation of the al Qaeda network responsible for 9/11 that shows the many ties between the hijackers of the four airplanes. After the Madrid bombing in 2004, Spanish sociologist Jose A. Rodriguez completed an analysis similar to Krebs' by using public sources to map the March 11th terrorist network. In his research, he found diffuse networks based on weak ties amongst the terrorists.[16]

Another bright spot is the 2004 publication of *Understanding Terror Networks* by Marc Sageman. Using public sources, Sageman collects biographies of 172 Islamic terrorist operatives affiliated with the global Salafi jihad (the violent revivalist Islamic movement led by al Qaeda). He uses social network analysis specifically on Al Qaeda operatives since 1998. This analysis yields four large terrorist clusters. The first cluster resides in the Pakistan-Afghan border and consists of the central staff of al Qaeda and the global Salafist jihad movement. The second cluster is a group of operatives located in core Arab states such as Saudi Arabia, Egypt, Yemen, and Kuwait. The third cluster is known as the Maghreb Arabs who, although they come from North African nations, currently reside in France and England. The final cluster is centered in Indonesia and Malaysia and is affiliated with Jemaah Islamiyah.[17]

Despite their many strengths, Krebs' and Sageman's works have a few key drawbacks. By dealing with open sources, these authors are limited in acquiring data. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist. This can be quite problematic as the data analysis may be misleading. If one cannot find an al Qaeda operative in the U.S. in publicly available sources, the researcher could assume there is no al Qaeda network. However, it is highly probable this is not the case, since terrorists generally try to keep a low profile before committing an attack. The data collectors can also be criticized because their work is more descriptive and lacks complex modeling tools. Fostering relationships with modelers could augment the work being conducted by data collectors, as statistical analysis might be able to take into account some of the limitations of the data and provide an additional analytical framework.

One promising activity is the development of a major terrorism web portal at the University of Arizona's Artificial Intelligence Center. This website makes social network tools and data related to terrorism publicly available.[18] One example is the Terrorism

Knowledge Portal, a database consisting of over 360,000 terrorism news articles and related Web pages coming from various high-quality terrorism Web sites, major search engines, and news portals. By providing publicly available network tools and data, the research opens itself to a number of new scholars. Academics can double-check the work of others to ensure quality. New scholars can enter the field without the lengthy time commitment and financial cost of developing basic tools and getting data. Such activities, combined with the federal government's support, will help push the field of terrorism-related social network analysis to new heights in the future.

Modelers

Complex models have been created that offer insight on theoretical terrorist networks. Kathleen Carley heads one of the largest computational model organizations that models terrorist networks, Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. Carley, along with her team of faculty and graduate students, has a number of ongoing projects in the Networks and Terrorism division that have received funding from government sources ranging from the Office of Naval Research to the Department of Defense. In a series of projects, Carley and her collaborators deal with a variety of terrorism-related issues. They looked at how to model the shape of a covert network when little information is known, through predictive modeling techniques based on inherent network structures.[19] Using a computational tool created at CASOS known as DyNet, they looked at ways to estimate vulnerabilities and destabilize terrorist networks.[20] They also developed a city-level network model of chemical and biological attacks (BioWar) in an attempt to understand how people move in networks that affect what they know, what they do, how they respond, especially when they get diseases, how they get diseases, and how they react.[21] Finally, they use network text analysis, a method 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.[22] Besides the aforementioned work, Carley and her team are beginning to look at a range of other related issues including work on the effectiveness of wiretapping programs in mapping the networks of rapidly evolving covert organizations.[23]

There has been limited work in the field of complex modeling of terrorist networks outside the work of Kathleen Carley and her associates. One group using complex models to look at terrorism issues is the researchers at the University of Arizona Dark Web Terrorism Research Center. In a series of articles, researchers at this center published a number of articles in which they used social network tools to study extremist-group web forums.[24] Through the analysis of web forum activities, they were able to construct social network maps and organization structures. In addition, in 2002, Tami Carpenter and others began to look at some of the practical issues and algorithms for analyzing terrorist networks by discussing a number of ways to construct various social network measures when dealing with covert networks.[25] Besides the aforementioned works, a few of the major social network analysis scholars such as Steve Borgatti at Boston College and David Jensen at University of Massachusetts have discussed the general implications of social network analysis of terrorist networks in invited presentation and conference talks; but they have not undertaken the issue in detail with complex modeling.

A common problem for the modelers is the issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. Modelers often do not have the best data, as they have not collected individual biographies (like Sageman) and do not have access to classified data. Many of the models are created data-free or without complete data, yet do not fully consider human and data limitations. The implication of this is that the results can be potentially misleading, as they cannot take into account behavioral and contextual issues that might affect the network structure and activity. For example, it would be quite difficult to model the network structure and evolution of al Qaeda since many of the organizations that claim ties to al Qaeda are lying and do not actually have those ties. It can be quite difficult differentiating these groups from other, truly loosely affiliated groups.

In addition, modelers often do not have a foundation in terrorist studies nor do they always work with top counter-terrorism experts. Without the help of counter-terrorism experts or a background in terrorism studies, it is difficult to turn the numbers and graphic models into interpretable results that make sense in the context of the vast literature on terrorism. The vast body of knowledge in terrorism studies created since the 1970s 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.[26]

Government Activities

Despite the seeming novelty of social network analysis, the federal government has used link analysis, a predecessor of SNA, for nearly fifty years. Karl Van Meter describes the two main types of link analysis: the village survey method and traffic analysis.[27] The village survey method was created and used by Ralph McGehee of the CIA in Thailand in the 1960s to understand family and community relationships. He conducted a series of open-ended interviews and in a short time was able to map out the clandestine structure of local and regional Communist organizations and associated "sympathetic" groups. Traffic analysis (also known as communication link analysis) began during World War II and its importance continues to this day. This technique consists of the study of the external characteristics of communication in order to get information about the organization of the communication system. It is not concerned with the content of phone calls, but is interested in who calls whom and the network members, messengers, and gatekeepers. Traffic analysis was used by the British MI5 internal security service to combat the IRA in the 1980s and 1990s and continues to be used across the world by law-enforcement agencies including the U.S. Defense Intelligence Agency (DIA) Office of National Drug Control Policy.[28]

The *Analyst Notebook* is the primary software used for link analysis. Currently on its sixth version, this software is recognized as one of the world's leading analytical tools and is employed in more than 1,500 organizations ("Contraband Enforcement"). 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. The change from single variable to multivariate analysis is quite significant when researching terrorism: a number of factors affect terrorism, not one single factor. For example, the propensity for one to participate in a terrorist activity might not be strongly affected by the single variable of being related to a terrorist member. However, 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. Multivariate analysis allows us to take into account these multiple variables and their effects when controlling for another variable.

From the outside, it is difficult to understand how social network analysis is being used in the federal government. Confidentiality prevents government social network analysts from discussing their work with professors and private companies without security clearances. Despite this lack of information, it is clear that the federal government is interested in using network techniques in fighting the war on terror. Many government agencies, such as the Defense Advanced Research Projects Agency (DARPA), U.S. Army Research Labs, the U.S. Office of Naval Research (ONR), the National Security Agency (NSA), the National Science Foundation (NSF) and the Department of Homeland Security (DHS), have funded research related to social network analysis. Also in the past few years, government agencies such as the Navy Joint Warfare Committee have created openings for network analysts. DHS has instituted the Department of Homeland Security Graduate Fellowship program for graduate students interested in terrorist-related studies. This program has funded research specifically in the field of network analysis. However, aside from these activities, the number of government employees actually using network analysis is unclear. The best evidence in this regard is the admission, by the few known government social network analysts, that social network techniques are quite prevalent but they will not discuss the specifics of this approach's use in government anti-terrorist activities.

DISCUSSION

The main limitation of social network analysis is the same that applies to any new and innovative technology: social network analysis is just one tool that can be used to understand terrorism, and is just one piece of the puzzle. Subject matter experts are needed to provide a context for the research. Furthermore, the basic assumption of network analysis regarding terrorism may not be completely valid. Despite their non-hierarchical approach, terrorist organizations are not completely organized in a network structure. There are still central headquarters and training facilities for most terrorist organizations. Also, social network analysis must attempt to address the underlying root cause of terrorism. It is helpful to understand how a network evolves and how to destabilize a network. It is more helpful, however, to understand how networks recruit participants and why people wish to join terrorist networks.

I would like to see an expansion of the research areas in which network analysis is being used with regard to terrorism. Only a limited amount of work has been completed, and there is much room for this tool to yield great insights into terrorism. I would be particularly interested to see this method used to analyze network recruitment. Network analysis could identify recruiters from peripheral participants, as well as the demographic and personal characteristics that repel – as well as draw – an individual to a terrorist organization. Are terrorist recruiters generally introduced to the organization through weak ties or strong ties? These characteristics may also affect the individual's degree of participation in terrorist activity. Such research could potentially help intelligence analysts in creating strategies to counteract terrorist recruiting initiatives.

Network analysis can also be used to understand the psychological effect of terrorism. One of the main effects of terrorism is fear, which is spread through network

structures such as media, the Internet, and personal relationships. For example, the number of ties an individual has to victims of terrorism may impact the individual's perception of the risk of terrorism. Finally, I would like to see further research on network structure evolution. It would be interesting to compare the structure of multiple terrorist networks to see how they evolve over time. The network structure may impact the ability of an organization to endure over the years and complete attacks. It is important for intelligence analysts to understand how to break up a network; they could potentially exploit the small world topology by eliminating weak ties in order to isolate the network and diminish its reach and power. The removal of individuals in key network locations may be even more important than attacking the traditional leaders of a group.

Further, I hope to see an expanded use of social network analysis among homeland security educators and practitioners. Homeland security education is in a pre-paradigm phase as a professional discipline and is being conceptualized differently among educators. Christopher Bellavita and Ellen Gordon have identified over fifty topic areas related to homeland security education; I would like social network analysis to be taught as one of the tools available in a number of these areas, including risk management and analysis, intelligence, terrorism prevention, and the sociology of homeland security.[29] Further, I would like to see increased use of social network analysis by intelligence analysts. As Bellavita has pointed out, the U.S. suffers from the fear of imagination when it focuses on the idea of prevention and we need new tools.[30] It is difficult for a hierarchical organization to cope with a widely dispersed, loosely integrated, disintermediated adversary; the U.S. government may want to consider changing some of its organizational structures to effectively fight such a foe. It may be worth experimenting with pilot programs in the intelligence community that consist of decentralized, loose networks of government employees, spanning the globe with various jobs and ideas, but focused on one goal: stopping terrorists.

The author would like to thank the Department of Homeland Security Scholars and Fellows Program for support of this research and ANSER for their help supporting this research while he was an intern there. Further, he would like to thank Laurence Raine, Joshua Sinai, and Elizabeth Vaquera for their help reading earlier drafts of this research paper.

Steve Ressler *is a member of the first class of the Department of Homeland Security Graduate Fellowship Program and president of the DHS Scholars and Fellows Alumni Program. He received his master's degree in sociology at the University of Pennsylvania, where he conducted research on social network analysis. He completed this article while a DHS Fellow intern at the ANSER Homeland Security Institute. Currently, Mr. Ressler serves as an IT auditor for the Department of Homeland Security.*

Suggested Web Links

http://www.insna.org (International Network for Social Network Analysis)
http://www.orgnet.com (Valdis Krebs' web page on social network analysis)
http://ai.bpa.arizona.edu (University of Arizona's Artificial Intelligence Center)
http://www.casos.cs.cmu.edu (Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University)

[1] Albert-Lazlo Barabasi, *Linked: The New Science of Networks* (New York: Perseus, 2002).
[2] Linton Freeman, *The Development of Social Network Analysis: A Study in the Sociology of Science* (Vancouver: Empirical Press, 2004).
[3] Stanley Milgram, "The Small World Problem," *Psychology Today,* May 1967: 60-67.
[4] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (1973): 1360-1380.
[5] D.J. Watts, "Networks, dynamics and the small world phenomenon," *American Journal of Sociology* 105, no. 2 (1999): 493-527.
[6] Mark Buchanan, *Small Worlds and the Groundbreaking Science of Networks* (New York: W.W. Norton, 2002).

[7] Charles Perrow, *Complex Organizations: A Critical Essay* (New York: Random House, 1986).
[8] Malcolm Gladwell, *The Tipping Point* (New York: Little Brown, 2000).
[9] John Arquilla and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, D.C.: RAND, 2001).
[10] J. Garreau, "Disconnect the Dots," *Washington Post,* September 17, 2001; Tom Siegfried, "Network Science Could Provide Patriotic Gains," *Dallas Morning News,* September 9, 2002.
[11] Patrick Keefe, "Can Network Theory Thwart Terrorists?" *New York Times,* March 12, 2006.
[12] Valdis Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3 (2001): 43-52.
[13] Kathleen Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Terrorist Networks," *Connections* 24, no. 3 (2001): 79-92.
[14] Richard Rothenberg, "From whole cloth: making up the terrorist network," *Connections* 24, no. 3 (2001): 36-42.
[15] See, for example, A. Abbasi and H. Chen, "Identification and Comparison of Extremist-Group Web Forum Messages using Authorship Analysis," *IEEE Intelligent Systems* 20, no. 5 (2005); Kathleen Carley, M. Dombroski, M. Tsvetovat, J. Reminga and N. Kamneva, "Destabilizing Dynamic Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Washington, D.C.: War College, 2003); Kathleen Carley, Neal Altman, Boris Kaminsky, Démain Nave and Alex Yahja, "BioWar: A City-Scale Multi-Agent Network Model of Weaponized Biological Attacks," CASOS Technical Report, CMU-ISRI-04-101 (2004); J.A. Rodriquez, "The March 11th Terrorist Network: In its weakness lies its strength," XXV International Sunbelt Conference, Los Angeles, 2005; and Y. Zhou, E. Reid, J. Qin, G. Lai, and H. Chen, "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis," *IEEE Intelligent Systems* (Special issues on artificial intelligence for national and homeland security, forthcoming).
[16] Rodriquez, "The March 11th Terrorist Network."
[17] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).
[18] Edna Reid, Jialun Quin, Wingyan Chung, Jennifer Xu, Yilu Zhou, Rob Schumaker, Marc Sageman, and Hsinchun Chen, "Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Address the Threats of Terrorism," (Working paper, 2004).
[19] Matthew Dombroski, Paul Fischbeck, and Kathleen M. Carley, "Estimating the Shape of Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Conference held at the National Defense War College, Washington D.C., 2003).
[20] Kathleen Carley, "Estimating Vulnerabilities in Large Covert Networks," in *Proceedings of the 2004 International Symposium on Command and Control Research and Technology* (San Diego, CA, 2004).
[21] Carley, et al., "BioWar."
[22] Jana Diesner and Kathleen Carley, "Using Network Text Analysis to Detect the Organizational Structure of Covert Networks," in *Proceedings of the North American Association for Computational Social and Organizational Science (NAACSOS) Conference* (Pittsburgh, PA, 2004); R. Popping, *Computer-assisted Text Analysis* (London, Thousand Oaks: Sage Publications, 2000).
[23] Maksim Tsvetovat and Kathleen Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," Workshop on Link Analysis, Counterterrorism, and Security, SIAM International Data Mining Conference (2006).
[23]Abbasi and Chen, 'Identification and Comparison"; Abbasi and Chen, *Applying Authorship Analysis to Extremist-Group Web Forum Messages* (IEEE Computer Society, September/October 2005): 67-75; Y. Zhou, et al., "U.S. Domestic Extremist Groups."

[25] Tami Carpenter, George Karakostas, and David Shallcross, "Practical Issues and Algorithms for Analyzing Terrorist Networks" (Telcordia Technologies, 2002).

[26] For history and political trends, see Ovid Demaris, *Brothers in Blood: The International Terrorist Network* (New York: Charles Scribner's Sons, 1977); Claire Sterling, *The Terror Network* (New York: Berkley Books, 1981); and Bruce Hoffman, *Inside Terrorism* (Boston: Little, Brown, and Co., 1987). Hoffman also addresses why people join terrorist groups. For psychology or terrorist attack tactics, including suicide, see Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind* (Woodrow Wilson Center Press: 1998); B. Bongar, L.M. Brown, L.E. Beutler, J. Breckenridge, and P. Zimbardo, eds., *Psychology of Terrorism* (New York: Oxford University Press, 2006); and Robert Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

[27] Karl M. Van Meter, "Terrorists/Liberators: Researching and Dealing with adversary social networks," *Connections* 24, no. 3 (2001): 66-78.

[28] Ibid.

[29] Christopher Bellavita and Ellen Gordon, "Changing Homeland Security: Teaching the Core," *Homeland Security Affairs* 2, no. 1 (2006): article 1.

[30] Christopher Bellavita, "What is Preventing Homeland Security?" *Homeland Security Affairs* 1, no. 1 (2005): article 3.