

Understanding the ways in which social networks interact is vital to establishing a system of defense. Social Network Analysis (SNA) is loosely defined by Wikipedia as “a social structure made of nodes (which are generally individuals or organizations) that are tied by one or more specific types of interdependency, such as values, visions, idea, financial exchange, friends, kinship, dislike, conflict, trade, web links, sexual relations, disease transmission (epidemiology), or airline routes.”¹ This form of critical analysis has become a vital asset to the success in the ongoing war on terror. The use of SNA, if the 3-lettered agencies could communicate amongst themselves, may have been able to prevent the attacks of 9/11. SNA can be looked at in many ways and is comprised of many parts. However, just like when you map out the data, it only makes sense when looking at the whole picture. Network theory and analytical methods are essential to SNA. The thought process of individuals contributing to a bigger network brought SNA about, and the analytical methods of how we look at networks keeps SNA going.

SNA is not useful by itself; it is informed by network theory and analytical methods. The Social Network Theory provides useful insights into the design and optimization of the network and enables predictions to be made based on the data you collect. Steve Ressler, a graduate of the first class of the Department of Homeland Security Graduate Fellowship Program conducted research on SNA at the University of Pennsylvania. In his research, Ressler argues that,

“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.”²

What I take from Ressler’s analysis is that terrorist groups, while dependant on individuals, function as singular units. In such social formations, adherence to a religious cause and interdependence upon others to achieve the aims of that cause, establishes a group identity that supplants individuality. In the case of extremists, Ressler’s point supports the idea that as long as people hold extremist values that the extremist way of life will continue. Combating

those values has become the job of America's counter-terrorism and law enforcement. Although SNA is just one of their tools, it is one of great importance. SNA allows counter-terrorist taskforces to map terrorist cells, discover those with tie ins to terrorism, predict future attacks based on people of interest inside the cell that has been mapped, and define nodes and links. SNA operates upon the premise that the first step to defeating the enemy is knowing the enemy. By becoming familiar with the social interactions and inner workings of the enemy's system of communication, counter-terrorist taskforces can better predict attacks, or behead the cell altogether.

In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, John Arquilla and David Ronfeldt look at the social aspect of the growing threat of cyberwar. In this book, the authors, combined with many other contributors, look at how analyzing networks is the future of counter-terrorist. Arquilla and Ronfeldt evaluate the usefulness of social network analysis in combating various enemy threats.

“The best solution for network disruption may be to discover possible suspects and then, via snowball sampling, map their ego networks – see whom else they lead to, and where they overlap. To find these suspects it appears that the best method is for diverse intelligence agencies to aggregate their information – their individual pieces to the puzzle – into a larger emergent map. By sharing information and knowledge, a more complete picture of possible danger can be drawn...To win this fight against terrorism it appears that the good guys have to build a better information and knowledge sharing network than the bad guys.”³

This quote wants us to focus on drawing a complete picture; the more data that can be gathered, the better SNA works. Its premise is that with better information, we make more informed decisions. When better decisions are made, there is a higher chance of successfully taking down a terrorist cell.

For SNA to be a useful resource, certain data is needed. First, identification of characteristics of networks that make criminals want to be a part of them is needed. Next, specify the critical roles that make the network function, followed by highlighting and looking at the operations of the network. Then, outline the ways to attack the network you have mapped.³

Further, contacts of people of interest are important so that you can nail down the network's tendencies. Data like names of contacts, means of communication, and the way the dots are connected help to accurately map any network. However, mapping a network is fraught with difficulty. Terrorist organizations do not advertise information on their members. This coupled with the fact that "the government rarely allows researches to use their intelligence data" makes constructing a network all the more frustrating.² What is needed to be done is a focus on SNA. If the government is going to prohibit certain people from critical data, critical errors will be made, or vital points will be missed. SNA can only to a useful tool for counter-terrorism if all the data we have is implemented. The government's expansive data on individuals should be accessible to researchers.

Dealing with data collection, there are competing public policies and legalities used to implement the mapping of networks. The USA PATRIOT act strengthens the surveillance abilities government wide. It allows the government to "eavesdrop" on those it feels are persons of interest. The ongoing debate is about whether or not it is in violation of our Freedom of speech, or the laws governing the use of warrants. These two aspects have clashed ever since the document was accepted into law. People believe that the government should not be able to just tap into their conversations. The constitution allows us to speak with whomever we want, whenever we want. But now this act lets the government know about it. The PATRIOT act is a real boost to SNA; it lets mappers have access to vital information about people's tendencies. However, the constitution prohibits SNA, because of its statements of freedom of speech. This gets into the common problem faced by anyone dealing with security today, how much information do we need to have openly available and how much do we want to hinder those we are securing with limits.

Despite this tension, SNA has been accepted as a major form of counter-terrorism, terrorists are trying to thwart the process. At one point, bin Laden had a satellite phone; however, after he realized that he could be tracked, he relied on carriers to deliver his messages. On this note, phasing out technology is a way for terrorists to figuratively behead SNA. Also, guerrilla tactics are quite effective against technological innovations. Recently, encryption techniques used by al Qaeda have become very advance. Jaikumar Vijayan, a writer for *Computerworld*, writes about Mujahideen Secrets 2, raising eyebrows about terrorist group's technological capabilities.

“Mujahideen Secrets 2 is a very compelling piece of software, from an encryption perspective, according to (Paul) Henry (Secure Computing Corp.). He said the new tool is easy to use and provides 2,048-bit encryption, an improvement over the 256-bit AES encryption supported in the original version. What makes the update especially interesting, he noted, is the fact that it can be used to encrypt Yahoo and MSN chat messages in addition to e-mails.”⁴

Encrypting this type of data could have serious consequences to network mapping. If we don't know what two parties are talking about, we have no ability to predict their movements. In addition, the use of stolen identities and aliases make mapping out these networks even more difficult. Since foreign driver's licenses are no more than paper, fake replicas with fake names are very easy to recreate.

The concept of SNA makes sense. Learning more about a network is easier when you know what it looks like, how it communicates, who it communicates with, and when it is active. An overall better profile of known terrorists will make SNA more useful. Collecting the right data, connecting it with the right people, and putting them in the right places are critical to using SNA correctly.

Works Cited

1. "Social Network." Wikipedia. 24 Feb. 2008. 25 Feb. 2008
<http://en.wikipedia.org/wiki/Social_network>.
2. Ressler, Steve. Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. Homeland Security Affairs. 2006.
3. Arquilla, John, and David F. Ronfeldt. Networks and Netwars: the Future of Terror, Crime, and Militancy. RAND Corporation, 2001.

4. Vijayan, Jaikumar. "Updated Encryption Tool for Al-Qaeda Backers Improves on First Version, Researcher Says." Computerworld. 5 Feb. 2008
<http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060939&intsrc=hm_list>.