2012

Social network analysis of terrorist networks: can it add value?

Mark Lauchs
Queensland University of Technology

Robyn L. Keast
Southern Cross University

Vy Le
Queensland University of Technology

Publication details

Postprint of: Lauchs, M, Keast, RL & Le, V 2012, 'Social network analysis of terrorist networks: can it add value?', *Pakistan Journal of Criminology*, vol. 3, no. 3, pp. 21-32.

Pakistan journal article

Social Network Analysis of Terrorist Networks: Can it add value?

What is the value of social network analysis (SNA) to the study of terrorism? The study of terrorism has increased since the attacks of September 11, 2001. This time period has coincided with the increase in personal computer processing power allowing desktop operation of network analysis programs enabling academic researchers to use SNA mechanisms to study social networks. This is still a relatively young field of study, particularly in the terrorist arena. Nonetheless, the authors suggest that it will add a valuable realm of data to help understand how terrorist groups operate and can be combated.

Terrorism occurs through highly visible acts. Yet the operation of the terror networks is largely invisible, hidden within an opaque and loose structure of individuals and groups. This invisibility shields the internal operation and functioning of the networks from scrutiny and limits understandings of how to either engage with members to negotiate mutual outcomes, or disrupt, dismantle or destroy these entities. This article is not about the detailed intelligence work conducted by intelligence agencies. Rather it asks the question of what academics can learn about the nature of terrorist networks through SNA techniques.

The nature of terrorist groups

Human society operates in networks of work, private relationships and broader social interaction. Most of these networks are mundane and open to the world. However, there are a category of

networks that are hidden from view. These *dark networks* are those where the network achievements come at the cost of other individuals, groups or societies and, in addition, their activities are both ‘covert and illegal’ (Raab and Milward, 2003). Terrorist groups fall within this category.

A distinction must be drawn at this point between the two types of dark networks. An organised crime network wants to remain invisible to all but their customers. They operate without the scrutiny of law enforcement. Terror networks, on the other hand, must have some level of visibility to achieve their goals. A terror group uses terror (fear and violence) attacks to draw attention to their political goal. These attacks are necessarily public and the group must claim responsibility to draw the nexus between the attack and their campaign. Even as acts of extortion (meet our demands or we will attack again), a terror group must identify their existence and their goal as a necessary part of the extortion technique. This does not mean that the group is entirely visible. It must keep its membership, location, organisation and finances outside the public gaze. Nonetheless sufficient study has taken place on terrorist groups to distinguish their unique characteristics which can inform SNA study.

Terrorist networks, from SinnFein to Al Quaeda, have proven to be resilient entities; resisting persistent and focused attempts to dismantle. Gupta (2008) has identified three potential areas of vulnerability related to their membership. First, terrorist groups rely upon charismatic leaders to succeed (Gupta, 2008). However, leaders can also be a point of vulnerability. Politically, "Through their vision these innovators 'connect the dots' for their followers, which not only suddenly allow them to see who they are in terms of a larger entity, but also a way out of their

current predicament." (Gupta, 2008) People have a proclivity to follow leaders but the leaders need the skills to motivate to become successful leaders. Gupta states that leaders do this by creating a group identity: framing issues in a manner that accentuates this identity through anxiety based on difference. Through this process other groups are scape-goated with the blame for all the perceived wrongs suffered by the group members and an ideal is promulgated that will right these wrongs (Gupta, 2008). Without a strong organizational structure and engrained operating framework, leaders and other core roles within networks, such as commanders (those that direct operations) and brokers (those that connect the groups with cells and supporters), are essential elements directing the work of the networks. Without these roles the terrorist network lacks the institutional capacity to survive. However, within networks leadership is dispersed, with multiple people taking on various leadership roles. This makes the location of key leaders and other central roles difficult.

Second, terror groups are supported by a particular nature of membership. There are three types of member motivations:

- *Mercenaries* (greed) are those who participate solely for personal gain.
- *Ideologues* (ideology) are those who participate primarily out of desire to help the group.
- *Captive participants* (fear) are those who participate because the cost of not participating is too high (Gupta, 2008).

If there is no money then the mercenaries will leave. If there is no leader then the ideological base of the group may dissipate. Finally, if the mercenaries and ideologues are gone then the captive participants will be free to cease involvement in the terror network. Thus, the

identification and location of funding streams and funding connectors has the potential to starve the network of the resources needed to sustain a mercenary workforce.

Third, public support is essential as a source of volunteers, money, safe houses and protection against infiltration by the government. A network gets stronger when its base grows. When a group gets large enough it can recruit captive participants. When it loses its legitimacy and core memberships it gets depleted (Gupta, 2008). Thus groups survive through tapping into existing networks such as religious groups and unions and financing, through crime, other governments and tithes from supporters (Gupta, 2008). Conversely, terror groups die off when either: their political goals become irrelevant; through loss of leadership by embarrassment through military defeat, the leader being killed or imprisoned, or if the leader changes sides; or, the group achieves its goals (Gupta, 2008). Assuming anti-terrorist organizations do not want the latter, and that they are not in a position to change broader politics, then they need to pursue a policy of cutting off the terrorist group from their base, their finance or their leader. Each of these three potential areas of vulnerability can be better facilitated and enacted by studying the network of a terrorist group.

Social network analysis (SNA)

Network analysis is an empirical tool which can be used to identify, measure, visualize and analyze the ties between people, groups and organizations (Scott, 1991). It plots relationships between individuals or entities by representing them as nodes and showing their relationships by linking nodes with lines. Lines can have different depictions to indicate characteristics of links including frequency and method of contact. The nodes and lines form a network map that reveals

relationships between members of the network such as gate keeping (controlling the network), liaisons and core and periphery members' (Sparrow, 1991). In so doing, it uncovers the often hidden or opaque patterns of interaction and enables the underlying structure of relationships to become more apparent (Cross et al., 2002). The graphical or mapping visualization capacity affords administrators and others charged with the responsibility for 'responding to terrorism' to more clearly and empirically examine the network topography, diagnose weak points and propose areas for intervention.

In addition to its visual contribution, the mathematical underpinnings of network analysis also generate network metrics that make it possible to gain deeper insights into the actual texture and operation of the networks. Social network analysis can be used to examine a network's resilience by analyzing vulnerability through identifying central nodes, the availability of alternate nodes to take the place of lost central nodes, and less-central but bridging nodes tying together remote sections of the network (Keast and Brown, 2005). Measures such as density (the level of connectivity) and centrality (the level of concentration) also provide important insights into the structural properties of dark networks.

Density is a measure of the number of actual connections compared to the total number of possible connections. Centrality measures how concentrated a network is; high concentration indicates that a small number of people control the flow of resources. Average Path Distance is an indication of how quick it is to navigate around the network. This measure provides insights into how close or removed certain actors are and, as a consequence, their level of knowledge. Closeness is a measure of the proximity that an actor has to all other actors in the network, and is

related to the flow of information within a network. Betweenness determines the shortest path distance between every pair of actors in a network, and then measures the degree to which an actor appears on those paths. Actors that control information within a network will have much higher betweenness values than those who appear on the fringes.

The study of the social network basis of covert networks precedes the modern visualization revolution by decades. Erickson (1981) noted that covert networks must be studied using these techniques. Similarly Baker and Faulkner (1993) examined the nature of white collar crime networks and drew conclusions about the nature of how such a network must operate. A RAND study by Arquilla and Ronfeldt (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, placed more emphasis on the organizational rather than social nature of the network.

SNA has already had extensive use in the analysis of organized crime groups. Since the 1930s, research into criminal interaction identified the significance of network structures in facilitating criminal activity (Sutherland, 1937). From the 1970s, studies into Italian-American and Sicilian organised crime families suggested that these groups were based upon social or familial networks, kinship ties and shared cultural values within a community (Albini, 1971, Ianni, 1972). The use of SNA as a method to analyse organised crime groups is well-motivated given that numerous scholars have argued that organised crime is, at a fundamental level, a product of overlapping and interrelated social relationships (Heber, 2009, Kleemans and de Poot, 2008, Bruinsma and Bernasco, 2004, McIllwain, 1999, Block, 1994).

Networks are seen as a more suitable structure for organised crime because they facilitate the flow of information, can adapt to changes in law enforcement responses and have the flexibility to deal with the associated risks inherent in all organised crime activities. Within an organised crime network, SNA techniques can identify network members that control information and how the removal of one or more members can inhibit the flow of information or alter the network's ability to adapt or perform at its best (Carley et al., 2002). This type of analysis is essential in destabilizing networks (Carley et al., 2002). Thus, the utility of SNA as an analytical framework is apparent given evidence that the structure of organised crime groups are shifting towards more flexible networks (von Lampe, 2009) and that the nature of information provided by SNA can potentially disrupt organised crime activity.

SNA and terror networks

One of the most important developments in the SNA field in the last decade has been the development of reliable visualization software packages that can be used on a desktop or laptop computer. The processing power of computers has made sophisticated data analysis a routine activity that can be performed with basic instruction in the packages software. It is no longer necessary for a researcher to have mastered the mathematics of SNA metrics. Most software packages like Analyst Notebook include the ability to produce SNA analytics literally with the 'click of a button'. It can, therefore, be expected that there will be a proportional growth in the use of these abilities as the price and power of SNA software increases. Visualization of a network provides a unique ability to study a network. Yang et al (2006) note that visualization of terror networks can reveal the subgroups within the network, the key players and how the members interact. Xu and Chen (2005) also noted the significance of visualization and using

SNA. However, neither of these studies uses the full potential of SNA metrics to study the nature of the groups and draw testable hypotheses for the study of terrorist networks generally.

The published studies of terrorist groups are far less extensive than those of organized crime. This may be a result of the relative inaccessibility of data. However, the publicity attached to terrorism is much greater than that for organized crime and this has allowed some researchers to construct their own datasets of terror networks. This occurs in two ways. First, detailed media coverage of terror group activities can be sufficient to build a network map. For example, Krebs (2002) was able to map the 9/11 terror network through media reports in the New York Times, the Wall Street Journal, the Washington Post and the Los Angeles Times. There are also increasingly detailed studies from independent research agencies such as RAND and especially the International Crisis Group, which can provide both intricate detail and high levels of reliability,

The arrival of accessible SNA software packages has led to a number of articles being published analyzing terrorist networks. Koschade (2006) studied Jemaah Islamiyah using SNA techniques to make significant findings about the strengths and weaknesses of the group. Mullins and Dolnik (2009) studied other Islamic terrorist groups. Memon et al (2008) found small world characteristics in terror networks. Many more studies are necessary before any reliable empirically based theories of terror networking can be developed.

Resilience of Networks

One of the most valuable contributions that academic study of terror networks can provide is an understanding of what makes a terror network resilient. The study of resilience is valuable in determining how to destabilize or break up a network. Reducing resilience increases vulnerability (Ayling, 2009). Studies of resilience should do more than just describe vulnerabilities such as central nodes or personalities. The removal of key personnel, such as the most central node, will not necessarily collapse the network (Milward and Raab, 2006). Resilient networks are flexible and adapt to survive. The adaption may take many forms from replacement of lost individuals through to a major reorganization of the network. The points of resilience are the characteristics that allow the network to avoid or recover from an attack. Thus we should be wary on conclusions about network vulnerability that assume the relationships within the network are static and do not account for adaptation. This does not mean that we should not attack a network by undermining its strength, but rather that we should avoid naïve assumptions as to what constitutes strength.

Long lasting networks are the most dangerous. Not only will they produce the largest quantity of attacks over their extended life, but they will have the longest time to learn from their mistakes, become terror veterans, and could be expected to produce the most effective attacks. Resilience is the capacity to survive environmental change and direct attack. Bakker et al (2011) proposed that resilience is ‘dynamic’ and networks should not be considered as fixed entities. When studying resilience researchers should also consider the nature of the external forces at work, the ability of a network to withstand these pressures (robustness), the ability to bounce back from

attack (rebound) and their vulnerability to attacks by an 'informed actor', that is someone who knows the network.

Most of the SNA work on resilience has been conducted on organized crime groups. In the case of such a group it refers to the ability of that group to continue its operations through a changing market and the direct interference of both competitors and policing agencies. Bouchard used environmental studies of resilience to develop a list of characteristics which are useful in determining network resilience: *vulnerability* referred to the likelihood of damage from a specific type of attack; *elasticity* is the system's ability to return to its original state after taking damage; and the network's *adaptive capacity* is its ability to change to reduce its vulnerability (Bouchard, 2007). The most common adaption by dark networks is to reduce their visibility either through reduced size or looser structures (Bouchard, 2007). Dark networks suffer unique vulnerabilities, namely, visibility attracts unwanted attention, especially from law enforcement. Visibility may not be a weakness in itself but it increases that likelihood of investigation. Visibility can occur in two ways: a large, formal network will be more visible to outsiders than a small, loose network; and, a central node (a person with many connections in the network) will be more visible than a node with less centrality because he will be associated with a greater range of activity. Not all networks have a centre of gravity, or *core*, which retains authority over the *periphery* of the network and directs its operations (Klerks, 2001, Morselli et al., 2007).

Milward and Raab (2006) point out that a dark network must follow certain steps to establish the network. First, they must find enough people for the network; a task usually met by finding

members in the same proximal group. Erickson (1981) concluded that risk can only be controlled by relying on trusted members and through the use of a strict hierarchical operational structure. Milward and Raab (2006) identified three alternative criteria of resilience. First the members needed to have character traits that supported the network. Second, the members had to be able to trust each other. Third the network is more resilient if it has *connectivity robustness*, the ability to respond and recover from losses of critical nodes.

We have already noted that hierarchies are avoided to offset the risks of visibility. However, trust sets the boundaries of dark networks. A dark network must limit its membership to those it can trust, i.e. it must be a *closed network*, made up of people with strong relationships (Burt, 2005). Members of the closed network share information about the reputation of other members. A member's reputation is determined by expectations of the person's future performance based on his or her past performance within the group; repeated good performance builds an expectation of future good performance. According to Burt, "You trust someone when you commit to a relationship before you know how the other person will behave." (Burt, 2005) A good reputation is built by emulating behavior that reflects the group's norms; norms which are built up over the social history of the group. Thus a terrorist group's members have a reputation that rates their commitment to the ideology and their trust worthiness to both maintain secrecy and reliably fulfill tasks. If a member of the group does not know a potential working partner they can obtain a reliable assessment of the person by seeking opinions other trusted group members (Burt, 2005).

Krebs (2002) mapped the terror cell responsible for the 9/11 attacks. He reached some conclusions about covert networks. Once in a conspiratorial network like a terror cell, the members rely on strong ties. They cannot afford to make new acquaintances outside the network. Krebs said that the terrorists formed strong ties in the past, for example, through school, and had such ties with all the members of the group. They do not expose these ties lest they reveal their network. The ties also allowed for redundancy; though he does not explain how. Krebs also says the same ties made the network strong and resilient, but once again did not explain how.

Williams presented two mechanisms by which networks protect themselves (Williams, 2001). Some networks defend themselves by developing buffer nodes at the periphery to protect the core from police investigation. The peripheral members undertake the high profile activity while the core members would keep such activity at arm's length to ensure deniability of any criminal action and to reduce their visibility to observers outside the network (Williams, 2001). Second, a network could be compartmentalized so that the loss of one compartment would not bring down the entire network (Lauchs et al., 2011b, Lauchs et al., 2011a). Both the structures can be revealed through visualization and SNA. But there are nuances that must be recognized, for example, having a network core does not mean that this is the locality of the network leadership. Carley, Lee and Krackhardt (2002) demonstrate that the leaders may not have the most contacts in the network; a leader may only communicate with one lieutenant who then interacts with agents and allies. In such a group the leader is protected by the more central decoy should law enforcement make assumptions about targeting group members based on centrality. Removal of a central node or a broker would still inhibit the network's operation. Removing one node may

not destroy the network if that node can be replaced by a new *emergent leader* to embody the leadership role or fill the network space (Carley et al., 2002). SNA can locate the true points of vulnerability in the network rather than simply the apparent leadership. It can also provide a clear picture of how information flows in the network.

Carley, Lee and Krackhardt (Carley et al., 2002) note that network destabilization can occur through a reduction in the rate of information flow in the network, a failure/destruction or significant slowing down of the decision making process, or a reduction in operational effectiveness – the ability to conduct its tasks. Latora and Marchiori (2004) point out that network efficiency measures how well communication flows in the network. They propose measuring the network efficiency of a group and attacking the nodes whose removal will bring about the greatest reduction in efficiency, noting that, the best node to attack is not always that which has the most connections. Once again, these flaws can be mapped in the visualization software and analysed via SNA metrics.

Conclusion

The increase in personal computer power has made it possible for academics to map and analyse complex networks such as terrorist groups. Due to the recent advent of this area of study there have been few published studies of terror networks using SNA and visualization. SNA offers an extremely useful tool for understanding how terror groups form and operate. In particular, it allows the 'hidden' or opaque structure and relations of the networks to become more visible and, therefore, open to intervention. We suggest that the most important area to study is resilience of the groups, as long lasting groups are the most dangerous to the community.

SNA helps attack the resilience of groups by identifying membership links, money movements and information flows within a network. The metrics analyse the strengths and weaknesses of a network and allow targeting of the individuals whose removal will most effectively disrupt the terror group's operations. While academics are unlikely to be studying real-time information in the same manner as intelligence agencies, they can still develop theories about terrorist group structures and operations which will help everyone better understand the groups vulnerabilities and longevity.

ALBINI, J. 1971. *The American Mafia: Genesis of a Legend,* New York, Appleton-Century-Crofts.

ARQUILLA, J. & RONFELDT, D. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica, RAND.

AYLING, J. 2009. Criminal organizations and resilience. *International Journal of Law, Crime and Justice,* 37**,** 182-196.

BAKER, W. E. & FAULKNER, R. R. 1993. The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review,* 58**,** 29.

BAKKER, R. M., RAAB, J. & MILWARD, H. B. 2011. A preliminary theory of dark network resilience. *Journal of Policy Analysis and Management***,** n/a-n/a.

BLOCK, A. 1994. *East Side-West Side: Organizing crime in New York City 1930-1950,* New Jersey, Transaction.
BOUCHARD, M. 2007. On the Resilience of Illegal Drug Markets. *Global Crime,* 8**,** 20.
BRUINSMA, G. & BERNASCO, W. 2004. Criminal groups and transnational illegal markets. *Crime, Law and Social Change,* 41**,** 79-94.
BURT, R. 2005. *Brokerage and Closure: An Introduction to Social Capital,* New York, Oxford University Press.
CARLEY, K. M., LEE, J.-S. & KRACKHARDT, D. 2002. Destabilizing Networks. *Connections,* 24**,** 14.
CROSS, R., BORGATTI, S. & PARKER, A. 2002. Making Invisible Work Visible: Using Social Network Analysis to Support Strategic Collaboration. *California Management Review,* 44**,** 12.
ERICKSON, B. 1981. Secret Societies and Social Structure. *Social Forces,* 60**,** 22.
GUPTA, D. 2008. *Understanding Terrorism and Political Violence: The life cycle of birth, growth, transformation, and demise,* London, Routledge.
HEBER, A. 2009. The networks of drug offenders. *Trends in Organized Crime,* 12**,** 1-20.
IANNI, F. 1972. *A Family Business: Kinship and Social Control in Organized Crime,* New York, Russell Sage Foundation.
KEAST, R. & BROWN, K. 2005. The Network Approach to Evaluation: Uncovering Patterns, Possibilities and Pitfalls. *Australasian Evaluation Society International Conference.* South Bank, Brisbane.
KLEEMANS, E. R. & DE POOT, C. J. 2008. Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology,* 5**,** 69-98.
KLERKS, P. 2001. The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigations? Recent developments in the Netherlands. *Connections,* 24**,** 13.
KOSCHADE, S. 2006. A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. *Studies in Conflict & Terrorism,* 29**,** 559 - 575.
KREBS, V. 2002. Uncloaking Terrorist Networks. *First Monday,* 7.
LATORA, V. & MARCHIORI, M. 2004. How the science of complex networks can help developing strategies against terrorism. *Chaos, Solitons & Fractals,* 20**,** 69-75.
LAUCHS, M., KEAST, R. & CHAMBERLAIN, D. 2011a. Resilience of a corrupt police network: the first and second jokes in Queensland. *Crime, Law and Social Change***,** 1-13.
LAUCHS, M., KEAST, R. & YOUSEPFOUR, N. 2011b. Corrupt Police Networks: Uncovering hidden relationship patterns, functions and roles. *Policing and Society,* 21**,** 18.
MCILLWAIN, J. S. 1999. Organized crime: A social network approach. *Crime, Law and Social Change,* 32**,** 301-323.
MEMON, N., HICKS, D. L., HARKIOLAKIS, N. & RAJPUT, A. Q. K. 2008. Small World Terrorist Networks: A Preliminary Investigation
Applications and Innovations in Intelligent Systems XV. *In:* ELLIS, R., ALLEN, T. & PETRIDIS, M. (eds.). Springer London.
MILWARD, H. B. & RAAB, J. 2006. Dark Networks as Organizational Problems: Elements of a Theory. *International Public Management Journal,* 9**,** 333 - 360.
MORSELLI, C., GIGUÈRE, C. & PETIT, K. 2007. The efficiency/security trade-off in criminal networks. *Social Networks,* 29**,** 143-153.

MULLINS, S. & DOLNIK, A. 2009. An exploratory, dynamic application of Social Network Analysis for modelling the development of Islamist terror-cells in the West. *Behavioral Sciences of Terrorism and Political Aggression,* 2**,** 3-29.

RAAB, J. & MILWARD, H. B. 2003. Dark Networks as Problems. *J Public Adm Res Theory,* 13**,** 413-439.

SCOTT, J. 1991. Social Network Analysis: A Handbook. London: Sage.

SPARROW, M. K. 1991. Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and CounterIntelligence,* 5**,** 255 - 274.

SUTHERLAND, E. 1937. *The Professional Thief by a Professional Thief,* Chicago, University of Chicago Press.

VON LAMPE, K. 2009. Human capital and social capital in criminal networks: introduction to the special issue on the 7th Blankensee Colloquium. *Trends in Organized Crime,* 12**,** 8.

WILLIAMS, P. 2001 Transnational Criminal Networks. *In:* ARQUILLA, J. & RONFELDT, D. (eds.) *Networks and Netwars.* Santa Monica: Rand.

XU, J. & CHEN, H. 2005. Criminal Network Analysis and Visualization. *Communications of the ACM,* 48**,** 8.