TSAS

canadian network for research on terrorism, security and society

Working Paper Series

No. 14-01

May 2014

Researching Terrorism and Counter-Terrorism through a Network Lens

Martin Bouchard and

Rebecca Nash

The Canadian Network for Research on Terrorism, Security, and Society

TSAS is supported as a national strategic initiative funded by **SSHRC** and **Public Safety Canada**, along with the following departments of the federal government:

- Canadian Security Intelligence Service (CSIS)
- Citizenship and Immigration Canada (CIC)
- Royal Canadian Mounted Police (RCMP)

TSAS also receives financial support from the University of British Columbia, Simon Fraser University, and the University of Waterloo.

 For more information, contact the Co-directors of the Centre, Daniel Hiebert, Department of Geography, UBC (daniel.hiebert@ubc.ca) and Lorne Dawson, Department of Sociology and Legal Studies, University of Waterloo (ldawson@uwaterloo.ca).

Table of Contents

TSAS

canadian network for research on
terrorism, security and society

Working Paper Series

Researching Terrorism and Counter-Terrorism through a Network Lens

Martin Bouchard

Simon Fraser University

Rebecca Nash

California State University – Long Beach

Introduction

One of the most fundamental findings of terrorism research is that terrorists are, as far we can tell, normal people. Serious analysis of their background shows they are neither poor nor rich, and most are not particularly religious except for an escalation phase in the strength of their beliefs that seems to be happening in the period leading to an event (Bakker 2006; Sageman 2004). There is no clearly defined terrorist personality (Horgan 2003), no simple profile to make individual-based predictions, and very little information available to distinguish the potential terrorist from the (relatively) non-violent supporter of a cause prior to a terrorist event.

These conclusions would not come as a surprise to criminologists who have found the same for criminals more generally. There are a host of risk factors predicting crime involvement, especially in adolescence where criminal offending is relatively common (e.g. for reviews, see Farrington 1998; Loeber and Hay 1997). But the gap between possessing any risk factor and actually becoming a criminal is wide enough to prevent empirical tests to achieve anything resembling accurate predictions (Weisburd and Piquero 2008). There is no crime "gene", both lower and upper social classes commit crime (although the poor are often over-represented in the criminal justice system), and although self-control may be lower for offending populations, not so much so that this characteristic is automatically associated with crime. In addition, many of the established sociological theories of criminal behavior start from the premise that there is little to distinguish criminals from non-criminals on fundamentals. Anomie theory, for example, establishes that a majority of individuals share similar values related to success, but that some (criminals) simply take illegal means (i.e. the means available to them) in order to reach that goal (Merton 1938). Differential association theory focuses on behavior as opposed to individuals, and posits that criminal behavior is learned the same way that most conventional behaviors are, that is, in the company of others (Sutherland 1947). If the frequency, duration, priority, and intensity of an individual's social interactions fall in favor of behavior on the illegal end of the spectrum, then that individual is more likely to adopt such behavior. The process is gradual, not necessarily lin-

ear, and a function of several interactions between social, psychological, and contextual factors.

A similarly complex set of social, political, structural, and opportunistic factors play a role in the trajectories of terrorists. To be sure, enough is known about terrorism and radicalization to imagine a point where the distinctions between terrorists and a relevant control group would be possible. Yet, the kind of fine-grained, multi-level data and longitudinal research designs to achieve this have yet to emerge. Among the slow discoveries of what makes a potential terrorist actualize his or her potential, scholars have increasingly found it hard to ignore the role of group processes and socialization in the etiology of terrorism. The social networks of friendships in which individuals are embedded, and how they identify with these social networks have shown to be lines of research most worthy of attention in understanding pathways to terrorism (Sageman 2004; 2008). If this assertion is valid, then detailed research into the nature and dynamics of social networks of potential terrorists should be a top priority among terrorism scholars. This research would examine the social networks involved in preparing specific terrorist events (e.g. Everton 2012; Koschade 2006; Krebs 2002; Magouirk et al. 2008; Rodriguez 2005), but also those developed over the entire lifetime of terrorists–including those who share similar backgrounds but never get involved in violent actions. It would also look into the social interactions that happen offline and those occurring online, including the overlap between the two and careful examinations of the significance (or lack thereof) of online behavior on radicalization processes (Ducol 2012). Ultimately, the field would also analyze continuity and change in the social networks of terrorists long after the initial events for which they became known for, including in the time period following incarceration, as convicted terrorists returning to the community.

A concern for social interactions does not stop, however, at the terrorist and the networks in which he or she is embedded. The various law enforcement agencies involved in fighting terrorism are also interacting and cooperating together in investigations, and the nature of these social interactions is likely to have an impact on effectiveness in the field. The nature of group processes involved in teams of any kind have an impact on performance, and there is no reason to believe things are different for agencies involved in fighting terrorism.

In this paper, we argue that integrating network concepts and network methods to the study of terrorism and counter-terrorism are central ingredients in bringing the field forward from theoretical, empirical, and policy perspectives. This is not exactly a new idea, although the move to study terrorist networks did not really take off until the events of 9/11 (Krebs 2002). Scholars like Marc Sageman were among the first to present a compelling argument for the use of network methods in the field of terrorism (Sageman 2004; 2008). Perliger and Pedahzur (2011), Carley et al. (2003), Asal and Rethemeyer (2006), and Everton (2012) argued for a similar focus on the empirical study of terrorist networks, each emphasizing different aspects of the strengths of a network approach, but also its limitations.

Notwithstanding these calls for the use of network methods in terrorism studies, a network approach to terrorism research is still not ubiquitous in the field, and many terrorism scholars do not come from fields with established training in social network methods (Perliger and Pedahzur 2011). Valid network data is typically more difficult to access from open sources, making developments slower than desirable. The idea that networks can also be analyzed on the other side of the spectrum, within the agencies tasked with responding to terrorism, is also rarely discussed in terrorism studies. This paper aims to contribute towards establishing network concepts and methods as critical to the development of the field.

Why Study Terrorism Through a Network Lens?

Much like some of our predecessors (e.g. Perliger and Pedazhur 2011), we believe that a network approach to study terrorism is one of the most productive ways forward for the field. There are at least three reasons why we think that it is the case. First, social ties and social influence have been argued to be central in the radicalization process of individuals (Bakker 2006; Hegghammer 2006; Sageman 2004; 2008). A compelling argument for this is the evidence that many friendship groups and social ties existed prior to devotion to a cause. Sageman (2008, 66-67) describes two pathways to friendship and terrorism, which incorporates data on the trajectories of two-thirds of his sample of 500 or so terrorists. The first pathway can be described as the collective decision of an existing friendship group to join the social movement and do something

concrete for the cause. The second is the case of the immigrant joining old childhood friends in the host country. Although the initial goal of the interaction may have been companionship, the new member may be invited to participate in terrorist activities if such activities are part of what the old friends do.

Understanding the dynamics of group formation and social influence is crux of social network analysis. The central assumption of social network analysis is that a detailed knowledge of the social structure in which individuals are embedded may be more informative in understanding behavior than common sets of attributes used to create profiles of individuals, such as age, gender, education, or socio-economic status (Knoke and Yang 2008). While group processes and small group research is informative in understanding identification, commitment, and behaviors associated with group membership, the use of network methods to map and analyze the networks as they unfold provides an additional layer of precision in connecting social ties and their influence on behavior (or lack thereof).

Second, network methods allows for an accurate depiction of the internal organization of terrorist groups without potentially false assumptions about the ways these group should function. A network approach does not impose a particular organizational structure or make assumptions about the division of labor within an organization. It lets the patterns emerge from the data, which opens up the possibility for unexpected findings, such as the discovery of information brokers among the lower levels of an organization, or the realization that the channels of communication in hierarchical organizations do not always behave in the ways expected by theory (Morselli 2009). In his initial analysis of 172 cases associated with Al-Qaeda and the Global Salafi Jihad, Sageman (2004) was shocked not to find evidence of top-down recruitment in the movement. As independent cases of homegrown terrorism became increasingly prominent in the years following 9/11, few people now expect to observe the type of recruitment expected of hierarchical organizations. The need to adopt methods amenable to track how individuals become embedded in these networks in the first place is even more salient than it was a decade ago.

Third, mapping terrorist networks can potentially improve the effectiveness of counter-ter-

rorist measures. In fact, it is often the practical implications of adopting a network approach that motivates scholars to adopt network methods, and for law enforcement agencies to share data with these scholars. The idea is attractive because in theory network methods can precisely identify which actors should be removed for maximum disruption (Borgatti 2003; Everton 2012; Joffres et al. 2011). In practice, the capacity of law enforcement agencies to accurately map a network as it exists prior to an intervention, and base its target selection on it, is rarely reported in the literature. Most disruption network studies are simulations of different possible strategies to disrupt the network (Carley et al. 2003; Chen 2012; Joffres et al. 2011; Roberts and Everton, 2011), or retrospective studies of what could have been done had network data been available prior to an intervention (Everton 2012; Malm et al. 2011). We come back on this literature in more detail below.

Conceptual Clarification

The term "network" is used in different contexts to mean different things in terrorism literature, potentially creating confusion. Networks are used in at least two ways that may seem incompatible, but in reality are not. First, the term network is used as a mode of organization based on loosely structured affiliations, to be contrasted with formal hierarchies. Organizing as a "network" means that power and decision-making is not centralized to a single cluster of individuals in the organization, but rather spread horizontally over multiple clusters of actors who have reciprocal lines of communication (Powell 1990). Network forms of organization are often seen as an adaptive response to environments where flexibility and efficiency are paramount, such as criminal, and terrorist organizations (Morselli et al. 2007).

The term "network" is also used in a broader sense to refer to the study of any kind of social structure using network methods. When used in that context, hierarchies and informal groups alike can be analyzed as "networks"–the only criterion is for entities to connect in some form and in ways that are not entirely monotonic. Social network analysis is a set of methods for the study of relations among actors (Knoke and Yang 2008), making them suitable for almost any social context. And although the form and content of social networks may be amenable to

more surprises when studying informal organizations than hierarchical ones, prior studies have shown that a systematic mapping of social relations, even in hierarchies, almost always leads to some unexpected patterns of importance. Magouirk et al.'s (2008) analysis of the evolution of the network of Jemaah Islamiyah from its formation in the 1990s through the multiple attacks of the early 2000s showed how what was perceived as a relatively hierarchical organization controlled by one-two leaders became an increasingly decentralized group with multiple centers of gravity. The perception of Jemaah Islamiyah as "led" by a single person, however, remained alive for a long time (Magouirk et al. 2008). In their analysis of Palestinian suicide bomber networks, Pedazhur and Perliger (2006) also showed how following the leader of these groups were unlikely to be productive routes of interventions. Instead, it is the brokers uncovered in the network who were most important in preparing successful attacks.

These two uses of the term are not incompatible, as "networks" may simultaneously describe a form of governance and a set of methods to describe the structure of social relations of any kind. Therefore, the qualifier used with the term is important (network organization vs. network methods). If the term is used on its own, however, the reader should have its broader meaning in mind. Unless otherwise specified, our use of the term refers to "network" in the broadest sense possible, to refer to a group of interconnected social entities of any shape or kind.

On the Network Implications of the Leaderless Jihad

Writing on the heels of the events of 9/11, Rothenberg (2002) made a series of assumptions about terrorist networks that served as a basis for subsequent publications by others (e.g. Tsvetovat and Carley 2007). While he hardly had any strong data to back his assumptions, some later passed the test using empirical data many years after formulation. Rothenberg had the Global Salafi Jihad in mind when he wrote his piece in which a command component and a multiplicity of loosely connected cells, mostly independent, form the bulk of the network. The author formulated assumptions about terrorist networks based on the little knowledge we had at the time. The first assumption, that *the entire global network is a connected component* is of particular importance in light of the "old" and "new" findings on terrorist networks.

When he made this assumption, Rothenberg (2002) was not assuming that most individuals taking part in the network are actually connected to a majority of others around the world. He was merely stating that there is at least an indirect path from most individuals to a far away, similarly minded cell. A good depiction of that idea was published two years later in Sageman's (2004) *Understanding Terror Networks*. The core of the network was the central staff formed around Bin Laden and his close allies. It was surrounded by three clusters loosely connected through the centre: the Core Arabs, the Maghreb Arabs, and the Southeast Asian cluster.

Among the many assertions made about terrorist networks post 9/11, the global network assumption is perhaps the only one that failed to survive the test of time. Not because Rothenberg (2002) was wrong at the time he wrote, but because things changed fast after the events of 9/11. In fact, the Global Salafi Network presented by Sageman (2004) was argued to have virtually disappeared in his subsequent book, *Leaderless Jihad* (Sageman 2008). The Al-Qaeda (AQ) command centre had been too risky to maintain, but more importantly, it was not necessary to have it. Instead, a transformation could be observed where "a multitude of local groups tried to emulate their predecessors by conceiving and executing operations from the bottom up" (Sageman 2008, vii). This offered the idea of a leaderless jihad where local, homegrown terrorist groups form and plan attacks often without any direct connections or support from any command centre, AQ, or otherwise. This assertion does not deny the fact that AQ leadership, in some form, may still exist. It simply argues that it does not have the same central brokering function it once had to facilitate terrorist attacks. From a practical standpoint, the more decentralized and diffuse the threat, the harder it is to prevent and detect. At the same time, homegrown terrorist groups tend to plan smaller, less lethal attacks than the AQ core groups (Helfstein and Wright 2011; Sageman 2008), which can be conceived as signs of organizational failure (McCalister 2004).

The truth is, the kind of data required to test some of these assumptions have yet to surface. A proper test would not only map the social networks immediately involved in a particular attack, but also the larger social circle of influence around each of the participants to the attack (ideally over a relatively long period of time). One of the criticisms of social network research is that it is sometimes difficult to determine the boundaries of the network (Morselli 2009). Those

chosen by the researcher appear to be artificially created, one way (e.g. arbitrary decisions by the researcher) or another (e.g. limits of the data). If the definition of social tie inclusions is broad enough, the network to be constructed around actors of interest may indeed be extremely large– large enough to stop being meaningful, at least for immediate practical purposes. Yet, mapping the larger social structure in which terrorists are embedded may be the only way to understand how they became considered as terrorists in the first place. It is also one of the most reliable ways of understanding the relative level of connections (or lack thereof) among those individuals self-identifying to the global social movement. Complicating matters even more, the social networks in which individuals are embedded also include contacts made online, especially those contacts deemed to be influential in their process of radicalization. While the role of the Internet should not be over-played as a *cause* of terrorism, its role as *facilitator* at key points in the trajectories of terrorists cannot be denied either.

Networks on the Internet

Terrorists are increasingly using the Internet to advance their goals and purposes (Coll and Glassner 2005; Conway 2002), allowing terrorist groups to form global networks of followers much beyond their capabilities before the early 90s (Lewis 2005). The Internet offers: 1) easy access; 2) little or no regulation, censorship, or other forms of government control; 3) potentially huge audiences spread throughout the world; 4) anonymity of communication; 5) fast flow of information; 6) interactivity; 7) inexpensive development and maintenance of a web presence; 8) a multimedia environment; and 9) the ability to shape coverage in the traditional mass media (Weimann 2006 30). These characteristics of the Internet have allowed modern terrorist groups to connect, communicate, plan, target, and command terrorist activities in a loosely connected, flexible, and decentralized network structure. These types of networks are extremely hard to identify and infiltrate, making it difficult to implement appropriate measures for identification and interdiction purposes (Conway 2006; Lewis 2005; Weimann 2006).

Advances in information technology are central in the creation of networks, including the new, decentralized terrorist networks emerging through their use of the Internet. By reducing the

transmission time and cost of information shared over the Internet and by increasing the amount and complexity of the information stored and shared, these advances have allowed for dispersed terrorists to communicate and coordinate their activities through online chat rooms, computer conferencing, forums, blogs, and personal websites (Zanini and Edwards, 2001). Coinciding with this view, Conway (2006) suggests that the internet enhances terrorists' capabilities to transform their group structures and generate new links. Because of the alternative space the Internet provides for communication and discussion and the hypertext nature of the web, groups can link to their internal subgroups and external organizations around the globe from their central website in seconds.

There is little empirical research into the actual networks of terrorist offenders as they occur online. There are two lines of research in this area, one seriously under-developed, focused on individuals as they connect to others via online discussion forums of other social media (Ducol 2012; Fu et al. 2010), and the other focused on extremists' groups websites and their surrounding network, usually extracted via the hyperlinks present on a website, (Bouchard et al. 2014; Burris et al. 2000; Chen 2012) but also via subscription to YouTube channels (Klausen et al. 2012). The research on online terrorist networks is best represented by the Dark Web project led by Hsinchun Chen (2012). In 2005, Zhou, Qin, Lai, Reid, and Chen proposed a semi-automated methodology that combines the efficiency of automatic data collection and the accuracy of manual collection for identifying, classifying, and organizing extremist website data. Starting from a seed website, the web crawler finds the hyperlinks found in the html of a web domain, and follows them through in order to create the network. The end result is a network of web-servers, the webpages contained within them, and the links between these webpages such that the data retrieved on the Internet by the web crawler can be used to map and analyze terrorist and extremist networks (Bouchard et al. 2014). Important to note here is that the entire process described in Chen's (2012) research and colleagues is automatic with little input from the user. The Dark Web project incorporates multilingual data mining, text mining, and web mining techniques to collect the most comprehensive collection of data generated by terrorist groups across the globe, including web sites, videos, forums, chat rooms, blogs, social networking sites to name some (Chen

2012). The Dark Web project has spawned several research studies on the nature of terrorist' use of the Internet and their online networks (e.g. Xu and Chen 2008; Qin et al. 2006; Zhou et al. 2005; Zhou et al. 2007). For example, Zhou, Qin, Lai, and Chen (2007) developed a web mining method of online extremist forums, while and Xu and Chen (2008) applied network topological analysis methods to study the design of online terrorist networks. The merge of content and network analysis in researching these websites and forums has yet to be fully developed.

Terrorist Network Disruption: Issues and Prospects for Counter-Terrorism

One of the benefits of a network approach to terrorism is the opportunity to link it to intervention efforts, which we label here as network disruption studies. The starting point of disruption studies is to consider the removal of key nodes (or key links between actors, or clusters of actors) in the network in order to decrease the network's efficiency and if possible, make the network dysfunctional. One issue with many disruption studies is the lack of theoretical guidance orienting the target selection process. Actors may be valuable to a network for a variety of reasons, and what distinguishes "key players" from actors that can more safely be ignored may depend on 1) the goals and priorities of law enforcement, and 2) the capacity of the network to recover (i.e. network resilience). Actors can be valuable because they have many connections in the network (hubs), or because they connect otherwise unconnected parts/members of the networks (brokers), or because they bring unique resources to the network, whether these resources represent social, human, or financial capital.

The majority of disruption studies include centrality measures, but fail to consider the resources or "value" that individuals bring to the network in their assessment (Carley et al. 2003). Schwartz and Rouselle (2009) solved this issue in designing a measure that takes both the structural location of an actor in the network and his or her "value" based on criteria relevant to the goals of the agencies planning the intervention. Labeled as "network capital", this measure takes into account both the structural location of actors and the resources they bring to the network based on parameters to be determined by the analysts. For online child pornography networks,

for example, network capital includes the popularity of a website in numbers of other websites hyperlinking to it, but also the severity of the content displayed on it (Westlake et al. 2011). For terrorist networks it is easy to imagine a composite measure of network capital that includes both network importance and the quality or scarcity of the resources brought by an actor, including funds, a particular skillset such as bomb making, or a unique contact with a corrupted official (see Carley et al. 2003). Magouirk et al. (2008) certainly had some of these considerations in mind when they chose to represent the importance of actors in the Jemaah Islamiyah networks based on their reputation as opposed to their network centrality. Similarly, Roberts and Everton's (2011) construction of Noordin Top's network is a fine example of network scholars purposefully designing network data collection and coding strategies to take the wide variety of roles and affiliations of terrorists into account, offering a rare amount of flexibility to researchers thinking about disruption issues from a variety of angles. And their efforts at classifying network-oriented, counter-terrorism strategies represent one of the few contributions of network disruption studies at the conceptual and practical levels. Still, much more work needs to be done to validate some of the assumptions built in their classification model, most likely in the form of evaluation studies where changes in terrorist networks are followed before, during, and post intervention (Carley et al. 2003; McCulloh and Carley 2011; Everton and Cunningham 2013).

As Roberts and Everton (2011) remind us, any intervention against terrorist groups carries its fair share of risks and potential perverse effects. A pure data-oriented approach to network disruption may not capture the local sensibilities and other idiosyncrasies of a particular group and its situation, thereby potentially exacerbating events.. While a network approach is far from immune to errors and omissions, this approach also has the (rarely used) potential to examine and map what those unintended consequences may be well in advance of making an intervention. For example, it is possible to make a prediction on who is likely to replace a leader who has been killed or captured, and how the network is likely to adapt post-intervention. Networks change over time (and some would say "all the time") for both endogenous and extragenous reasons, and the lessons emerging from full consideration of network dynamics on disruption have yet to permeate the field (for potential solutions, see Carley et al. 2003; Everton and Cunningham

2013; Tsvetovat and Carley 2005).

Conclusion

The unfortunate deaths and destruction from the September 11, 2001 terrorist attacks have left an indelible impression on the world. The events that unfolded on that day were the catalyst for the emergence of a "new" terrorism and the realization that current counter-terrorist measures are ill-equipped in combating this emergent new terrorist threat. For instance, several researchers note that terrorist groups have shifted from rigid, hierarchical designs to more amorphous, horizontal, networked structures; in turn, these have impacted their operations, decision making, and targeting (Arquilla, Ronfeldt, and Zanini 1999; Asal and Rethemeyer 2006; Hoffman 2002; Sageman 2004; Zanini and Edwards 2001). Before 9/11, Al Qaeda was a centralized organization "with a clear, distinct center of gravity", with a very noticeable, outspoken core leadership (Sageman 2004). However, after 9/11, and in response to traditional counter-terrorist measures today, terrorist groups such as Al Qaeda have become decentralized, loosely connected networks. They appear resilient to traditional counter-terrorist measures, and have an increasing presence on the Internet (Conway 2006; Denning 2011; Lewis 2005; Sageman 2008). Counter-terrorism measures must adapt to the changing nature of the highly adaptive new terrorism, but only after it has gained a detailed understanding of the networks in which terrorists are embedded.

The importance of a network approach to the study of terrorism can be summarized in three points. First, networks are of great consequence in the whole life trajectory of terrorists–from the radicalization process to the planning and execution of terrorist events. Second, a network approach offers a more powerful framework to describe the variety of structures found in terrorist groups as they actually are. Third, approaching terrorist groups as networks allows researchers the opportunity to better measure concepts such as leadership and influence within the group, and allows for unexpected patterns in the sources of power within a group to emerge. Similarly, it avoids making false assumptions about cohesion within the group (e.g. do all members know and interact with each other?), and the extent to which members of the group actually connect to

a wider network of external influences (e.g. is Al-Qaeda Central indirectly involved in this attack?).

The improved understanding of terrorism via the network approach has important practical implications for counter-terrorism policies as well. For one, the effects of these interventions can be simulated and as such, be much better understood. And if the true sources of influence within terrorist networks are not solely the one derived from the leaders in name, then interventions targeting specific individuals stand to gain both in relevance, and in potential effectiveness.

References

Arquilla, J., D. Ronfeldt, and M. Zanini. 1999. Networks, netwar and information-age terrorism. In *Countering the new terrorism* edited by I. Lesser, B. Hoffman, J. Arquilla, D. Ronfeldt, M. Zanini & B. Jenkins, 39-84. Santa Monica, CA: Rand. http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf.

Asal, V., and R.K. Rethemeyer. 2006. Researching terrorist networks. *Journal of Security Education* 1 (4): 65-74.

Bakker, E. 2006. *Jihadi terrorists in Europe their characteristics and the circumstances in which they joined the jihad: An exploratory study*. Hague, Netherlands: Netherland Institute of International Relations Clingendael.

Bouchard, M., K. Joffres, and R. Frank. 2014. Preliminary analytical considerations in designing a terrorism and extremism online network extractor. In *Computational Models of Complex Systems* edited by V. Mago and V. Dabbaghian, 171-184. New York, NY: Springer.

Carley, K., M. Dombroski, M. Tsvetovat, J. Reminga, and N. Kamneva. 2003. "Destabilizing Dynamic Covert Networks". In *Proceedings of the 8th international Command and Control Research and Technology Symposium, 2003.* Washington, DC: National Defence University.

Chen, W. 2012. *Dark web: Exploring and data mining the dark side of the web*. New York, NY: Springer.

Coll, S., and S. B. Glassner. 2005. Terrorists turn to the web as base of operations. *The Washington Post,* August 7. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html.

Conway, M. 2002. Reality bites: Cyberterrorism and terrorist 'use' of the internet. http://www.firstmonday.org/Issues/issue7_11/conway/index.html.

Conway, M. 2006. Terrorist 'use' of the Internet and fighting back. *Information & Security. An International Journal* 19: 9-30.

Denning, D. E. 2011. Terror's web: How the Internet is transforming terrorism. In *Handbook on Internet Crime* edited by Y. Jewkes and M. Yar, 194-213. Portland, OR: Willan Publishing.

Ducol, B. 2012. Uncovering the French-speaking jihadisphere: An exploratory analysis. *Media, War and Conflict* 5 (1): 51-70.

Everton, S.F. 2012. *Disrupting Dark Networks.* Cambridge, UK: Cambridge University Press.

Everton, S.F., and D. Cunningham. 2013. Detecting significant changes in dark networks. *Behavioral Sciences of Terrorism and Political Aggression* 5 (2): 94-114.

Farrington, D. 1998. Predictors, causes, and correlates of male youth violence. *Crime and Justice: An Annual Review of Research* 24: 421-475.

Hegghammer, T. 2006. Terrorist recruitment and radicalization in Saudi Arabia. *Middle East Policy* 13 (4): 39-60.

Helfstein, S., and D. Wright. 2011. Covert or Convenient? Evolution of Terror Attack Networks. *Journal of Conflict Resolution* 55 (5): 785-813.

Hoffman, B. 2002. Rethinking terrorism and counterterrorism since 9/11. *Studies in Conflict & Terrorism* 25 (5): 303-316.

Horgan, J. 2003. The search for the terrorist personality. In *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences* edited by A. Silke, 3-28. Chichester, UK: John Wiley and Sons Ltd.

Joffres, K., M. Bouchard, R. Frank, and B. Westlake. 2011. "Strategies to Disrupt Online Child Exploitation Networks". In *Proceedings of the EISIC - European Intelligence and Security Informatics*, 2011, 163-170. Athens, Greece: Hellenic American University.

Knoke, D. and S. Yang. 2008. *Social network analysis, 2nd ed*. Los Angeles, CA: Sage Publications.

Koschade, S. 2006. A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict and Terrorism* 29 (6): 559-575.

Krebs, V. 2002. Uncloaking terrorist networks. *First Monday* 7 (4). http://firstmonday.org/ojs/index.php/fm/article/view/941/863/.

Lewis, J.A. 2005. "The Internet and Terrorism". In *Proceedings of the Annual Meeting (American Society of International Law),* 2005, 99: 112-115. Washington, DC: Lowes L'Enfant Plaza Hotel.

Loeber, R., and D. Hay. 1997. Key issues in the development of aggression and violence from childhood to early adulthood. Annual Review of Psychology 48: 371-410.

Magouirk, J., S. Atran,, and M. Sageman. 2008. Connecting terrorist networks. *Studies in Conflict and Terrorism* 31 (1): 1-16.

McAllister, B. 2004. Al Qaeda and the innovative firm: Demythologizing the network. *Studies in Conflict & Terrorism* 27: 297–319.

McCulloh, I., and K. Carley. 2011. Detecting change in longitudinal networks. *Journal of Social Structure* 12: 1-37.

Merton, R.K. 1938. Social structure and anomie. *American Sociological Review* 3 (5): 672-682.

Morselli, C. 2009. *Inside Criminal Networks*. New York, NY: Springer.

Morselli, C., C. Giguere, and K. Petit. 2007. The efficiency/security trade-off in criminal networks. *Social Networks* 29 (1): 143-153.

Pedahzur, A., and A. Perliger. 2006. The changing nature of suicide attacks: A social network perspective. *Social Forces* 84 (4): 1987-2008.

Perliger, A., and A. Pedahzur. 2011. Social network analysis in the study of terrorism and political violence. *Political Science and Politics* 44 (1): 45-50.

Powell, W.W. 1990. Neither market nor hierarchy: Network forms of organization. In *The Sociology of Organizations: Classic, Contemporary, and Critical Readings* edited by M.J. Handel, 315-330. California: Sage Publications.

Qin, J., Y. Zhou, E. Reid, G. Lai, and H. Chen. 2006. Analyzing terror campaigns on the internet: Technical sophistication, content richness, and web interactivity. *International Journal of Human-Computer Studies* 65: 71-84.

Roberts, N. and S. Everton. 2011. Strategies for combating dark networks. *Journal of Social Structure* 12: 1-32.

Rodriguez, J.A. 2005. The March 11th terrorist network: In its weakness lies its strength. http://www.ub.edu/epp/redes/redes.htm.

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

Sageman, M. 2004. *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. 2008. *Leaderless Jihad: Terror networks in the twenty-first century.* Philadelphia, PA: University of Pennsylvania Press.

Sutherland, E.H. 1947. *Principles of criminology, 4th edition*. Chicago, IL: Lippincott.

Tsvetovat, M., and K. Carley. 2005. Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence. *Journal of Social Structure* 6: 1-38.

Tsvetovat, M., and K. Carley. 2007. On effectiveness of wiretap programs in mapping social networks. *Computational and Mathematical Organization Theory* 13: 63-87.

Weisburd, D., and A. Piquero. 2008. How well do criminologists explain crime? Statistical modeling in published studies. *Crime and Justice: An Annual Review of Research* 37: 453-502.

Westlake, B., M. Bouchard, and R. Frank. 2011. Finding the key players in online child exploitation networks. *Policy and Internet* 3 (6): 1-32.

Xu, J., H. Chen, Y. Zhou, and J. Qin. 2006. The topology of the dark web of terrorist groups. *Communications of the ACM* 51 (10): 58-65, 200.

Zhou, Y., J. Qin, G. Lai, and H. Chen. 2007. "Collection of U.S. Extremist Online Forums: A Web Mining Approach". In *Proceedings of the 40th Hawaii International Conference on System*

Sciences, Waikoloa, Hawaii, January 3-6, 2007. http://www.computer.org/comp/proceedings/hicss/2007/2755/00/27550070c.pdf.

Zhou, Y., J. Qin, G. Lai, E. Reid, and H. Chen. 2005. "Building Knowledge Management System for Researching Terrorist Groups on the Web". Paper presented at *Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE, August 11-15, 2005*, 2524-2536. Red Hook, NY: Curan Associates Inc.