Emerging Trends in Social Network Analysis of Terrorism and Counterterrorism

DAVID KNOKE

Abstract

A key issue in tracking transnational terror trends is the utility of social network analysis, both as a theoretical perspective and as a methodological toolkit, for understanding and assessing terror organizations, and for developing counterterror policies and practices to detect and disrupt terror attacks. Foundational efforts were case studies of particular groups or operations, culling data from newspaper reports and court trial documents, then creating matrix files for analysis with social network computer programs. Mathematicians, game theorists, and computer scientists are dramatically expanding research beyond foundational case studies of terrorist networks. Much of their work centers on devising strategies for counterterror organizations to destabilize clandestine organizations. They develop elegant and precise mathematical models and computer algorithms, then systematically change parameters to assess capabilities of detecting and disrupting terrorist activities under varying conditions. Key issues for future network research include: conducting rigorous comparative analyses of four historical waves of modern terrorism for clues about the present and future waves; building more comprehensive, cohesive, and integrated theoretical models capable of explaining the formation, structure, and consequences of terrorist networks; developing new methods of measuring network relations among terrorists; performing more laboratory experiments as an alternative to collecting inaccessible and dangerous field observation data; and creating large, high-quality relational datasets to test social network theories of terrorism.

INTRODUCTION

Although terrorism recurs throughout human history, the recent wave of transnational jihadism arose over the past four decades and shows few signs of abating. The social structures and dynamics of both terrorist networks and counterterror organizations coevolved and continue their mutual adaptations to changing environments and innovative technologies. A key issue in tracking transnational terror trends is the utility of social network analysis, both as a theoretical perspective and as a methodological toolkit,

Emerging Trends in the Social and Behavioral Sciences. Edited by Robert Scott and Stephen Kosslyn.
ISBN 978-1-118-90077-2.

for understanding and assessing terror organizations, and for developing counterterror policies and practices to detect and disrupt terror attacks. Advances in terrorism research have implications for investigating and thwarting other types of criminal clandestine, covert, and dark networks, such as arms-trafficking, diamond smuggling, human and sexual trafficking, nuclear proliferation, toxic waste disposal, and trade in endangered species. These applications have broader significance for the many professions and fields contributing to terrorism studies, including sociology, criminology, organization studies, political science, international relations, military science, mathematics, computer science, security studies, law, and law enforcement.

The myriad definitions of terrorism typically emphasize the political objectives of individuals or groups engaged in violent acts. These goals often derive from an ideology, such as anarchism or Marxism, or from group identification, such as nationalist or religious affiliation. This article concentrates on emerging trends in transnational terror networks and counterterror efforts against them. Title 22 of the United States Code defines international terrorism as "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents" which involves citizens or the territory of more than one country (U.S. Department of State, 2013, p. 293). Further, section 219 of the United States' Immigration and Nationality Act defines a "foreign terrorist organization" (FTO) as one that "must engage in terrorist activity … or terrorism … or retain the capability and intent to engage in terrorist activity or terrorism" and "must threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States" (p. 244). For 2012, the State Department designated 51 FTOs fitting this definition. On the basis of their thumbnail sketches, 36 FTOs were Islamist; three Colombian; two Irish; two Greek; and one ach Basque, Filipino, Israeli, Japanese, Kurdish, Peruvian, Sri Lankan, and Turkish. Of course, many hundreds of terrorist groups operate within national or subnational territories.

FOUNDATIONAL RESEARCH

Although Claire Sterling's *The Terror Network* (1981) described links among Palestinian and Irish Republican Army terrorists and the KBG in the 1970s, academic researchers began applying social network methods to terrorist networks after the 9/11 Al-Qaida attacks inside the United States. Foundational efforts were case studies of particular groups or operations, culling data from newspaper reports and court trial documents, then creating matrix files for analysis with social network computer programs. Within weeks after 9/11, Valdis Krebs (2001, 2002) constructed a seminal two-dimensional diagram (graph) showing the connections among the 19 hijackers and 43 accomplices who provided money, skills, and information. Mohammed Atta, leader of the field operations, was the central actor and the four pilots formed a tight clique. Every hijacker was two or fewer steps from two others, Nawaf Alhazmi and Khalid Almihdhar. The Central Intelligence Agency knew these two men had participated in a January 2000 planning meeting with top Al-Qaida leaders in Malaysia. But, the CIA failed to inform the Federal Bureau of Investigation when the men returned to America (National Commission, 2004). The Intelligence Community's failure to track these suspects was a missed opportunity to detect and possibly apprehend the 9/11 network before it struck. Krebs (2001) concluded that a "dense under-layer of prior trusted relationships made the hijacker network both stealth and resilient," but "concentrating both unique skills and connectivity in the same [persons] makes the network easier to disrupt—once it is discovered." In another foundational analysis, Marc Sageman (2004) used biographies of 366 participants in the "global Salafi network" to identify ties based on kinship, friendship, religious, and work relations. He found four large clusters built around highly connected "hubs": Al-Qaida Central Staff, Maghreb Arabs (North Africa), Core Arabs (Saudi Arabia, Egypt, Yemen, Kuwait), and Southeast Asians (Indonesia and Malaysia). However, his only network diagram was schematic, rather than based on actual relations among specific individuals.

Other network researchers constructed matrices and diagrams of known connections within terrorist cells. Steven Koschade (2006) found a high density of ties (0.43) among 17 members of a large Jemaah Islamiyah cell that bombed a Bali, Indonesia, nightclub in 2002. The structure was very centralized, revealing a "mix between efficiency and covertness" (p. 570). Field commander Samudra and logistics commander Idris had exceptionally high scores on three centrality measures, which placed both men at the center of the graph. Samudra had "the highest ability to access others, and the greatest control over the flow of information in the network .... Exclusively due to his connection to Team Lima [support group], and the suicide bomber Arnasan" (p. 571). Given the high connectivity inside the cell, detection and capture of any member by law enforcement might have exposed the entire group and thwarted the bombing. By comparing four terrorist cells operating in or against Australia, Koschade (2007) concluded that cells focused on efficiency rather than covertness were more successful in carrying out attacks. Betweenness centrality (control over information flow) was crucial for identifying cell leaders. A broader analysis of Jemaah Islamiyah mapped a half-dozen leadership, kinship, and attack networks from 1993 to 2005 (Magouirk, Atran, & Sageman, 2008).

A network of 45 jihadis conducted the March 11, 2004, Madrid train bombings (Jordán, Mañas, & Horsburgh, 2008). Although that operation was inspired by Osama bin Laden's explicit threat to target Spain because of its military involvement in the Iraq War, the participants had few connections to Al-Qaida. Instead, it was a largely grassroots action organized by three immigrants of Moroccan and Tunisian origins. Its decentralized cell structure had advantages of "autonomy of operational and tactical command and control, the capacity to adapt to environments, logistical autonomy, and protection by way of judicial guarantees" (p. 35). However, lack of professionalism and reliance on open social networks for recruitment, financing, and arms and explosives made the Madrid operation potentially vulnerable to detection and disruption. Ami Pedahzur and Arie Perliger (2006) diagrammed four Palestinian networks behind 42 suicide bombings during the al-Aqsa Intifada and Jewish terrorist networks inside Israel that targeted Palestinians and assassinated Prime Minister Yitzak Rabin (Pedahzur & Perliger, 2009). Other researchers applied network analytic methods to the Turkish Ergenekon terrorist organization (Demiroz & Kapucu, 2012), the Bakri-Hamza network at London's Finsbury Park mosque (Horne & Horgan, 2012), a global network of 381 persons affiliated with Islamist organizations (Medina, 2014), and a Melbourne jihadi cell disrupted before it could launch an attack (Harris-Hogan, 2013). Common features of these analyses were formal network measures that identify central, inner circle, and peripheral actors and plot their positions and connections in diagrams.

A related strand of terrorist research asserted an emerging nexus between organized criminals and terrorist groups. Terrorists not only engage in criminal activities to fund operations, but many transact with organized criminals to buy and sell goods and services, such as weapons and forged documents. Tamara Makarenko (2005) saw the origins of the nexus in 1980s Latin American *narco-terrorism*, exemplified in drug trafficking by the Revolutionary Armed Forces of Colombia (FARC). The terrorism-crime nexus went global in the 1990s with the ascendancy of transnational organized crime. Some analysts saw increasing integration (Curtis & Karacan, 2002), but others doubted whether genuine convergence is feasible (Dishman, 2001; Dandurand & Chin, 2004). This unresolved debate offers opportunities for future research.

Theorists speculated that counterterror pressures by law enforcement and military forces compel terrorist groups to change their structures and actions. In seeking an optimal balance between resilient security and communication inefficiencies, hierarchical organizations become more decentralized. Brian Jackson (2006) proposed an evolutionary process from tightly coupled organization, to coupled network, and thence to loosely coupled movement. Loose-coupling hinders the ability of counterterror organizations to detect tactical cells and "what actions should be taken to identify and exploit any vulnerabilities found there" (p. 242). Al-Qaida exemplified this trajectory from a corporate-like command structure before 9/11 to a subsequent "leaderless jihad" (Sageman, 2008). But, as decentralized cells acquire more independence to manage their logistics and select their own targets, top leaders lose control and efficiency. The shift to weakly connected network structures risks imperiling the organization's core mission, when incompetent rogue cells launch unsuccessful and counterproductive attacks.

CUTTING-EDGE RESEARCH

Mathematicians, game theorists, and computer scientists are dramatically expanding research beyond foundational case studies of terrorist networks. Much of their work centers on devising strategies for counterterror organizations to destabilize clandestine organizations. They develop elegant and precise mathematical models and computer algorithms, then systematically change parameters to assess capabilities of detecting and disrupting terrorist activities under varying conditions. Some models are not based on empirical data, but are theory-driven efforts that simulate network dynamics with artificial datasets. Other models harvest vast quantities of information from open sources, such as news reports and Websites, then mine these texts for data patterns that identify key network actors, relations, and properties. This section discusses a few exemplary cutting-edge models of both kinds.

An early effort applied the mathematical theory of ordered sets to quantify the extent to which a terrorist group ceases to function when some members are captured or killed (Farley, 2003). Assuming a hierarchical cell structure of leaders and followers, the model enables counterterror agencies to estimate the probability of disconnecting a network by removing a specified number of members. The method involves searching for the network's cutset, the network actors whose removal breaks all vertical chains of command linking leaders to foot soldiers. Of course, the mathematical model is moot for real terrorist groups that are not structured as hierarchical communication networks. (For related work, see Farley, 2007, 2009 and McGough, 2009.)

Another approach applied graph theoretic metrics to recognize and understand network structural properties. Lindelauf, Borm, and Hamers (2009a) compared models of covert communication networks to find structures with optimal trade-offs between two group objectives: secrecy to avoid detection and operational efficiency of information flow to coordinate and control cell members. Which model is optimal depends on assumptions about the likely exposure of all cell members if one person is randomly detected. For example, a star graph (all cell members communicate only with the leader) is the optimal structure for balancing the conflicting objectives if the detection of one member also exposes all his links to the other cell members. In contrast, if the probability of exposure varies by member centrality in the network, the optimal structures are reinforced rings and reinforced wheel graphs. Other scenarios making different exposure assumptions and imbalanced secrecy-efficiency trade-offs identify different optimal structures. (For related models, see Lindelauf, Borm, & Hamers, 2009b, 2010.) Notably absent from these graph theoretic models are counterterror organizations that actively try to detect and disrupt the terror networks.

Computational methods allow computer simulations of terrorist networks and the impacts of alternative counterterror strategies on their resiliency and capacity to conduct future attacks. Agent-based modeling methods involve "(i) the simulation of automated agent behaviors and interactions in the context of their environments; (ii) the analysis of macro-level patterns resulting from micro-level agent interactions" (Keller, Desouza, & Lin, 2010, p. 1020). By running thousands of simulations under varying parameter assumptions, researchers can provide some understanding and insight into potentially effective counterterror strategies against terrorist networks adapting to their opponents' actions. An example is the Stochastic Opponent Modelling Agent (SOMA) package of computational and network tools that used textual data automatically extracted from document sources to generate rules explaining a terrorist group's behavior (Sliva, Subrahmanian, Martinez, & Simari, 2008). Applied to 25 years of monthly data on the Pakistan-based Lashkar-e-Taiba (LeT), SOMA learned 10 rules that predicted when LeT was most likely to attack targets in the disputed Jammu and Kashmir provinces of India and Pakistan (Mannes, Shakarian, & Subrahmanian, 2011). These rules could "provide accurate probabilistic forecasts for both real and hypothetical situations," helping policymakers and counterterror organizations make strategic decisions (p. 6). Other exemplary data-mining, event-forecasting, link-prediction models, and experimental methods include Mahesh, Mahesh, and Vinayababu (2010); Arce, Croson, and Eckel, (2011); Chaurasia, Dhakar, Tiwari, and Gupta (2012); Desmarais and Cranmer (2013); and Petroff, Bond, and Bond (2013).

Kathleen Carley's (2003) Dynamic Network Analysis (DNA) package integrated traditional social network analysis of actor-to-actor links with computational multiagent modeling to connect actors, locations, events, tasks, knowledge, resources, and other elements. It treats terrorist groups as "complex dynamic networked systems that evolve over time" (Carley, 2006, p. 1). DNA is a "toolchain" of computer programs for collecting extracting data from texts, mapping networks of words in texts, and forecasting changes. "Map analysis systematically extracts and analyzes the links between words in a text in order to model the author's 'mental map' as networks of words" (Diesner & Carley, 2004, p. 2). Network analytic methods identify actors' spheres of influence, emergent leaders, and paths among critical actors. Theories of social interaction, such as homophily, can be applied to estimate the probability of a tie between two actors where no connection is observed. Analysts can run can virtual DNA experiments, simulating the removal of actors and observing the consequences. Quantitative measures assess potential immediate and near-term threats from alternative actions by counterterror organizations. Carley (2006) illustrated DNA with an automatic collection of thousands of open-source texts about Iraq and Al-Qaida. The emerging network had a "decidedly cellular structure with 5–12 persons per cell" (p. 5). Over a decade, it decreased in density and communication levels, but increased in congruence, suggesting "a movement to a more distributed and efficient organizational form, possibly with larger cells" (p. 4). One counterterror implication was that removing highly central actors in communication network would be less effective than taking out key emergent leaders. DNA software was provided to the Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) project, which sought to develop automated tools to "connect the dots" in raw multimedia data by modeling and simulating terrorist networks and attacks (Weinstein, Campbell, Delaney, & O'Leary, 2009, p. 1). A serious limitation was the difficulty in obtaining "truth-marked data" (p. 13) to test the SNAIR algorithms.

KEY ISSUES FOR FUTURE RESEARCH

Constantly mutating transnational terror networks will shape emerging trends in the social network analysis of terrorism and counterterrorism. Although predicting the actions of terrorist groups is notoriously imprecise, some broad tendencies are discernible. Under pressures by counterterror organizations, global jihadism evolved during the past two decades from centralized hierarchies to networked groups, then to fragmented or isolated cells. Disconnected units are more difficult to detect and disrupt, especially lone-wolf attacks (Borum, Fein, & Vossekuil, 2012), such as the November 9, 2009, Fort Hood shooting and the April 15, 2013, Boston Marathon bombing. Unstable and failed states increasingly offer sanctuaries for terrorists to assemble, train, plan, and launch operations, such as the September 21, 2013, attack by Al-Shabaab gunmen from Somalia on Westgate Mall in Nairobi, Kenya. Insurgencies and guerilla wars, flaring across Libya, Mali, Yemen, Sudan, the Sinai, Syria, and other parts of the Middle East and North Africa, offer training grounds for terrorist organizations and their foot soldiers to acquire arms, weapon skills, and combat experience. With the impending 2014 withdrawal of U.S. and NATO forces from Afghanistan, the Taliban, Al-Qaida, and "a dozen like-minded groups … are slowly and steadily returning to Afghanistan, re-creating the pre-9/11 sanctuary" (Gunaratna, 2013, p. 2). Although the U.S. and its allies decimated the original Al-Qaida top leadership, in the past five years, proliferating affiliate groups "have unquestionably expanded their operational reach and capability … We can be certain, however, that they will have much more extensive resources and capabilities than any group that has yet tried to attack us, if and when they do" (Kagan, 2013, pp. 5–6). Transnational terror will likely plague the planet into the foreseeable future.

Trends in transnational counterterrorism will likely continue the brutal, lethal, and sometimes illegal government strategies and tactics that emerged after 9/11 (Kurtulus, 2011). The Bush Administration's prosecution of "the global war against terror" violated the Geneva Conventions on torture and human rights, greatly expanded the national security state, and harmed domestic civil liberties (Chadwick, 2003; Liese, 2009). The Obama Administration curbed some egregious abuses of power, for example, closing the CIA's secret "black site" prisons and banning coercive interrogation methods. But, it extended other Bush counterterror policies and practices, such as asserting the state secrets privilege and federal immunity from lawsuits on behalf of tortured victims of U.S. renditions (Cole, 2010). Targeted killings of suspected terrorists by drone strikes in Afghanistan, Pakistan, and Yemen increased fivefold, with high numbers of civilian casualties, euphemistically called *collateral damage*. Obama greatly expanded the National Security Agency's phone and Internet surveillance programs (Greenwald, 2013). By creating a chain of contacts from massive metadata mining, NSA seeks "to identify hubs or common contacts between targets of interest who were previously thought to be unconnected, and potentially to discover individuals willing to become US Government assets" (Lizza, 2013, p. 57). After former NSA contractor Edward Snowden revealed the vast scope of data-dredging, one federal judge ruled the program an unconstitutional violation of privacy: "No court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion" (Nakashima & Marimow, 2013). But, another judge ruled it legal. Whatever the ultimate outcome of judicial appeals, presidential reviews, and congressional restrictions, cyber snooping will undoubtedly remain a counterterror priority for detecting dubious data.

Scholars in the interdisciplinary field of terrorism studies too often trail behind event-driven trends in transnational terrorism. To get ahead of the curve, researchers must look beyond investigating contemporary incidents to understanding broader contexts and longer-range perspectives. Some key issues and opportunities for future network research include:

Conduct rigorous comparative analyses of four historical waves of modern terrorism for clues about the present and future waves. An anarchist wave, beginning in late-19th century, was followed by anti-colonialist, New Left, and the contemporary jihadist wave (Rapoport, 2001). Comparing each wave's long-term network dynamics will yield important contrasts and insights into their similar and unique trajectories. One result will be better understanding of the origins of terror campaigns, responses of counterterror organizations, innovation and evolution of strategies and tactics, and processes of desistance that bring terrorism to an end.

Build more comprehensive, cohesive, and integrated theoretical models capable of explaining the formation, structure, and consequences of terrorist networks. Analytic models of network dynamics must explicate the interpersonal processes by which people are recruited to clandestine organizations, trained in nefarious skills, allocated to organizational positions, and assigned roles in terror operations. Elements for building social network theories of terrorism will be drawn from diverse social science disciplines, encompassing psychological, sociology, geographic, political, economic, and related paradigms. Connecting these elements necessitates close collaborations among substantive experts. Generating testable hypotheses will benefit from the participation of researchers from the computational sciences. Barriers to effective interdisciplinary research must be overcome, particularly the lack of understanding of alternative professional perspectives and incompatible taken-for-grant assumptions.

Develop new methods of measuring network relations among terrorists. In addition to improving the accuracy of automated text analysis techniques, how will more reliable information be extracted from photographic, video, and audio recordings? Will security software, such as biometric authentication and face-recognition software, be adapted to generate new network data? How will these diverse modes of data collection be effectively integrated using network analytic methods?

Perform more laboratory experiments as an alternative to collecting inaccessible and dangerous field observation data. Researchers will construct theoretically based models of interdependent terrorist and counterterror networks comprising both computer programs and human subjects. Controlled manipulation of parameters, such as information and costs, will test hypotheses predicting actor reactions and network structural changes. Investigators will study the impacts of varying scenarios on subjects' actions and collective outcomes such as detection, deterrence, disruption, network resilience, security decision, resource allocation, target selection, and attack success. For greater complexity and realism, experimental findings will be adapted to massively multiuser online role-playing games pitting virtual terrorists against counterterror agents.

Create large, high-quality relational datasets to test social network theories of terrorism. Researchers will shift from case studies of particular events to encompassing systems of people, organizations, institutions, and events. Counterterror actions will be integrated with terrorist behaviors to create more realistic coevolving network dynamics. Given the paucity of primary data collected from terrorists, many researchers will continue to depend on collecting secondary data from public documents. Other analysts will emphasize the importance of the Internet and cyberspace communication networks linking thousands of extremist Websites for propaganda, radicalization, recruitment, and financial transactions. Vastly more sophisticated massive data-mining algorithms will improve content-based pattern detection. But, quality assurance will necessitate such automated routines be supplemented by painstaking hands-on correction of gaps and errors.

Regardless of specific future directions, social network researchers must surely rise to the challenge of how to use network analytic theory and methods for better understanding, detecting, and thwarting of miscreants engaged in terrorist activities.

REFERENCES

Arce, D. G., Croson, R. T. A., & Eckel, C. C. (2011). Terrorism experiments. *Journal of Peace Research*, *48*, 373–382. doi:10.1177/0022343310391502

Borum, R., Fein, R., & Vossekuil, B. (2012). A dimensional approach to analyzing lone offender terrorism. *Aggression and Violent Behavior*, *17*, 389–396. doi:10.1016/j.avb.2012.04.003

Carley, K. M. (2003). Dynamic network analysis. In R. Breiger, K. Carley & P. Pattison (Eds.), *Dynamic social network modeling and analysis: Workshop summary and papers* (pp. 133–145). Washington, DC: Committee on Human Factors, National Research Council.

Carley, K. M. (2006). A dynamic network approach to the assessment of terrorist groups and the impact of alternative courses of action. In *Visualising Network Information*. Meeting Proceedings RTO-MP-IST-063, Keynote 1 pp. KN1-1–KN1-10. Neuilly-sur-Seine, France: RTO. Retrieved from http://www.vistg.net/documents/IST063_PreProceedings.pdf.

Chadwick, E. (2003). It's war, Jim, but not as we know it: A 'reality-check' for international laws of war? *Crime, Law and Social Change*, *39*, 233–262. doi:10.1023/A:1022907030010

Chaurasia, N., Dhakar, M., Tiwari, A., & Gupta, R. K. (2012). A survey on terrorist network mining: Current trends and opportunities. *International Journal of Computer Science & Engineering Survey*, *3*(4) Retrieved from http://www.airccse.org/journal/ijcses/papers/3412ijcses05.pdf. doi:10.5121/ipcses.2012.3405

Cole, D. (2010). Breaking away. *New Republic* December 30. Retrieved from http://www.newrepublic.com/article/magazine/politics/79752/breaking-away-obama-bush-aclu-guantanamo-war-on-terror.

Curtis, G., & Karacan, T. (2002). *The Nexus among terrorists, narcotics traffickers, weapons proliferators, and organized crime networks in Western Europe*. Washington, DC: Federal Research Division, Library of Congress. Retrieved from http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.

Dandurand, Y., & Chin, V. (2004). *Links between terrorism and other forms of crime*. Vancouver, BC: International Centre for Criminal Law Reform and Criminal Justice Policy. Retrieved from http://icclr.law.ubc.ca/sites/icclr.law.ubc.ca/files/publications/pdfs/LinksBetweenTerrorismLatest_updated.pdf.

Demiroz, F., & Kapucu, N. (2012). Anatomy of a dark network: the case of the Turkish Ergenekon terrorist organization. *Trends in Organized Crime*, *15*, 271–295. doi:10.1007/s12117-012-9151-7

Desmarais, B. A., & Cranmer, S. J. (2013). Forecasting the locational dynamics of transnational terrorism: A network analytic approach. *Security Informatics*, *2*, 1–13. Retrieved from http://www.security-informatics.com/content/pdf/2190-8532-2-8.pdf. doi:10.1186/2190-8532-2-8

Diesner, J., & Carley, K. M. (2004). *Using network text analysis to detect the organizational structure of covert networks* (Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.5240&rep=rep1&type=pdf).

Dishman, C. (2001). Terrorism, crime, and transformation. *Studies in Conflict & Terrorism*, *24*, 43–58. doi:10.1080/10576100118878

Farley, J. D. (2003). Breaking Al Qaeda cells: A mathematical analysis of counterterrorism operations (A guide for risk assessment and decision making). *Studies in Conflict & Terrorism*, *26*, 399–411. doi:10.1080/10576100390242857

Farley, J. D. (2007). *Toward a mathematical theory of counterterrorism: Building the perfect terrorist cell*. Proteus Monograph Series Volume 1 Issue 2. Retrieved from http://www.rit.edu/~w-cmmc/literature/Proteus.pdf.

Farley, J. D. (2009). Two theoretical research questions concerning the structure of the perfect terrorist cell. In N. Memon, J. D. Farley, D. L. Hicks & T. Rosenorn (Eds.), *Mathematical Methods in Counterterrorism* (pp. 91–103). New York, NY: Springer-Verlag/Wien.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian* June 5. Retrieved from www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gunaratna, R. (2013). Terrorists to bounce back in 2013. *Counter Terrorist Trends and Analysis*, *5*, 2–4.

Harris-Hogan, S. (2013). Australian neo-jihadist terrorism: Mapping the network and cell analysis using wiretap evidence. *Studies in Conflict & Terrorism*, *35*, 298–314. doi:10.1080/1057610X.2012.656344

Horne, C., & Horgan, J. (2012). Methodological triangulation in the analysis of terrorist networks. *Studies in Conflict & Terrorism*, *35*, 182–192. doi:10.1080/1057610X.2012.639064

Jackson, B. A. (2006). Groups, networks, or movements: A command-and-control-driven approach to classifying terrorist organizations and its application to Al Qaeda. *Studies in Conflict & Terrorism*, *29*, 241–262. doi:10.1080/10576100600564042

Jordán, J., Mañas, F. M., & Horsburgh, N. (2008). Strengths and weaknesses of grassroot jihadist networks: The Madrid bombings. *Studies in Conflict & Terrorism*, *31*, 17–39. doi:10.1080/10576100701767148

Kagan, F. W. (2013). The continued expansion of al Qaeda affiliates and their capabilities. Washington: Testimony before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade. Retrieved from http://www.aei.org/speech/foreign-and-defense-policy/terrorism/al-qaeda/the-continued-expansion-of-al-qaeda-affiliates-and-their-capabilities.

Keller, J., Desouza, K. C., & Lin, Y. (2010). Dismantling terrorist networks: Evaluating strategic options using agent-based modeling. *Technological Forecasting & Social Change*, *77*, 1014–1036. doi:10.1016/j.techfore.2010.02.007

Koschade, S. (2006). A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism*, *29*, 559–575. doi:10.1080/10576100600798418

Koschade, S. (2007). *The internal dynamics of terrorist cells: A social network analysis of terrorist cells in an Australian context*. Unpublished doctoral dissertation, Queensland University of Technology, Brisbane, Australia. Retrieved from http://eprints.qut.edu.au/16591.

Krebs, V. (2001). Mapping networks of terrorist cells. *Connections*, *24*, 43–52. Retrieved from http://vlado.fmf.uni-lj.si/pub/networks/doc/Seminar/Krebs.pdf.

Krebs, V. (2002). Uncloaking terrorist networks. *First Monday*, *7*, 1–14. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/941.

Kurtulus, E. N. (2011). The new counterterrorism: Contemporary counterterrorism trends in the United States and Israel. *Studies in Conflict & Terrorism*, *35*, 37–58. doi:10.1080/1057610X.2012.631456

Liese, A. (2009). Exceptional necessity: How liberal democracies contest the prohibition of torture and ill-treatment when countering terrorism. *Journal of International Law and International Relations*, *5*, 17–47.

Lindelauf, R., Borm, P., & Hamers, H. (2009a). The influence of secrecy on the communication structure of covert networks. *Social Networks*, *31*, 126–137. doi:10.1016/j.socnet.2008.12.003

Lindelauf, R., Borm, P., & Hamers, H. (2009b). On heterogeneous covert networks. In N. Memon, J. D. Farley, D. L. Hicks & T. Rosenorn (Eds.), *Mathematical methods in counterterrorism* (pp. 215–228). New York, NY: Springer-Verlag/Wien.

Lindelauf, R., Borm, P., & Hamers, H. (2010). One-mode projection analysis and design of covert affiliation networks. Tilburg, Netherlands: Tilburg University Center for Economic Research, Discussion Paper 2010–53. Retrieved from https://pure.uvt.nl/portal/files/1225410/2010-53.pdf.

Lizza, R. (2013). State of deception: Why won't the president rein in the intelligence community? *New Yorker,* December, *16*, 48–61.

Magouirk, J., Atran, S., & Sageman, M. (2008). Connecting terrorist networks. *Studies in Conflict & Terrorism*, *31*, 1–16. doi:10.1080/10576100701759988

Mahesh, S., Mahesh, T. R., & Vinayababu, M. (2010). Using data mining techniques for detecting terror-related activities on the Web. *Journal of Theoretical & Applied Information Technology*, *16*, 99–104.

Makarenko, T. (2005). Terrorism and transnational organized crime: Tracing the crime-terror nexus in South East Asia. In P. Smith (Ed.), *Terrorism and violence in South East Asia: Transnational challenges to states and regional stability* (pp. 169–187). New York, NY: M. E. Sharpe.

Mannes, A., Shakarian, J., & Subrahmanian, V. S. (2011). A computationally-enabled analysis of Lashkar-e-Taiba attacks in Jammu and Kashmir. In *Intelligence and Security Informatics Conference (EISIC), 2011 European* (pp. 224–229. Retrieved from http://shakarian.net/janaPapers/let_eisic_camera.pdf. doi:10.1109/EISIC.2011.61).

McGough, L. R. (2009). Mathematically modeling terrorist cells: Examining the strength of structures of small sizes. In N. Memon, J. D. Farley, D. L. Hicks & T. Rosenorn (Eds.), *Mathematical methods in counterterrorism* (pp. 55–67). New York, NY: Springer-Verlag/Wien.

Medina, R. M. (2014). Social network analysis: A case study of the Islamist terrorist network. *Security Journal*, *27*, 97–121. Retrieved from. doi:10.1057/sj.2012.21

Nakashima, E., & Marimow, A. E. (2013). Judge: NSA's collecting of phone records is probably unconstitutional. *Washington Post* December 16. Retrieved from http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html.

National Commission on Terrorist Attacks Upon the United States (2004). *The 9/11 commission report*. New York, NY: W.W. Norton. Retrieved from http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

Pedahzur, A., & Perliger, A. (2006). The changing nature of suicide attacks: A social network perspective. *Social Forces*, *84*, 1987–2008. doi:10.1353/sof.2006.0104

Pedahzur, A., & Perliger, A. (2009). *Jewish terrorism in Israel*. New York, NY: Columbia University Press.

Petroff, V. B., Bond, J. H., & Bond, D. H. (2013). Using hidden Markov models to predict terror before it hits (again). In V. S. Subrahmanian (Ed.), *Handbook of computational approaches to counterterrorism* (pp. 163–180). New York, NY: Springer-Verlag/Wien.

Rapoport, D. C. (2001). The fourth wave: September 11 in the history of world terrorism. *Current History*, *100*, 419–424.

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

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

Sliva, A., Subrahmanian, V. S., Martinez, V., & Simari, G. I. (2008). The SOMA Terror Organization Portal (STOP): Social network and analytic tools for the real-time analysis of terror groups. *First International Workshop on Social Computing, Behavioral Modeling, and Prediction*. Retrieved from http://content.schweitzer-online.de/static/content/catalog/newbooks/978/038/777/9780387776712/9780387776712_Excerpt_001.pdf.

Sterling, C. (1981). *The terror network: The secret war of international terrorism*. New York, NY: Holt, Rinehart and Winston.

U.S. Department of State (2013). *Country reports on terrorism 2012*. Retrieved from http://www.state.gov/j/ct/rls/crt/2012.

Weinstein, C., Campbell, W., Delaney, B., & O'Leary, G. (2009). Modeling and detection techniques for counter-terror social network analysis and intent recognition. *Institute of Electrical and Electronics Engineers*. Retrieved from dspace.mit.edu/openaccess-disseminate/1721.1/71803.

FURTHER READING

Everton, S. F. (2012). *Disrupting dark networks*. New York, NY: Cambridge University Press.

McCulloh, I., Armstrong, H., & Johnson, A. (2013). *Social network analysis with applications*. New York, NY: John Wiley & Sons, Inc.

Memon, N., Farley, J. D., Hicks, D. L., & Rosenorn, T. (Eds.) (2009). *Mathematical methods in counterterrorism*. New York, NY: Springer-Verlag/Wien.

Mullins, S. (Ed.) (2013). Special issue: Applying social network analysis to terrorism. *Behavioral Sciences of Terrorism & Political Aggression*, *5*(2), 67–175.

Ranstorp, M. (Ed.) (2007). *Mapping terrorism research: State of the art, gaps and future direction*. New York, NY: Routledge.

Subrahmanian, V. S. (Ed.) (2013). *Handbook of computational approaches to counterterrorism*. New York, NY: Springer-Verlag/Wien.

DAVID KNOKE SHORT BIOGRAPHY

David Knoke is professor of sociology at the University of Minnesota, where he teaches courses in statistics, networks, and organizations. He received his PhD in 1972 from the University of Michigan and was professor of sociology at Indiana University from 1972 to 1985. He was a Fulbright research scholar at Kiel University (1989) and a fellow at the Center for Advanced Study in the Behavioral Sciences (1992). In 2008, he received the University of Minnesota College of Liberal Arts' Arthur "Red" Motley Exemplary Teaching Award. With various colleagues, he received several National Science Foundation research grant and published the results in research monographs on political, organizational, and social network behavior. Some of these books are *The Organizational State, Organizing for Collective Action, Political Networks, Organizations in America, Comparing Policy Networks, Changing Organizations*, *Social Network Analysis*, and *Economic Networks*. His current research investigates diverse social networks, including intra- and interorganizational, health care, economic, financial, terrorist, and counterterror networks.

RELATED ESSAYS

Problems Attract Problems: A Network Perspective on Mental Disorders *(Psychology)*, Angélique Cramer and Denny Borsboom

Migrant Networks *(Sociology)*, Filiz Garip and Asad L. Asad

Interdependence, Development, and Interstate Conflict *(Political Science)*, Erik Gartzke

Herd Behavior *(Psychology)*, Tatsuya Kameda and Reid Hastie

Regime Type and Terrorist Attacks *(Political Science)*, Kara Kingma *et al*.

How Networks Form: Homophily, Opportunity, and Balance *(Sociology)*, Kevin Lewis

Network Research Experiments *(Methods)*, Allen L. Linton and Betsy Sinclair

Culture, Diffusion, and Networks in Social Animals *(Anthropology)*, Janet Mann and Lisa Singh

Gender and Women's Influence in Public Settings *(Political Science)*, Tali Mendelberg *et al*.

The Role of School-Related Peers and Social Networks in Human Development *(Psychology)*, Chandra Muller

Social Relationships and Health in Older Adulthood *(Psychology)*, Theodore F. Robles and Josephine A. Menkin

How Do Labor Market Networks Work? *(Sociology)*, Brian Rubineau and Roberto M. Fernandez

War and Social Movements *(Political Science)*, Sidney Tarrow

Creativity in Teams *(Psychology)*, Leigh L. Thompson and Elizabeth Ruth Wilson