

Terrorist Network Adaptation to a Changing Environment

By

Sean F. Everton, PhD; Assistant Professor, Naval Postgraduate School
Dan Cunningham, MA; Research Associate, Naval Postgraduate School

August 31, 2011

Terrorist Network Adaptation to a Changing Environment

Abstract

To date most social network (SNA) analyses of terrorist groups have tended to use network data that provide snap-shots of the groups at a single point in time. Seldom have they used network data that takes into account how the groups have changed over time. In this paper we draw on a unique longitudinal network data set of the Noordin Top terrorist network from 2001-2010 in order to explore how the network's topography (e.g., centralization, density, degree of fragmentation,) and effectiveness (e.g., recruitment, number of quality network members) changed over time in light of efforts by Indonesian authorities to disrupt it. Our analysis allows us to draw tentative conclusions with regard to various theories about how terrorist networks adapt to a hostile environment and how such adaptations influence their effectiveness. For example, available evidence suggests that in a hostile environment, successful terrorist groups become increasingly dense and tend to adopt a more decentralized form of organization that not only provides greater security but also improves effectiveness. Adaptation can create new vulnerabilities, however. Terrorist groups that become too dense or fail to decentralize can become vulnerable to rapid deterioration in the event of a well-connected member's capture. This appears to have happened with the Noordin Top network. Instead of decentralizing in the face of external pressure, it became more centralized, and when Indonesian authorities killed Noordin Top (and a few of his key associates), the network rapidly deteriorated. We conclude our analysis with what this analysis suggests for the crafting of strategies for the disruption of dark networks.

Terrorist Network Adaptation to a Changing Environment

Introduction

Dark networks, that is, covert and illegal networks (Raab and Milward 2003), evolve over time. They undergo changes caused by both endogenous and exogenous factors, such as the attempt by network leaders to recruit talented members to plan and carry out attacks or their reaction to operations by hostile authorities. Much of the same evolutionary processes that “bright” or “light” networks undergo are seen in dark networks. Changes in network structure can be gradual and/or rapid, and they affect the way in which the network behaves and its ability to launch successful attacks. Indeed, the study and use of the term “terrorist networks” has grown dramatically in recent years as has the application of social network analysis (SNA) to explore and understand the phenomenon. However, most social network analyses of terrorist groups have tended to use data that merely provide snap-shots of them at single points in time. Seldom have such studies drawn on longitudinal network data that capture how groups have changed and adapted over time, making it impossible to explore how important changes in network structure affect a host of related issues, such as network resiliency, network structure and performance, and measuring the effectiveness of counter-terrorism strategies.

Nevertheless, a few scholars, building on the insights of research on bright networks, have begun applying longitudinal modeling techniques to dark network data. These studies have examined the issues mentioned above, but most have not fully accounted for the interaction between them. This paper’s purpose is to contribute to this growing body of research by fusing the related issues of network adaptability, the relationship between network structure and performance, and strategies for targeting dark networks. We draw on social network analysis to examine a unique longitudinal data set, namely, the Noordin Top terrorist network, combining descriptive analysis and multivariate regression statistical models. Our analyses allow us to draw tentative conclusions with regard to various theories about how terrorist networks adapt to a hostile environment and how such adaptations influence their effectiveness. For example, recent research suggests that, all else being equal, in a hostile environment, successful terrorist groups tend to become increasingly dense and adopt a more decentralized form of organization. Such adaptation not only provides greater security but also improves effectiveness. Adaptation can create new vulnerabilities, however. Terrorist groups that become too dense or fail to decentralize can become vulnerable to a well-connected member’s capture or elimination.

This paper begins with an overview regarding the analysis of longitudinal dark network data. The next section examines the topographical metrics we use to explore Noordin Top’s network structure over time. Our analysis does not draw on all metrics of network topography, but it does focus on three commonly used sets of metrics. This section is followed by a brief discussion of the network data used in this paper. In particular, we focus on what we call Noordin’s trust and operational networks, although future analyses may want to consider others (e.g., communication and financial networks). Next, we conduct an exploratory analysis that examines how our topographical metrics of interest vary across time. Then, we expand this analysis by regressing these topographical measures on a handful of variables that we believe lead dark networks to adapt and change. Finally, we conclude with a reflection on our results as well as offer suggestions for future research.

Terrorist Network Adaptation to a Changing Environment

The Longitudinal Analysis of Dark Networks

Historically, longitudinal network data have been difficult to come by, and the methods for examining them underdeveloped. As a case in point, Wasserman and Faust's classic text on social network analysis makes little mention of longitudinal networks. Only in the final chapter do the authors note the importance of developing good and easy-to-use methods for examining longitudinal network data (Wasserman and Faust 1994:730-731). In recent years, this situation has begun to change. Longitudinal network data and their analysis are becoming more common. Many analyses have been largely descriptive in nature, but they are increasingly becoming more sophisticated, employing model-based approaches that seek to identify the underlying mechanisms of network change (Breiger, Carley and Pattison 2003; de Nooy 2011; Doreian and Stockman 1997; McCulloh and Carley 2011; Snijders 2005; Snijders, Bunt and Steglich 2010; Steglich, Snijders and Pearson 2010). In this regard, scholars have overwhelmingly used some variation of the Markov property for modeling longitudinal networks and have largely accounted for tendencies of link formation, including reciprocity (Leenders 1996; Wasserman 1980), homophily (Kossinets and Watts 2009; Leenders 1996), and transitivity (Kossinets and Watts 2006; 2009). Using these methods analysts have analyzed a variety of types of networks (Doreian and Stockman 1997), such as friendship (Leenders 1996), and communication ties (Kossinets and Watts 2006). Snijders and his colleagues (Snijders 2001; 2005; Snijders, Bunt and Steglich 2010; Steglich, Snijders and Pearson 2010; Van de Bunt, Van Duijn and Snijders 1999) have taken a different approach to these process models by developing a set of stochastic actor-based models in which actors drive change in network structures, which is also the approach implemented in the popular software program *SIENA*. Recent analysts have applied both continuous (Kossinets and Watts 2006; 2009; Leenders 1996; Snijders 2001) and discrete (Banks and Carley 1996; Robins and Pattison 2001) recovery techniques in order to account for longitudinal network variation. None of this is meant to suggest that descriptive analyses of longitudinal network data are invaluable. Indeed, we employ them in this paper to initially explore our data. Rather, it is merely to point out that the development of these new models allows analysts to supplement descriptive approaches with more sophisticated approaches. Whether all of these new modeling techniques meet Wasserman and Faust's "easy-to-use" criterion, however, is a matter of debate.

To date the majority of longitudinal analyses have focused on the application of models to "bright" or "light" networks. Only a handful of scholars have applied them to the longitudinal study of dark networks. Most notably, Carley and her colleagues (Carley 2003 see e.g., ; Carley 2001-2011; Carley, Lee and Krackhardt 2002) have contributed significantly to the field through modeling dynamic dark networks and the development of the meta-matrix approach. Xu, Hu and Chen's (2009) interesting analysis of the Global Salafi Jihad (GSJ) network and its survival suggests that the network experienced three distinct phases over time, including an emerging, maturing and disintegrating phase. They also found that the GSJ network gradually displayed a scale-free topology over time. Building on Kossinets and Watts (2006), Hu, Kaza and Chen (2009) applied a Cox survival analysis on a co-offending network for identifying facilitators of cyclic and focal closure. They found that acquaintances and shared vehicle affiliations serve as key link facilitators, while homophily in age, race and gender were not significant predictors of either type of closure. McCulloh and Carley (2011) recently took a unique approach by applying social network change detection (SNCD) techniques to a number of longitudinal networks,

Terrorist Network Adaptation to a Changing Environment

including the al Qaeda communication network from 1988 to 2004. SNCD allows real-time analysis and alerts analysts whether and when a statistically significant change occurs in the network so that they can focus on specific times and examine the potential causes for the change.

An additional set of scholars have examined the factors contributing to network resiliency (Bakker, Raab and Milward 2008), which is essentially a dynamic perspective to the study of dark networks since they must continuously withstand and adapt to various levels of external pressure in order to survive. Some influential studies have accounted for the relationship between resilience and scale-free networks (Barabási and Bonabeau 2003; Sageman 2004a; Xu, Hu and Chen 2009), and network survival and decentralized network structures (Arquilla and Ronfeldt 2001; Bakker, Raab and Milward 2011; Milward and Raab 2006; Raab and Milward 2003). Tsvetovat and Carley's (2005) simulated attacks on a cellular terrorist network suggests that covert networks rebound from shocks primarily through activating latent resources. Milward and Raab's (2006) insightful work argues that dark networks are resilient to the extent that they can balance differentiation and integration (i.e., the capacity to act and persist) in the face of mounting pressure. Furthermore, a dark network's ability to operate and respond to shocks is largely contingent upon the group's motivations and resources, such as money, access to technology, and territory. Building upon this research, Bakker, Raab and Milward (2011) examine how the operational activity of a series of dark networks reacted and adapted to external shocks and, in so doing, identify additional factors that contribute to the resiliency of dark networks. For instance, they note that to be successful dark networks must maintain and replace nodes and ties at a rate faster than they are destroyed. They also argue that legitimacy (both internal and external) is a crucial factor for network survival, particularly for grievance-based dark networks. Finally, they identify a number of network characteristics, such as the degree to which a network is decentralized, that they believe contribute to dark network resiliency.

Some scholars have gone beyond examining the factors contributing to network survival and explored the relationship between structural characteristics of dark networks and their ability to effectively launch attacks. For example, Rodriguez's (2005) examination of the Madrid terrorist network concluded that "weak" ties (Granovetter 1973; 1983) were crucial not only to its security and adaptability but also to its operational success. Most studies also appear to conclude (or assume) that dark networks must balance operational capacity with network security but do so in the environmental contexts in which they operate, some of which are more hostile than others (Bakker, Raab and Milward 2011; Bienenstock and Bonacich 2003; Enders and Su 2007; Kenney 2007; Lindelauf, Borm and Hamers 2009; Milward and Raab 2006). However, it is often difficult for dark networks to reach or maintain an optimal balance. For instance, while some research suggests that network density is positively related to a network's command and control capability, it may also render the network more vulnerable to rapid deterioration in the event of a well-connected member's capture (Granovetter 1973; 1983; Koschade 2006; U.S. Army 2007). On the other hand, Helfstein and Wright's (2011) recent analysis of six successful attack networks found that neither operational security type (OPSEC) nor scale-free structures are associated with network success (as measured by casualties). They also concluded that network characteristics such as density had no causal relationship with success (i.e., casualties) although they did find that the networks became increasingly dense and cohesive over time, particularly as they entered an operation's execution phase.

Multiple authors have also suggested strategies for disrupting and destabilizing dark networks. Marc Sageman (2004a; b), for instance, discovered that the global salafi jihad (GSJ) shares the characteristics

Terrorist Network Adaptation to a Changing Environment

of scale-free networks, which have been found to be relatively immune to random failures but vulnerable to targeted attacks on well-connected actors known as hubs (Barabási 2002; Barabási and Albert 1999; Barabási, Albert and Jeong 1999; Barabási and Bonabeau 2003). Building upon this analysis Xu, Hu and Chen (2009) used Sageman's data to compare simulated and actual node removal strategies from 1993 to 2003. They found that actual counter-attacks launched against the GSJ were largely ineffective in disrupting the network, while simulated attacks targeting hubs were relatively successful. Other scholars have also contributed significantly to the study of destabilizing dark networks through simulated counter-attacks (Carley 2006; Carley, Lee and Krackhardt 2002; Tsvetovat and Carley 2005), proposing alternative actor-centric strategies, including targeting actors with critical skills (Klerks 2001), and by developing new and useful algorithms for identifying key actors for the purposes of diffusing something (i.e. information) or fragmenting a network (Borgatti 2006). More recently, Roberts and Everton (2011) have considered a variety of kinetic and non-kinetic strategies and proposed that counter-terrorism strategies should be context driven rather than using SNA metrics to drive particular strategies. The available literature using SNA for targeting dark networks, however, has yet to account for changes in strategies across time and what those changes mean for a dark network's structure and consequently its ability to operate. Similar to static analyses of dark networks, longitudinal studies, including those focusing on network resilience and the relationship between structure and attacks, will often suggest ways to disrupt the networks. Nevertheless, it appears that the available social network literature does not fully account for the interaction between dark network evolution, structure and performance, and strategies for disrupting them across time.

Network Topography

In this paper we combine descriptive and multivariate regression analysis in order to tease out how a particular dark network, the Noordin Top terrorist network, adapted and changed from 2001 to 2010 in reaction to endogenous and exogenous factors. Before turning to this analysis, however, we need to first examine the various topographical measures we will use to track these changes. While there are a number of topographical measures available for use, in this paper we will focus on three of the more common ones: density, centralization, and fragmentation. Density measures capture a network's inner connectedness. As we will see the traditional measure of density is unhelpful when analyzing networks that vary in size; consequently, we use an alternative measure, average degree, which is not sensitive to network size. Centralization metrics estimate the degree to which a network revolves around different centers of power. As those familiar with social network analysis know, however, there are a variety of centrality metrics. In this paper, we focus on two—degree and betweenness centrality—although subsequent analysis may want to consider analyzing dark networks with other or additional measures. Finally, fragmentation algorithms, which are somewhat similar to density algorithms, calculate the proportion of network members who are unconnected (either directly or indirectly) to one another. The traditional measure is simply the proportion. An alternative measure weights this proportion by how close (in terms of path distance) each actor is, on average, to all other actors in the network. We utilize both of these in this analysis. It is to a discussion of these metrics that we now turn.

Terrorist Network Adaptation to a Changing Environment

Density and Average Degree

In what is now considered a classic study Mark Granovetter (1973; 1974) discovered that when it came to finding jobs, people were far more likely to use personal contacts than they were other means such as formal means¹ or directly applying for their job.² Moreover, of those who found their jobs through personal contacts, most were weak (i.e., acquaintances) rather than strong ties (i.e., close friends). Granovetter concluded that this was because not only do we tend to have more weak ties than strong ties (because weak ties demand less of our time), but also because our weak ties are more likely to form the bridges that tie densely knit clusters of people together. In fact, if it were not for these weak ties, Granovetter argues, these clusters would not be connected at all. Thus, whatever is to be diffused (e.g., information, influence, and other types of resources), it will reach a greater number of people when it passes through weak ties rather than strong ones. Because of this, actors with few weak ties are more likely to “confined to the provincial news and views of their close friends” (Granovetter 1983:202).

Granovetter did not argue that strong ties are of no value, however. He noted that while weak ties provide individuals with access to information and resources beyond those available in their immediate social circles, strong ties are more likely to be sources of support in times of uncertainty. Others have noted this as well (see e.g., Krackhardt 1992). “There is a mountain of research showing that people with strong ties are happier and even healthier because in such networks members provide one another with strong emotional and material support in times of grief or trouble and someone with whom to share life’s joys and triumphs” (Stark 2007:37).

An implicit suggestion of all this is that people’s networks differ in terms of their mix of weak and strong ties. They range from local (i.e., provincial) ones, consisting of primarily of strong, redundant ties, to worldly (i.e., cosmopolitan) ones, consisting of numerous weak ties and few strong ties (Stark 2007:37-38). It also suggests that peoples’ networks should ideally consist of a mix of weak and strong ties. Their networks should be neither too provincial nor too cosmopolitan but rather should land somewhere between the two extremes, not necessarily at the arithmetic mean, but rather at a “golden mean” of sorts (Aristotle 1998:36-43).

Pescosolido and Georgianna’s (1989) study of suicide illustrates this dynamic. They found that the density of actors’ social networks has a curvilinear (or inverted U) relationship to suicide. Individuals whose social networks are very sparse (i.e., cosmopolitan) or very dense (i.e., provincial) are far more likely to commit suicide than are those whose networks lie between the two extremes. Why? People located in sparse social networks often lack the social and emotional ties that provide them the support they need during times of crisis. They also typically lack ties to others who might otherwise prevent them from engaging in self-destructive (i.e., deviant) behavior (Finke and Stark 2005; Granovetter 2005). On the other hand, individuals embedded in dense networks are often cut-off from people outside of their immediate social group, which increases the probability that they will lack the ties to others who could prevent them from taking the final, fatal step.

¹ Formal means is where the job seekers used the services of impersonal intermediaries such as advertisements, public and private employment agencies, interviews and placements sponsored by universities or professional associations.

² Direct application is where the job seekers went or wrote directly to a firm, did not use a formal or personal intermediary, and had not heard about a specific opening from a personal contact.

Terrorist Network Adaptation to a Changing Environment

An ideal mix of weak and strong ties appears to not only provide benefits at the individual level but also at the organizational level. In his study of the New York apparel industry, Brian Uzzi (1996) found that a mix of weak and strong ties proved beneficial to the long-term survival of apparel firms.³ The firms he studied tended to divide their market interactions into two types: “market” or “arms-length” relationships (i.e., weak ties) and “special” or “close” relationships (i.e., strong ties), which Uzzi refers to as “embedded” ties. He found that while market relationships were more common than embedded ties, they tended to be less important. Embedded ties were especially important in situations where fine-grained information had to be passed to the other party, and when certain types of joint problem-solving were on the agenda (Uzzi 1996:677). According to Uzzi, embeddedness increases economic effectiveness along a number of dimensions crucial to competitiveness in the global economy: organizational learning, risk sharing, and speed-to-market. He also found, however, that firms that are too embedded suffer because they lack access to information from distant parts of the social structure, rendering them vulnerable to rapidly changing situations. This led Uzzi to argue that firms should seek to maintain a balance of embedded and market ties. In support of this he found that the topography of interfirm networks (i.e., in terms of embedded and market ties) varied and that a U-shaped association exists between the degree of embeddedness and the probability of firm failure (Uzzi 1996:675-676). Firms with extremely high levels of embedded ties (i.e., provincial networks) or extremely high levels of market ties (i.e., cosmopolitan networks) were much more likely to fail than those that maintained a balance between the two.

Interestingly, Uzzi and Spiro (2005) found that an inverted U relationship also existed between extent to which the networks of creative teams that produced Broadway musicals from 1945 to 1989 exhibited “small-worldness” (measured by what they called “small world Q ”) and the probability that a musical would be a critical and financial success. They believe that this relationship existed because up to a point, connectivity and cohesion facilitate the flow of diverse and innovative material across the network. Moreover, connectivity and cohesion make risk-taking among the teams more likely because they are embedded in networks of trust. However, as connectivity and cohesion increase, homogenization and imitation set in and returns become negative. In other words, connectivity and cohesion initially increase a network’s overall creativity by encouraging human innovation, but beyond a certain point, they begin to stifle it.

While it may be difficult to conceive of criminal and terrorist networks as varying in their ability to encourage innovative thinking and creative risk-taking, what these studies suggest is that in order to be successful, dark networks can be neither too provincial nor too cosmopolitan. What constitutes a particular dark network’s optimum balance will likely vary depending on the environment in which it operates (e.g., the IRA can operate more openly in Ireland than Al-Qaeda can in the United States). However, because the survival of dark networks depends largely on them recruiting members whom they can trust (Berman 2009; Tilly 2004; 2005), they tend to recruit through strong (rather than weak) ties, and networks formed primarily by strong ties become increasingly dense as ties form between previously unlinked actors (Granovetter 1973; Holland and Leinhardt 1971; Rapoport 1953a; b; Rapoport and Horvath 1961). Thus, we should expect that dark networks will, on the whole, be denser than will light networks, recognizing that if it can become too dense and consequently limit its effectiveness.

³ Uzzi does not use the weak and strong tie terminology in the article.

Terrorist Network Adaptation to a Changing Environment

Formally, network density is defined as the total number of ties in a network divided by the total possible number of ties. Networks with no ties have a density of 0.0 (or 0%), while in networks where all possible ties between actors exist have a density of 1.0 (or 100%). This formal measure of density, however, is inversely related to network size (i.e., the larger the network, the lower the density) because the number of possible lines increases exponentially as actors are added to the network, while the number of ties that each actor can maintain tends to be limited. Thus, social network analysts often turn to average degree, which is simply the average number of ties that each actor in the network has, in order to measure how “dense” a network is (de Nooy, Mrvar and Batagelj 2005; Scott 2000).

Degree and Betweenness Centralization

Another well-developed body of research has explored how the extent to which an organization is hierarchically structured impacts its performance (see e.g., Nohria and Eccles 1992; Podolny and Page 1998; Powell 1985; 1990; Powell and Smith-Doerr 1994). This literature typically identifies two ideal types of organizational form: networks and hierarchies. The former are seen as decentralized, informal, and/or organic, while the latter are seen as centralized, formal and/or bureaucratic (see e.g., Burns and Stalker 1961; Powell 1990; Ronfeldt and Arquilla 2001). While this distinction is useful in some contexts (see, e.g. Arquilla and Ronfeldt 2001; Castells 1996; Podolny and Page 1998; Powell and Smith-Doerr 1994; Ronfeldt and Arquilla 2001), among social network analysts, all organizations are networks, regardless if they are hierarchical or decentralized, which is why a number of metrics have been developed to capture this dimension. Thus, it is better to think of these two ideal types as poles on either end of a continuum, running from highly decentralized networks one end to highly centralized networks on the other.

Current research suggests that, much like the provincial-cosmopolitan dimension, there is an optimal level of centralization or hierarchy appears to exist. For example, Rodney Stark (1987; 1996), in his analysis of why some new religious movements succeed, identified centralized authority as an important factor. Nevertheless, he notes that too much centralization can be a bad thing and that successful religious movements, such as the Mormon (LDS) Church, balance centralized authority structures with decentralized ones. As Stark notes, the LDS Church displays a high level of participatory democracy, perhaps best symbolized by the fact that to be a priest in the LDS church is to be “an unpaid, part-time role that all committed males are expected to fulfill” (Stark 2005:125). Like the provincial-cosmopolitan dimension, the optimal level almost certainly varies depending on environmental context (Tucker 2008). Because decentralized networks tend to be better suited for solving nonroutine, complex and/or rapidly-changing problems or challenges because of their adaptability, it is likely that successful dark networks will land more toward the decentralized end of the continuum than the hierarchical one (Arquilla and Ronfeldt 2001; Ronfeldt and Arquilla 2001). Even here, though, dark networks that are too decentralized may find it difficult to mobilize resources, leading them to underperform and suggesting, once again, that analysts need to take into account this dimension of a network when crafting strategies to disrupt it.

Social network analysis uses the variation in actor centrality to calculate the level of centralization in a network (Wasserman and Faust 1994). More variation yields higher network centralization scores; less variation yields lower scores. In general, the larger a centralization index is, the more likely it is that a single actor is very central while the other actors are not (Wasserman and Faust 1994:176); thus,

Terrorist Network Adaptation to a Changing Environment

centralization scores can be seen as measuring how unequal the distribution of individual actor values are. However, because network centralization scores are based on various measures of centrality (e.g., degree, betweenness, closeness, and eigenvector), we need to interpret them in light of the centrality metric that is used. For example, degree centrality counts the number of ties each individual actor has; thus, the centralization metric based on it measures the extent to which one or a handful of actors possess a lot of ties while other actors in the network do not. By contrast, betweenness centrality estimates the extent to which individual actors lie in network positions that provide them with opportunities for brokering the flow of resources through a network; thus, betweenness centralization is probably best interpreted as indicating the level to which a handful of actors are in a position of brokerage. The more it is confined to a few individuals, the higher the level of betweenness centralization; the more that is distributed throughout the network, the lower the level of betweenness centralization.

Fragmentation

Network fragmentation, as its name implies, measures a network's cohesiveness (or lack thereof). It is equal to the proportion of all pairs of actors that cannot either directly or indirectly reach one another. In addition to this "traditional" approach to calculating network fragmentation, an alternative measure takes into account the (path) distance between actors. Network fragmentation metrics could prove useful for understanding how a network has changed over time as well in the crafting of strategies. For instance, if analysts were seeking to determine the degree to which different scenarios will fragment a particular network, they could estimate before and after measures of fragmentation. In fact, one social network analysis package, UCINET (Borgatti, Everett and Freeman 2011), reports a series of scores for each actor in the network that indicate the degree of network fragmentation, the degree of distance weighted network fragmentation, the change in network fragmentation, the change in distance-weighted network fragmentation, the percent of change in fragmentation, and the percent of change in distance-weighted fragmentation if a particular actor is removed from the network.

Because key actors often lie close to one another in a network, the removal of both is not always the most efficient strategy. The removal of just one plus a handful of other actors located in different parts of the network is often a better approach. Building upon this fact, Borgatti (2006) has developed a series of algorithms that instead seek to identify *sets of actors* whose removal *significantly fragments* the network (Borgatti 2011). Two variations of the algorithm exist: One that uses the traditional measure of fragmentation, and one that uses the distance-weighted measure.⁴ In this paper we do not use Borgatti's key player algorithm, but we mention it here because it illustrates the potential it holds for the crafting of strategies for the disruption of dark networks.

⁴ Borgatti has also developed two additional algorithms that identify the optimal set of actors for diffusing information or other resources through the network. The logic lying behind these algorithms is to find the optimal set of actors who are tied to (i.e., reach) as many distinct actors as possible (Borgatti 2006:29). Similar to the fragmentation algorithms, one ("Percent Nodes Reached") counts the proportion of distinct actors reached by the set, while the other ("Distance-Weighted Reach") weights this calculation by the distance between the set of key nodes and all other nodes in the network.

Terrorist Network Adaptation to a Changing Environment

Data

The Noordin Top network serves as a suitable case study for exploring the relationships between dark network structure, performance (resilience and ability to attack) and counter-terrorism strategies over time. Until his death in September 2009, Noordin Top was Indonesia's most wanted terrorist and was thought to have been the mastermind behind a series of attacks in Indonesia, namely the August 2003 Marriott bombing, the September 2004 Australian Embassy attack, and the October 2005 second Bali bombing. At one time Noordin was an active member of the well-known Jemaah Islamiyah (JI) and may have participated in the first Bali bombings of October 2002. Evidence suggests that not too long after this bombing, Noordin began to separate himself from JI and form his own terrorist network. Sought by a host of authorities in Southeast Asia, he was placed on the FBI's Seeking Information-War on Terrorism List in 2006. Noordin and his associates carried out simultaneous bombings three years later against the Ritz-Carlton and Marriott hotels in August 2009, which subsequently led to stepped-up police operations and ultimately his demise. Interestingly, not long after Noordin was killed, his network essentially fell apart, suggesting that it was structured in ways that did not facilitate its resiliency. In order to analyze Noordin's network, we utilize the relational data taken from two International Crisis Group (ICG) reports, namely "Terrorism in Indonesia: Noordin's Networks" (2006) and "Indonesia: Noordin Top's Support Base" (2009). We supplement these data with open source literature in order to generate time codes by month from January 2001 through August 2011, which allows us to account for when actors entered the network and if and when individuals were arrested or killed.

The two ICG reports on Noordin contain rich one-mode and two-mode data on a variety of relations and affiliations (friendship, kinship, meetings etc.) along with significant attribute data (education, group membership, physical status etc). From these we constructed three networks from several subnetworks each containing 237 individuals. Specifically, we created a *trust network* that is an aggregation of one-mode classmate, friendship, kinship and soulmate subnetworks. We constructed a second network, what we call Noordin's *operational network*, from four one-mode networks that were derived from corresponding two-mode networks, namely logistics, meetings, operations, and training events. We then created a *combined network* that is simply the aggregation of the *trust* and *operational* networks in order to obtain a better overall picture of the Noordin Top network. Finally, we assigned time codes to each actor in the network that indicated when they entered and left Noordin's trust, operational, and combined networks. In assigning these time codes, we assumed that ties between actors were constant over time. That is, if two actors were coded as friends at one point in time, we assumed that they remained friends throughout their mutual presence in the networks. The one exception to this concerns the meetings subnetwork where, building on the work of Krebs (2001), we assumed that a meeting tie did not form until the meeting took place (unless, of course, a tie was previously formed along another relation such as friendship or kinship). We recognize the potential limitations of these assumptions and how they may affect the estimation of the various topographic metrics we utilize in this paper. Nevertheless, we believe that the approach taken here is reasonable and valid.

One could argue that the network configurations that we utilize in this paper could have been constructed differently. The classmate subnetwork, for example, might not indicate relationships based on trust for all dark networks and within all contexts. The level in which one can make this assumption is largely based on the available data. We believe that the reports and other available data suggest that

Terrorist Network Adaptation to a Changing Environment

relationships indicating trust (i.e. friendship, kinship) in our dataset often began when actors simultaneously attend or are employed at the same academic institution. In some cases, individuals developed friendships in “JI affiliated schools” and appear to have been inducted into the group along with individuals with whom they were classmates. A similar argument goes for soulmate ties, or those actors who simultaneously attend or work at the same religious institution. We also argue that choosing which networks to parse is a part of the process for crafting strategies. The important element of this process is being clear and explicit to which networks you have aggregated so that others may follow your analysis (Everton 2012).

Moreover, some readers may question whether it is justifiable to derive one-mode networks from two-mode data since shared affiliations do not necessarily indicate the presence of a relationship between actors. While inferring such relationships in many cases is problematic, here that is not the case for a few reasons. One is that our two-mode data is largely event specific and two or more actors involved in an event are extremely likely to have interacted. For example, we can safely assume that two or more actors participating in a meeting at a specific date and location have some sort of relationship. We recognize that one could argue that actors participating in the same operation may not have been involved during the same stage (surveying targets, the actual attack etc) and therefore do not automatically know one another. On the other hand, dark network actors often form companies, transfer funds, and/or participate in any stage of an operation with people they trust, which in many cases are friends and kin. Consequently, we follow a similar argument for operations that can be used for assuming ties based on organizational affiliations, which is that if two individuals who do not know one another prior to joining a group share a common friend, then it is likely that a tie will form between them (Granovetter 1973; 1974; Holland and Leinhardt 1971; Rapoport 1953a; b; Rapoport and Horvath 1961). The data taken from the ICG reports also support our assumption by often explicitly indicating that two actors participating in the same operation have in fact interacted directly. In short, we believe not inferring ties in these cases would lead us to underestimate the number of ties within Noordin’s network.

As noted above, we use both descriptive statistics and multivariate regression analysis to explain the variation in several key topographical characteristics of Noordin’s network. We begin with our descriptive analysis of the network, visually graphing the change in the topographical metrics outlined above. We then turn to a multivariate analysis of these same metrics along with two others that are discussed below. It is to the descriptive analysis that we now turn.

Exploratory Descriptive Analysis

Figures 1 through 3 graphically present results of our analysis of the Noordin Top trust, operational, and combined networks. Specifically, the figures graph the average degree, centralization (both degree and betweenness), and fragmentation (normal and distance-weighted) for each of the three networks. The six vertical red lines in each of the graphs indicate key points in the life cycle of Noordin’s network. Moving from left to right they indicate the first Bali bombings (October 2002), the Marriott Hotel bombing (August 2003), the Australian Embassy bombing (July 2004), the second Bali bombings (October 2005), the Jakarta Hotel bombings (July 2009), and the death of Noordin and other key operatives (September 2009). Because the combined network is simply a combination of the trust and operational networks, for the most part we limit our comments to the trust and operational networks.

Terrorist Network Adaptation to a Changing Environment

Trust Network

Several observations are in order concerning the trust network. One is that it displays less variability than does the operational network and combined networks. Average degree, which functions as proxy for density, begins at a relatively low level. However, shortly after the first Bali bombing in October 2002, which is about the time that Noordin begins to pull away from JI, the network becomes increasingly provincial (i.e., dense), which is what we would expect as the network closes in on itself out of concern for security. There is a small drop just before and after the JW Marriott bombing in Jakarta in August 2003. Then we see a sharp increase through the Australian Embassy bombing in July 2004 and up to the second Bali bombings in October 2005. Then it slowly decreases for the next four years while the network was apparently on the run and relatively inactive. The July 2009 bombings of the Ritz Carlton and JW Marriott hotels mark the beginning of the end of Noordin's network. Two months later, Indonesian authorities killed Noordin and other key operatives, and coinciding with the network's demise, its average degree drops precipitously.

[Figure 1 about here]

A similar pattern is observable in the trust network's level of centralization although the effect of Noordin's death is even more pronounced. In terms of both degree and betweenness centralization, we see a steady increase from the first Bali bombing up until the Australian Embassy bombing. The increase in betweenness centralization is the more dramatic of the two, suggesting that the network became increasingly more reliant on a handful of individuals for the brokerage of information and other resources as time went by. This could reflect the fact that as Noordin pulled farther away from JI, he was forced to recruit from a variety of different resources and use individuals who could broker between him and leaders of other insurgent groups (International Crisis Group 2006). What is somewhat surprising, however, is the increase in the degree centralization of Noordin's trust network. As mentioned earlier, in rapidly changing environments, decentralized networks are typically more effective than centralized ones, and we expected to discover that Noordin's network became more decentralized over time. However, this could be an exception that proves the rule because the increasing centralization of Noordin's network may help explain why it was so vulnerable to the removal of a handful of leaders in September 2009. As we noted earlier, shortly after Noordin's death, his network fell apart. And as Baaker, Raab, and Milward (2011) argue, centralized networks are more vulnerable to exogenous shocks (e.g., the removal of central nodes) than are decentralized ones.⁵

The variation in the trust network's fragmentation levels tell a similar story (although in reverse) to the average degree story. Both fragmentation measures indicate that the network became increasingly less fragmented (i.e., more cohesive) between the first and second Bali bombings, then stabilized in the four years between the 2005 Bali bombing and the 2009 Jakarta hotel bombings, and then broke apart dramatically after Noordin and some of his key operatives were killed. The distance-weighted fragmentation measure suggests that the change over time was not as dramatic as the more traditional

⁵ It is also consistent with the contention of Barabási and his colleagues (Barabási 2002; Barabási and Albert 1999; Barabási, Albert and Jeong 1999; Barabási and Bonabeau 2003) that networks with a handful of well-connected nodes (i.e., hubs) are more vulnerable to targeted attacks than are those with few or none.

Terrorist Network Adaptation to a Changing Environment

measure indicates. This difference between the two primarily reflects the fact that while the proportion of unconnected pairs in Noordin's network decreased substantially from 2002 to 2005, so did the average (path) distance between network actors. This increase in average distance indicates the network was becoming more distributed over that period of time, and may reflect a decision on Noordin's part to spread his network out, or it may simply reflect the fact that his network was growing in size during that time. Of course, it may be a function of both.

Operational Network

The operational network reflects similar patterns to that of the trust network. Average degree remains constant from January 2001 until the Bali bombings in 2002. This is hardly surprising given Noordin's near absent role in the bombings, while this timeframe also represents the period in which Noordin and his close associates began to emerge. The subsequent drop in average degree between the Bali bombings and the August 2003 attacks likely highlights the increase in counter-terrorism operations targeting the Bali perpetrators, which removed some highly dedicated and skilled terrorists as well as putting significant pressure on others, such as Umar Patek and Dulmatin. This may have created a power vacuum within JI that Noordin was able to leverage to his own advantage. This trend reversed itself with a sharp increase from August 2003 to September 2004. One might argue that this increase lends support to theories that argue that density is positively related to command and control. The sharp decrease following the Australian Embassy bombing in September 2004 could reflect effective counter-terrorism operations on the part of Indonesian authorities, but the network rebounded immediately prior to the second Bali bombing, which could suggest that Noordin risked network security for operational success. Noordin's success, however, led to an increase in counter-terrorism operations that targeted the network; the drop in average degree following Bali II may indicate that these operations met with initial success, but they ultimately failed to prevent the July 2009 hotel bombings.

[Figure 2 about here]

The trends in network centralization for the operations network are in many ways similar to the trust network. There is an overall increase in both degree and betweenness centralization from the first Bali bombings through the second. As with the trust network, this increase in centralization initially struck us as surprising, but after considering the network's ultimate fate, it did not. It suggests that Noordin increasingly relied on fewer and fewer actors for brokerage and resources. The increase in degree centralization is more pronounced in this network, which might indicate that the operations increasingly became largely in the hands of a few actors, particularly from the August 2003 attack through the second Bali bombing as Noordin moved away from the formal JI structure. Finally, the comparison of this graph with that of the trust network suggests that Noordin relied more those with whom he could trust rather than those with whom he had an operational tie.

The operation network's fragmentation scores indicate that the network drastically became more cohesive from the August 2003 operation to the second Bali bombing and may have provided it with greater operational capability. However, the higher fragmentation scores in the immediate aftermath of the second Bali bombing highlight the largely successful counter-terrorism operations in degrading the

Terrorist Network Adaptation to a Changing Environment

network directly after the attack. This success of the Indonesian authorities, however, appears to have been only temporary, as the network appears to have begun rebounding and stabilizing around 2006. It remained fairly stable prior to the July 2009 attacks, but it almost completely disintegrates following Noordin's demise in September 2009. Although the combined network is an aggregation of the trust and operational networks, it more closely mirrors the operational network than it does the trust network in that it displays more variability than the trust network. That said, the rise and fall of average degree, centralization, and the fall and rise of fragmentation, closely follows what we see in the operational and trust networks.

[Figure 3 about here]

Multivariate Analysis

We now turn to our multivariate regression analysis of the three networks. Except where noted below, ordinary least squares (OLS) multivariate models were used to regress several outcome variables on a series of factors that we believe could account for the variation observed in Figures 1 through 3. The outcome (or dependent) variables included in our models include the topographical metrics presented in Figures 1 through 3 (average degree, degree and betweenness centralization, fragmentation, and distance-weighted fragmentation) along with two additional variables: a "recruitment" variable that attempts to capture the ability of Noordin's network to recruit new members, and a "quality" variable that indicates that extent to which Noordin was able to retain quality individuals in his network. The recruitment variable is measured by the growth or decline in the size of Noordin's network from one month to the next. The quality variable is a count of the individuals in Noordin's network who fulfilled one of the following roles: strategist, bomb maker, trainer, commander, or religious leader.⁶

Explanatory variables included in our analysis seek to capture the effect of various exogenous factors on the topography of Noordin's network. To this end we include three variables that may indicate a shift in the strategic approach taken by Indonesian authorities during the period under analysis: (1) the formation of *Detachment 88*, which is the Indonesian counter-terrorism squad, (2) the establishment of the *Jakarta Centre for Law Enforcement Cooperation* under an agreement between the Australian and Indonesian Governments, and (3) the election of *Susilo Yudhoyono* to the Indonesian Presidency. Detachment 88 was formed in July 2003 shortly after the first Bali bombings and is funded, equipped, and trained by the United States and Australia. A dummy variable is included in our models that indicates the time Detachment 88 has been in operation. The Jakarta Centre for Law Enforcement Cooperation (JCLEC) was established in July 2004 under an agreement between the Australian and Indonesian Governments. It is located in Semarang, Indonesia, and provides a range of training programs, seminars and workshops on the priority issues for law enforcement with the goal of enhancing regional law enforcement capacity. A dummy variable is included in our models that indicates the formation of the center and its continued existence. Finally, in October 2004, Susilo Yudhoyono, a retired Army general, ascended to the Presidency of Indonesia; he was reelected in 2009 and is currently the President. He ran on a platform to combat terrorist groups such as *JI* and *Noordin Top*. Thus, a dummy variable is included

⁶ Because in the quality variable is a count variable, a poisson model, rather than a traditional OLS model, was used to analyze the data.

Terrorist Network Adaptation to a Changing Environment

in the analysis to capture the effect, if any, of the policies he put into place to fulfill this pledge. We have also included a dummy variable that attempts to measure the effect of the death of Noordin and a few of his key operatives had on his network. Specifically, we have included a dummy variable that indicates the *death of Noordin and his key operatives* and their subsequent “absence” from the network from September 2009 through the end of our analysis. We also have added a series of *post-operation* dummy variables that capture the three-month period immediately following each of the five major operations: Bali I, the JW Marriott Hotel bombing, the Australian Embassy bombing, Bali II, and the Jakarta Hotel bombings. Not surprisingly, in each of these periods, Indonesian authorities increased their efforts to kill or capture Noordin and his colleagues, and we expect that these operations caused his network to become increasingly dense and less fragmented. Initially, we believed that such operations would have lead Noordin to decentralize his network, but as we just saw in Figures 1 through 3, that was not the case.

Finally, to control for the curvilinear effect that time appears to have on the various dependent variables (see Figures 1 through 3), independent variables that capture the passage of time are included in our models. Specifically, a *month* variable is included in order to model the initial effects of time, while a *month squared* variable is included in order to capture the apparent opposite effects of time.

Results

Tables 1 through 3 present the estimated coefficients for multivariate regression models that regresses various topographical measures on the explanatory variables. Table 1 includes the results for the trust network, Table 2 includes the results for the operational network, and Table 3 includes the results for the combined network. Because there are three tables with each containing seven dependent variables and eleven independent variables, it is impossible to discuss all 231 coefficients. Thus, we concentrate on overall patterns and focus on coefficients that are both substantively and statistically significant (McCloskey 1995; Ziliak and McCloskey 2008).⁷

[Tables 1 through 3 about here]

The tables contain many interesting findings. Most notably, the adjusted R^2 for the models that regress average degree, the two centralization measures, and the two fragmentation measures on the various independent variables are extremely high and indicate that our models largely account for the variation in most of our dependent variables. Adjusted R^2 scores above 0.20 warm the hearts of all but the most hardened social scientists, and the fact that they range from .80 to .90 should provide us with the confidence that our models do an adequate job of explaining the variability in our dependent variables. Our models are not quite as good at predicting Noordin’s ability to recruit new members although they do reasonably well with R^2 ’s ranging from .25 to .32. The same cannot be said of the models that attempt to explain the retention of quality individuals. None of the coefficients in any of the models are statistically significant, and the adjusted R^2 ’s are relatively low (at least when compared to the others). This could indicate one of two things. Either the models are not well specified, or that we have inadequately

⁷ Because we are not working with a random sample here but a complete sample, statistical significance does technically apply. However, because measures of statistical significance are a function of the size of coefficients (a measure of substantive significance) and the coefficients’ underlying variance, they can be reasonably used as indicators of importance.

Terrorist Network Adaptation to a Changing Environment

operationalized our measure of what constitutes a "quality" individual. We will reexamine this issue in order to determine if we can capture this variable in our future work, which could provide insight into the relationship between network characteristics and performance.

As far as the post operation periods, it appears that the three months immediately following the Marriott bombing (and to a lesser extent, the three months following the Australian Embassy bombing), Noordin's trust network became less dense, less centralized (at least in terms of degree centralization), and less cohesive (i.e., more fragmented). It also experienced a downturn in its ability to recruit new members, which may have been the result of the network having to operate in an increasingly hostile environment. The same basic pattern holds true for the operational and combined networks.

The deaths of key individuals (including Noordin) clearly had a deleterious effect on the network. They led to a serious decrease in its average degree, centralization (both measures), and cohesiveness (i.e., an increase in fragmentation -- both measures). The structural characteristics of the network prior to Noordin's death suggest that a few other actors possessed the majority of the command and control, which may have permitted the network to be successful in July 2009, but ultimately made the network extremely vulnerable. As we noted earlier, this provides support for Bakker, Raab and Milward's (2011) contention that decentralized networks are less vulnerable to exogenous shocks than are centralized ones. These results are also unsurprising given that only remnants of the network continued to operate after Noordin's death, some of which were involved in the "al-Qaeda in Aceh" group that was broken up last year (International Crisis Group 2010). Put simply, while the targeting of key individuals does not always lead to the implosion of dark networks, it can when the network that is targeted is highly centralized, which in this case it was.

It appears that in the long run the formation of Detachment 88 and the JCLEC helped lead to the demise of Noordin's network. Both appear to have led to an increase in the trust network's average degree, and the formation of the JCLEC appears to have caused an increase in the average degree of the operational and combined networks. It is hard to say whether this was a good or bad move on the part of the network. It is what we would expect, though, since as we have already discussed, all else being equal, dark networks should be denser than light networks and become increasingly dense in the face of hostile environments. It also appears that the formation of the two institutions helped cause the trust, operational, and combined networks to become more centralized. Interestingly, the formation of Detachment 88 appears to have helped Noordin's recruitment efforts. As the coefficients indicate, the effect is both positive and statistically significant. It is not certain why this occurred, but it is possible that the presence of the U.S. and Australian trained and funded counter-terrorist unit fed into anti-Western sentiment within some circles.

The election of President Yudhoyono had some effect, but not always in the expected magnitude or direction. In terms of the trust network, his election led to an increase in betweenness centralization and network cohesiveness. This could have resulted for multiple reasons. One possibility is the President's active counter-terrorism policies that specifically targeted Noordin's network; another, one that was mentioned previously, is that Noordin increasingly relied on a handful of individuals to broker and reach out to other groups as his network faced hostile environmental pressures and moved farther away from JI. Interestingly, Yudhoyono's policies appear to have been among the factors that led Noordin's network to become more cohesive (i.e., less fragmented) but less dense (at least in terms of the operational and combined networks).

Terrorist Network Adaptation to a Changing Environment

Conclusion: Strategic Implications

What implications does this analysis have for the crafting of strategies for the disruption of networks? In answering this question it is helpful to distinguish between two general approaches to countering dark networks: kinetic and non-kinetic (Roberts and Everton 2011).⁸ The kinetic approach pursues aggressive measures designed to eliminate or capture network members and their supporters and employs such things as bombs and bullets to pursue the campaign. It can be further subdivided into two types of kinetic action: action directed by the U.S. military and action directed by the host-nation military. By contrast, the non-kinetic approach employs neither bombs nor bullets but instead uses non-coercive means to counter networks and impair a combatant's will to fight. It includes activities such as the reconstruction of war-torn areas, the disruption of electronic fund transfer networks, information campaigns to win over the "hearts and minds" of local populations, and efforts at the rehabilitation and reintegration of dark network members into civil society. Like the kinetic approach, it too can be U.S. or host-nation led.

Based solely on the results of this study, one might conclude that decapitation strategies are an effective approach for disrupting dark networks. Such a conclusion, however, would fail to take into account the fact that this strategy probably only succeeded because Noordin appears to have made the crucial strategic mistake of centering his network around a few key actors. If he had not, then alternative strategies may have proven more successful. In fact, one could argue that the establishment and gradual improvement of counter-terror organizations, such as Detachment 88, along with improved counter-terrorism training and targeting operations, appear to have been critical to creating the environment that caused Noordin to turn inward and place the future of his organization in the hands of a few people. In other words, without the Indonesian authorities non-kinetic approaches to disrupting Noordin's network, the killing of Noordin in September of 2009 may have had less of an effect than it did.

Something else to keep in mind is that, as Charles Tilly (2004; 2005) has noted, throughout history covert networks (e.g., insurgencies, trade diasporas, clandestine religious groups, terrorist groups)⁹ have segregated themselves from what they perceive to be hostile or predatory regimes. Tilly argues, however, that regimes, and in particular democratic ones, cannot survive without at least the partial integration of these networks back into civil society. In other words, although the Indonesian authorities appear to have successfully put an end to Noordin's network, there is still work for them to do. Specifically, they need to pursue strategies that facilitate the reintegration of members of Noordin's network and other insurgent groups into Indonesian society. If they do not, there is a strong possibility that a new insurgency will raise its ugly head and pick up where Noordin left off.

To conclude: this paper has sought to demonstrate the utility of analyzing longitudinal dark network data. It moved beyond previous research by examining the relationship between resilience, structure and performance, and strategies targeting dark networks. It has also sought to highlight the utility of alternative strategies targeting dark networks and the effect that non-kinetic strategies have on shaping these networks. Clearly, we have only begun to scrape the surface of what is possible in the examination

⁸There is no agreement in the literature on how to describe the alternative approaches to countering terrorism. Some authors use different characterizations e.g. direct and indirect strategies (Arreguin-Toft 2001; 2005; Fridovich and Krawchuck 2007; Krawchuck ND). Our preference is to focus on the behavior of the combatants and the level of the coercion involved in their strategies and hence we have chosen to use the terms "kinetic" and "non-kinetic."

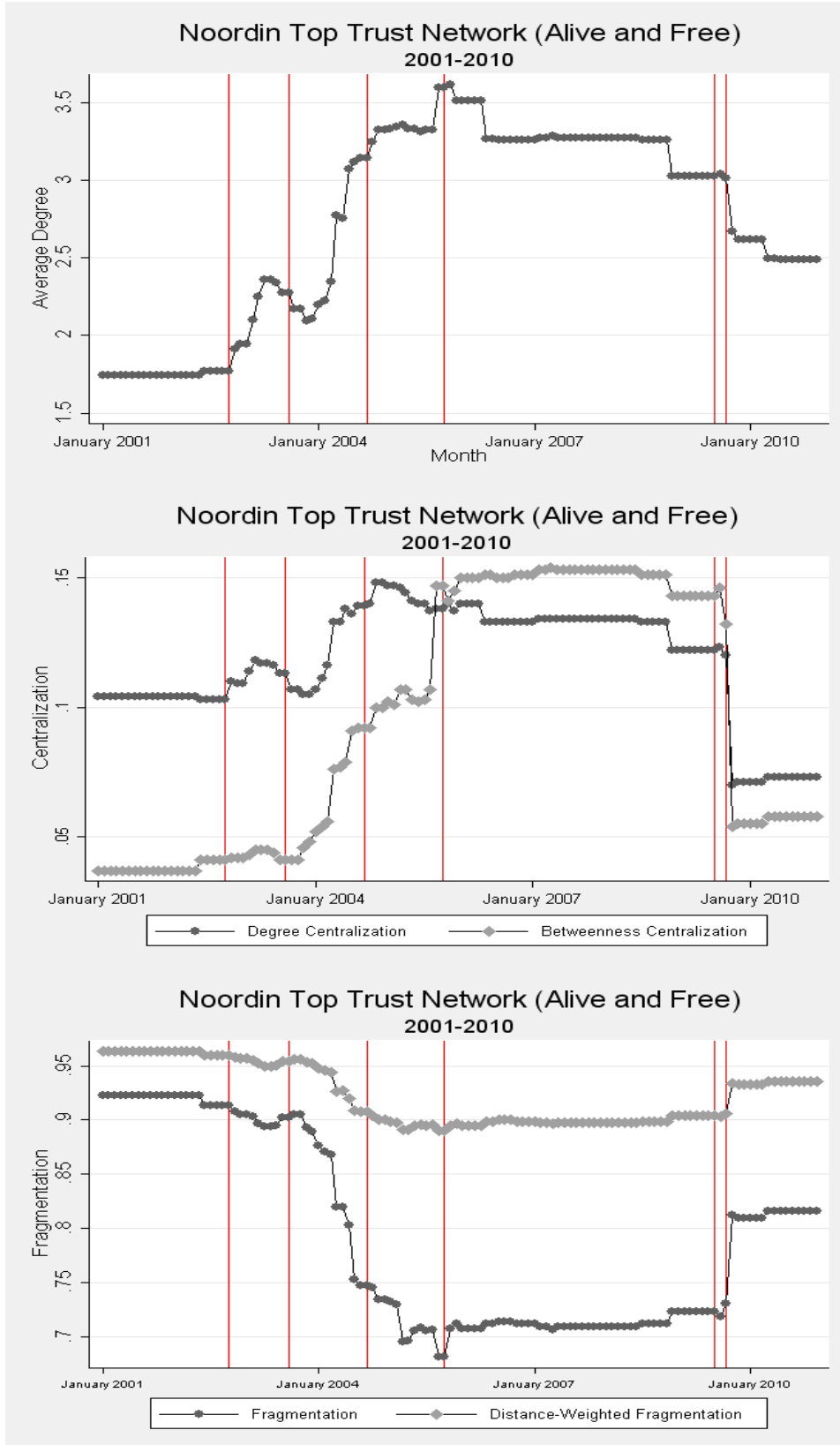
⁹ Tilly defines trust networks as "ramified interpersonal connections, consisting mainly of strong ties, within which people set valued, consequential long-term resources and enterprises at risk to the malfeasance, mistakes, or failures of others" (Tilly 2005:41)

Terrorist Network Adaptation to a Changing Environment

of longitudinal networks. In the future analysts will want to expand the approach taken here and employ more sophisticated modeling techniques, such as McCulloh and Carley's (2011) social network change detection (SNCD) approach or Snijders (Snijders 2005; Snijders, Bunt and Steglich 2010) stochastic actor-based models.

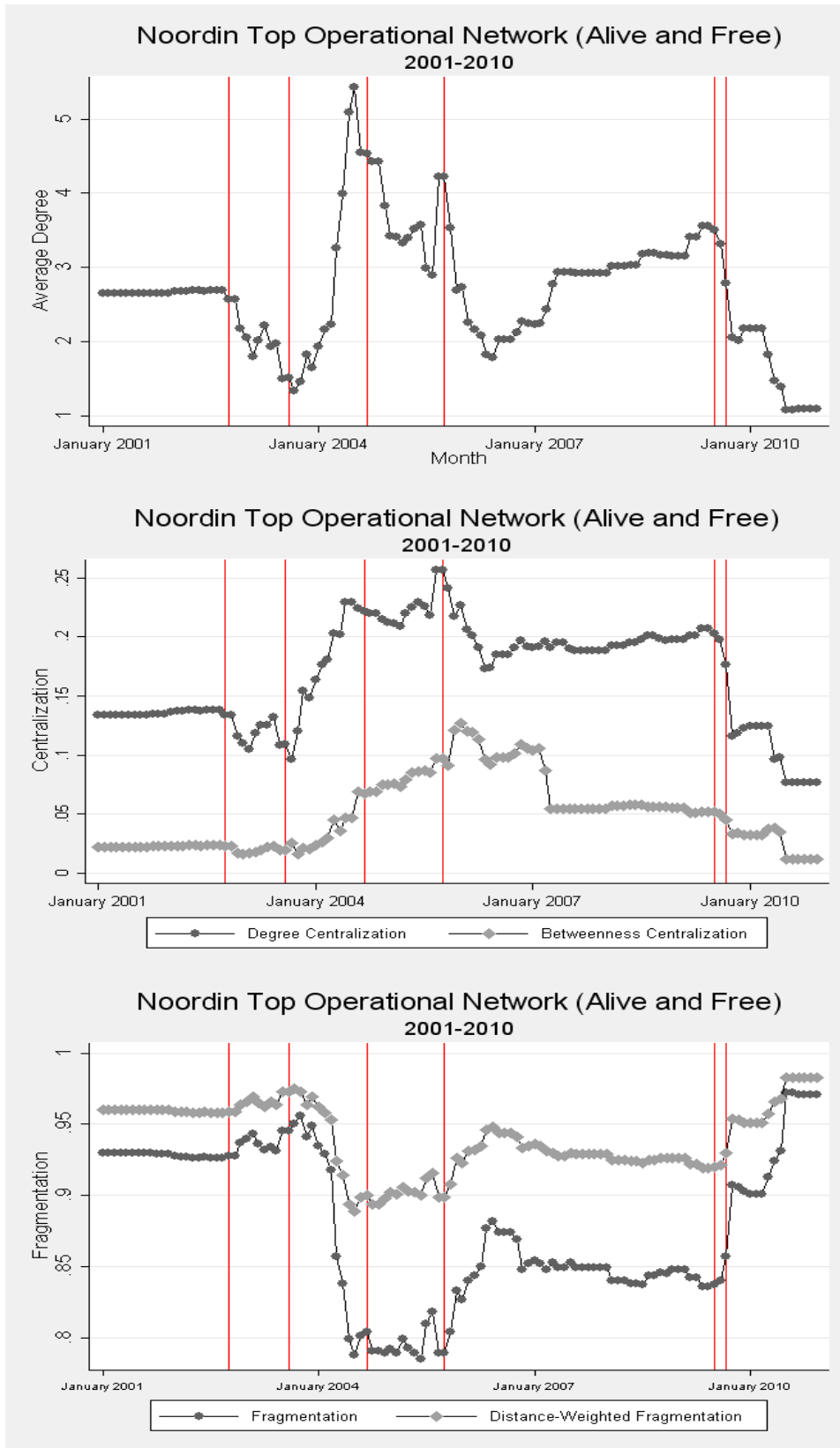
Figures

Figure 1: Noordin Top Trust Network (Alive and Free)



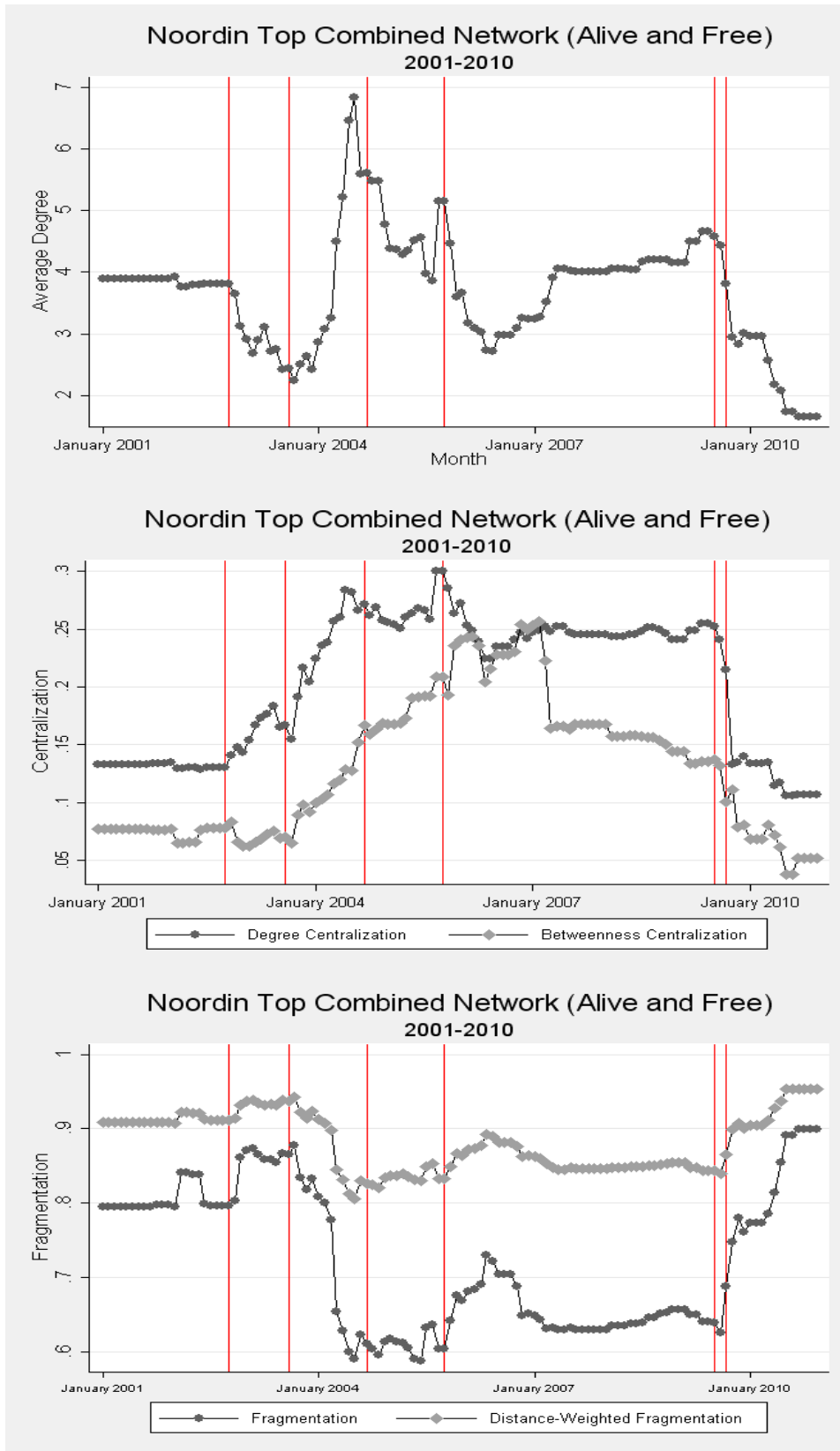
Figures

Figure 2: Noordin Top Operational Network (Alive and Free)



Figures

Figure 3: Noordin Top Combined Network (Alive and Free)



Tables

Table 1: Multivariate Regression Results for Noordin Top Trust Network (Alive and Free)

	Average Degree	Centralization Degree	Betweenness	Fragmentation	Distance Fragmentation	Recruitment	Quality Individuals
Intercept	-59.026	-1.425	-1.404	4.670	2.549	-91.490	2.575
Month	0.222***	0.006***	0.005*	-0.014***	-0.006***	0.356	0.003
Month ²	-0.000***	-0.000***	-0.000*	0.000***	0.000***	-0.000	-0.000
Post Bali I (2002)	-0.138	-0.002	-0.006	0.003	0.002	0.047	-0.024
Post Marriott (2003)	-0.269**	-0.012***	-0.013	0.037***	0.013***	-2.807*	-0.194
Post Australian (2004)	-0.010	0.006*	-0.028***	0.026**	0.004	1.045	-0.116
Post Bali II (2005)	0.190*	0.000	0.011	0.001	-0.000	-2.032	0.099
Post Hotels (2009)	0.010	0.003	-0.011	0.002	0.001	-2.145*	-0.008
Key Deaths	-0.300***	-0.045***	-0.100***	0.081***	0.026***	0.702	-0.122
Detachment 88	0.251**	0.007*	-0.001	-0.031***	-0.010***	3.548***	-0.042
JCLEC	0.624***	0.019***	0.028***	-0.108***	-0.031***	-1.709	0.119
President Yudhoyono	0.156	0.001	0.031***	-0.036***	-0.010***	-0.669	0.147
Adjust R ²	0.959	0.953	0.955	0.983	0.978	0.317	0.112
Note: N=120; * p < .05	** p < .01	*** p < .001	(two-tailed)				

Tables

Table 2: Multivariate Regression Results for Noordin Top Operational Network (Alive and Free)

	Average Degree	Centralization Degree	Betweenness	Fragmentation	Distance Fragmentation	Recruitment	Quality Individuals
Intercept	58.935	-0.309	-2.460	2.151	1.084	70.948	2.715
Month	-0.205	0.002	0.010***	-0.005	-0.001	-0.239	0.003
Month ²	0.000	-0.000	-0.000***	0.000	0.000	0.000	-0.000
Post Bali I (2002)	0.076	-0.003	-0.002	0.000	-0.001	-0.944	-0.024
Post Marriott (2003)	-1.084**	-0.046***	-0.010	0.048**	0.025**	-13.226***	-0.194
Post Australian (2004)	1.333***	0.007	-0.026**	-0.031	-0.023**	-1.139	-0.115
Post Bali II (2005)	0.146	0.021	0.023**	-0.006	-0.002	-2.773	0.100
Post Hotels (2009)	0.146	0.004	0.003	-0.016	-0.008	-3.524	-0.007
Key Deaths	-1.680***	-0.082***	-0.003	0.065***	0.033***	-0.458	-0.122
Detachment 88	0.410	0.042***	0.008	-0.033*	-0.018*	6.031**	-0.042
JCLEC	2.308***	0.058***	0.033***	-0.106***	-0.052***	-3.888	0.119
President Yudhoyono	-1.920***	-0.013	0.037***	0.022	-0.022**	0.233	0.146
Adjust R ²	0.538	0.831	0.847	0.801	0.729	0.262	0.112
Note: N=120; * p < .05	** p < .01	*** p < .001	(two-tailed)				

Tables

Table 3: Multivariate Regression Results for Noordin Top Combined Network (Alive and Free)

	Average Degree	Centralization Degree	Betweenness	Fragmentation	Distance Fragmentation	Recruitment	Quality Individuals
Intercept	89.888	-3.934	-4.915	-0.598	-0.084	72.977	2.575
Month	-0.312*	0.015***	0.010***	-0.005	0.004	-0.246	0.003
Month ²	0.000*	-0.000***	-0.000***	0.000	-0.000	0.000	-0.000
Post Bali I (2002)	0.136	-0.115	-0.003	0.005	-0.001	-0.938	-0.024
Post Marriott (2003)	-1.223**	-0.036**	-0.017	0.087**	0.038**	-13.227***	-0.194
Post Australian (2004)	1.303**	0.014	-0.055***	-0.022	-0.023	-1.145	-0.116
Post Bali II (2005)	0.066	0.020*	0.015	0.026	0.008	-2.774	0.100
Post Hotels (2009)	0.210	-0.004	0.000	-0.030	-0.011	-3.525	-0.008
Key Deaths	-2.116***	-0.105***	-0.040***	0.168***	0.076***	-0.464	-0.122
Detachment 88	0.534	0.061***	0.021	-0.079**	-0.036*	6.046**	-0.042
JCLEC	2.482***	0.042***	0.050**	-0.157***	-0.071***	-3.884	0.119
President Yudhoyono	-2.030***	-0.026*	0.071***	0.016	0.028*	0.240	0.147
Adjust R ²	0.636	0.922	0.875	0.801	0.752	0.262	0.113
Note: N=120; * p < .05	** p < .01	*** p < .001	(two-tailed)				

References

- Aristotle. 1998. *The Nichomachean Ethics*. Translated by David Ross, J. L. Ackrill, and J. O. Urmson. Oxford and New York: Oxford University Press.
- Arquilla, John, and David Ronfeldt. 2001. "The Advent of Netwar (Revisited)." Pp. 1-25 in *Networks and Netwars*, edited by John Arquilla and David Ronfeldt. Santa Monica, CA: RAND.
- Arreguin-Toft, Ivan. 2001. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26:93-128.
- _____. 2005. *How the Weak Win Wars: A Theory of Asymmetric Conflict*. Cambridge, UK: Cambridge University Press.
- Bakker, René M., Jörg Raab, and H. Brinton Milward. 2008. A Preliminary Theory of Dark Network Resilience. Paper read at Sunbelt XXVIII: The Annual Meeting of the International Network for Social Network Analysis, at St. Pete Beach, FL.
- _____. 2011. "A Preliminary Theory of Dark Network Resilience." *Journal of Policy Analysis and Management* 31.
- Banks, David, and Kathleen Carley. 1996. "Models for Network Evolution." *Journal of Mathematical Sociology* 21:173-196.
- Barabási, Albert-László. 2002. *Linked: The New Science of Networks*. Cambridge, MA: Perseus Publishing.
- Barabási, Albert-László, and Reka Albert. 1999. "Emergence of Scaling in Random Networks." *Science* 286:509-512.
- Barabási, Albert-László, Reka Albert, and Hawoong Jeong. 1999. "Mean-Field Theory for Scale-Free Random Networks." *Physica A* 272.
- Barabási, Albert-László, and Eric Bonabeau. 2003. "Scale-Free Networks." *Scientific American* 288:60-69.
- Berman, Eli. 2009. *Radical, Religious, and Violent: The New Economics of Terrorism*. Cambridge, Massachusetts: The MIT Press.
- Bienenstock, Elisa Jayne, and Phillip Bonacich. 2003. "Balancing Efficiency and Vulnerability in Social Networks." Pp. 253-264 in *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*, edited by Ron Breiger, Kathleen Carley, and Philippa Pattison. Washington DC: National Academy of Sciences / National Research Council: National Academies Press.
- Borgatti, Stephen P. 2006. "Identifying Sets of Key Players in a Social Network." *Computational, Mathematical and Organizational Theory* 12:21-34.
- _____. 2011. *Key Player 1.45*. Lexington, KY: Analytical Technologies.
- Borgatti, Stephen P., Martin G. Everett, and Linton C. Freeman. 2011. *UCINET for Windows: Software for Social Network Analysis*. Lexington, KY: Analytical Technologies.
- Breiger, Ron, Kathleen Carley, and Philippa Pattison (Eds.). 2003. *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*. Washington DC: National Academy of Sciences / National Research Council: National Academies Press.
- Burns, Tom, and G. M. Stalker. 1961. *The Management of Innovation*. London: Tavistock.
- Carley, Kathleen. 2003. "Dynamic Network Analysis." Pp. 133-145 in *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*, edited by Ron Breiger, Kathleen Carley, and Philippa Pattison. Washington DC: National Academy of Sciences / National Research Council: National Academies Press.
- Carley, Kathleen M. 2001-2011. *Organizational Risk Analyzer (ORA)*. Pittsburgh, PA: Center for Computational Analysis of Social and Organizational Systems (CASOS): Carnegie Mellon University.
- _____. 2006. "A Dynamic Network Approach to the Assessment of Terrorist Groups and the Impact of Alternative Courses of Action." *Visualizing Network Information Meeting Proceedings RTO-MP-IST-063*. Neuilly-sur-Seine, France: RTO. Retrieved from http://www.vistg.net/documents/IST063_PreProceedings.pdf
- Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. 2002. "Destabilizing Networks." *Connections* 24:79-92.

References

- Castells, Manuel. 1996. *The Information Age: Economy, Society and Culture, Vol. I: The Rise of the Network Society*. Malden, MA: Blackwell Publishers.
- de Nooy, Wouter. 2011. "Networks of Action and Events over Time: A Multilevel Discrete-Time Event History Model for Longitudinal Network Data." *Social Networks* 33:31-40.
- de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. 2005. *Exploratory Social Network Analysis with Pajek*. Cambridge, UK: Cambridge University Press.
- Doreian, Patrick, and F. N. Stockman (Eds.). 1997. *Evolution of Social Networks*. Amsterdam: Gordon and Breach Publishers.
- Enders, Walter, and Xuejuan Su. 2007. "Rational Terrorists and Optimal Network Structure." *Journal of Conflict Resolution* 51:33-57.
- Everton, Sean. 2012. *Disrupting Dark Networks*. Cambridge and New York: Cambridge University Press.
- Finke, Roger, and Rodney Stark. 2005. *The Churching of America, 1776-2005: Winners and Losers in Our Religious Economy*. 2nd ed. New Brunswick, NJ: Rutgers University Press.
- Fridovich, David P., and Fred T. Krawchuck. 2007. "Special Operations Forces: Indirect Approach." *Joint Forces Quarterly* 44:24-27.
- Granovetter, Mark. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 73:1360-1380.
- _____. 1974. *Getting a Job*. Cambridge, MA: Harvard University Press.
- _____. 1983. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* 1:201-233.
- _____. 2005. "The Impact of Social Structure on Economic Outcomes." *Journal of Economic Perspectives* 19:33-50.
- Helfstein, Scott, and Dominic Wright. 2011. "Covert or Convenient? Evolution of Terror Attack Networks." *Journal of Conflict Resolution*.
- Holland, Paul W., and Samuel Leinhardt. 1971. "Transitivity of Structural Models of Small Groups." *Comparative Group Studies* 2:107-124.
- Hu, Daning, Siddharth Kaza, and Hsinchun Chen. 2009. "Identifying Significant Facilitators of Dark Network Evolution." *Journal of the American Society for Information Science and Technology* 60:655-665.
- International Crisis Group. 2006. "Terrorism in Indonesia: Noordin's Networks." Brussels, Belgium: International Crisis Group.
- _____. 2009. "Indonesia: Noordin Top's Support Base." Brussels, Belgium: International Crisis Group.
- _____. 2010. "Indonesia: Jihadi Surprise in Aceh." Brussels, Belgium: International Crisis Group.
- Kenney, Michael. 2007. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park: Pennsylvania State University Press.
- Klerks, Peter. 2001. "The Network Paradigm Applied to Criminal Organisations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands." *Connections* 24:53-65.
- Koschade, Stuart. 2006. "A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence." *Studies in Conflict & Terrorism* 29:559-575.
- Kossinets, Georgi, and Duncan J. Watts. 2006. "Empirical Analysis of an Evolving Social Network." *Science* 311:88-90.
- _____. 2009. "Origins of Homophily in an Evolving Social Network." *American Journal of Sociology* 115:405-50.
- Krackhardt, David. 1992. "The Strength of Strong Ties: The Importance of Philos in Organizations." Pp. 216-239 in *Networks and Organizations: Structure, Form and Action*, edited by Nitin Nohria and Robert G. Eccles. Boston: Harvard University Press.
- Krawchuck, Fred T. ND. "Winning the Global War on Terrorism in the Pacific Region: Special Operations Forces' Indirect Approach to Success." Retrieved from <http://igcc.ucsd.edu/pdf/krawchuk.pdf> (accessed February 26, 2009)
- Krebs, Valdis. 2001. "Mapping Networks of Terrorist Cells." *Connections* 24:43-52.

References

- Leenders, Roger Th. A. J. 1996. "Evolution of Friendship and Best Friendship Choices." *Journal of Mathematical Sociology* 21:133-148.
- Lindelauf, Roy, Peter Borm, and Herbert Hamers. 2009. "Understanding Terrorist Network Topologies and Their Resilience Against Disruption." *CentER Discussion Paper No. 85*.
- McCloskey, Deirdre. 1995. "The Insignificance of Statistical Significance." *Scientific American* April:32-33.
- McCulloh, Ian, and Kathleen Carley. 2011. "Detecting Change in Longitudinal Social Networks." *Journal of Social Structure*. 12(3). Retrieved from <http://www.cmu.edu/joss/content/articles/volume12//McCullohCarley.pdf>
- Milward, H. Brinton, and Jörg Raab. 2006. "Dark Networks as Organizational Problems: Elements of a Theory." *International Public Management Journal* 9:333-360.
- Nohria, Nitin, and Robert G. Eccles (Eds.). 1992. *Networks and Organizations: Structure, Form, and Action*. Boston: Harvard Business School Press.
- Pescosolido, Bernice A., and Sharon Georgianna. 1989. "Durkheim, Suicide, and Religion: Toward a Network Theory of Suicide." *American Sociological Review* 54:33-48.
- Podolny, Joel M., and Karen L. Page. 1998. "Network Forms of Organization." Pp. 57-76 in *Annual Review of Sociology 1998*. Palo Alto: Annual Reviews, Inc.
- Powell, Walter W. 1985. "Hybrid Organizational Arrangements: New Form or Transitional Development." *California Management Review* 30:67-87.
- _____. 1990. "Neither Market Nor Hierarchy: Network Forms of Organization." Pp. 295-336 in *Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews*, edited by Barry M. Staw and L. L. Cummings. Greenwich, CT: JAI Press, Inc.
- Powell, Walter W., and Laurel Smith-Doerr. 1994. "Networks and Economic Life." Pp. 368-402 in *The Handbook of Economic Sociology*, edited by Neil J. Smelser and Richard Swedberg. Princeton, N.J.: Princeton University Press.
- Raab, Jörg, and H. Brinton Milward. 2003. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13:413-439.
- Rapoport, Anatole. 1953a. "Spread of Information Through a Population with Socio-Structural Bias I: Assumption of Transitivity." *Bulletin of Mathematical Biophysics* 15:523-533.
- _____. 1953b. "Spread of Information Through a Population with Socio-Structural Bias II: Various Models with Partial Transitivity." *Bulletin of Mathematical Biophysics* 15:535-546.
- Rapoport, Anatole, and W. J. Horvath. 1961. "A Study of a Large Sociogram." *Behavioral Science* 6:279-291.
- Roberts, Nancy, and Sean F. Everton. 2011. "Strategies for Combating Dark Networks." *Journal of Social Structure*. 12(2). Retrieved from <http://www.cmu.edu/joss/content/articles/volume12//RobertsEverton.pdf>
- Robins, Gary, and Philippa Pattison. 2001. "Random Graph Models for Temporal Processes in Social Networks." *Journal of Mathematical Sociology* 25:5-41.
- Rodriguez, Jose' A. 2005. "The March 11th Terrorist Network: In Its Weakness Lies Its Strength." *EPP-LEA Working Papers*. Barcelona, Spain: Departament de Sociologia i Anàlisi de les Organitzacions: Universitat de Barcelona. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.98.4408> (accessed March 3, 2009)
- Ronfeldt, David, and John Arquilla. 2001. "What Next for Networks and Netwars?" Pp. 311-361 in *Networks and Netwars*, edited by John Arquilla and David Ronfeldt. Santa Monica, CA: RAND.
- Sageman, Marc. 2004a. "Statement to the National Commission on Terrorist Attacks Upon the United States."
- _____. 2004b. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press.
- Scott, John. 2000. *Social Network Analysis: A Handbook*. 2nd ed. Thousand Oaks, CA: Sage Publications.
- Snijders, Tom A. B. 2001. "The Statistical Evaluation of Social Network Dynamics." *Sociological Methodology* 31:361-395.

References

- _____. 2005. "Models for Longitudinal Network Data." Pp. 215-247 in *Models and Methods in Social Network Analysis*, edited by Peter J. Carrington, John Scott, and Stanley Wasserman. New York: Cambridge University Press.
- Snijders, Tom A. B., Gerhard G. van de Bunt, and Christian Steglich. 2010. "Introduction to Stochastic Actor-based Models for Network Dynamics." *Social Networks* 32:44-60.
- Stark, Rodney. 1987. "How New Religions Succeed: A Theoretical Model." Pp. 11-29 in *The Future of New Religious Movements*, edited by David G. Bromley and Phillip E. Hammond. Macon Georgia: Mercer University Press.
- _____. 1996. "Why Religious Movements Succeed or Fail: A Revised General Model." *Journal of Contemporary Religion* 11:133-146.
- _____. 2005. *The Rise of Mormonism*. Edited by Reid L. Nielson. New York: Columbia University Press.
- _____. 2007. *Sociology*. 10th ed. Belmont, CA: Wadsworth Publishing Company.
- Steglich, Christian, Tom A. B. Snijders, and Michael Pearson. 2010. "Dynamic Networks and Behavior: Separating Selection From Influence." Pp. 329-393 in *Sociological Methodology*. Washington DC: American Sociological Association.
- Tilly, Charles. 2004. "Trust and Rule." *Theory and Society* 33:1-30.
- _____. 2005. *Trust and Rule*. Cambridge and New York: Cambridge University Press.
- Tsvetovat, Maksim, and Kathleen M. Carley. 2005. "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence." *Journal of Social Structure*. 6. Retrieved from <http://www.cmu.edu/joss/content/articles/volume6/TsvetovatCarley/index.html>
- Tucker, David. 2008. "Terrorism, Networks and Strategy: Why the Conventional Wisdom is Wrong." *Homeland Security Affairs*. 4:2 (June 2008). Retrieved from www.hsaj.org
- U.S. Army. 2007. *U.S. Army/Marine Counterinsurgency Field Manual (FM 3-24)*. Old Saybrook, CT: Konecky & Konecky.
- Uzzi, Brian. 1996. "The Sources and Consequences of Embeddedness for the Economic Performance of Organizations: The Network Effect." *American Sociological Review* 61:674-698.
- Uzzi, Brian, and Jarrett Spiro. 2005. "Collaboration and Creativity: The Small World Problem." *American Journal of Sociology* 111:447-504.
- Van de Bunt, G.G., M.A.J. Van Duijin, and Tom A. B. Snijders. 1999. "Friendship Networks through Time: An Actor-Oriented Statistical Network Model." *Computational and Mathematical Organization Theory* 5:167-192.
- Wasserman, Stanley. 1980. "A Stochastic Model for Directed Graphs with Transition Rates Determined by Reciprocity." *Sociological Methodology* 11:392-412.
- Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. Cambridge, UK: Cambridge University Press.
- Xu, Jie, Daning Hu, and Hsinchun Chen. 2009. "The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad." *Journal of Homeland Security and Emergency Management* 6:Article 1.
- Ziliak, Stephen T., and Deirdre N. McCloskey. 2008. *The Cult of Statistical Significance*. Ann Arbor: The University of Michigan Press.