



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Publications

2015

Dark Network Resilience in a Hostile Environment: Optimizing Centralization and Density

Everton, Sean F.; Cunningham, Dan

S.F. Everton, D. Cunningham, "Dark Network Resilience in a Hostile Environment: Optimizing Centralization and Density," *Criminology, Criminal Justice Law, & Society*, Vol. 16, Issue 1, pp. 1-20, (2015)
<https://hdl.handle.net/10945/46761>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



E-ISSN 2332-886X

Available online at

<https://scholasticahq.com/criminology-criminal-justice-law-society/>

Dark Network Resilience in a Hostile Environment: Optimizing Centralization and Density

Sean F. Everton and Dan Cunningham

Naval Postgraduate School

ABSTRACT AND ARTICLE INFORMATION

In recent years, the world has witnessed the emergence of violent extremists (VEs), and they have become an ongoing concern for countries around the globe. A great deal of effort has been expended examining their nature and structure in order to aid in the development of interventions to prevent further violence. Analysts and scholars have been particularly interested in identifying structural features that enhance (or diminish) VE resilience to exogenous and endogenous shocks. As many have noted, VEs typically seek to balance operational security and capacity/efficiency. Some argue that their desire for secrecy outweighs their desire for efficiency, which leads them to be less centralized with few internal connections. Others argue that centralization is necessary because security is more easily compromised and that internal density promotes solidarity and limits countervailing influences. Unsurprisingly, scholars have found evidence for both positions. In this paper, we analyze the Noordin Top terrorist network over time to examine the security-efficiency tradeoff from a new perspective. We find that the process by which they adopt various network structures is far more complex than much of the current literature suggests. The results of this analysis highlight implications for devising strategic options to monitor and disrupt dark networks.

Article History:

Received 26 April 2014

Received in revised form 9 Sept 2014

Accepted 17 Sept 2014

Keywords:

dark networks, terrorism, social network analysis.

© 2015 *Criminology, Criminal Justice, Law & Society* and The Western Society of Criminology
Hosting by Scholastica. All rights reserved.

Violent extremist networks (aka covert networks, dark networks) are an ongoing concern for countries around the globe. Their nature and structure have been examined for the purpose of developing interventions that destabilize, disrupt, or otherwise prevent further violence. Identifying structural features that enhance (or diminish) their resilience to exogenous and endogenous shocks is of particular interest. As many have noted, groups generally seek to balance operational security and capacity/efficiency (see e.g., *Combating Terrorism Center*, 2006; Crossley, Edwards, Harries, &

Stevenson, 2012; McCormick & Owen, 2000; Morselli, Giguère, & Petit, 2007). A consensus, however, has not been reached as to which features enhance the ability of dark networks to maintain such a balance. For example, existing literature offers two somewhat conflicting hypotheses about the relationship between network structure and operational security. Some argue that when the desire for secrecy outweighs the desire for efficiency, dark networks tend to be internally sparse and decentralized (Baker & Faulkner, 1993; Enders & Su, 2007; Raab & Milward, 2003). Others argue just the

Corresponding author: Sean F. Everton, Naval Postgraduate School, 1 University Circle, Monterey, CA, 93943, USA.

Email: sfeverto@nps.edu

opposite: the desire for secrecy leads dark networks toward high levels of centralization and density. Centralization is necessary because security can be compromised when transactions have to traverse long paths, and this can be overcome when a central hub coordinates activity (Lindelauf, Borm, & Hamers, 2009). They also contend that density is the norm among dark networks because it promotes solidarity and limits countervailing influences (Coleman, 1988), as well as the fact that they recruit primarily along lines of trust (Erickson, 1981).

Evidence has been found for several points of view regarding the security-efficiency tradeoff (Crossley et al., 2012; Everton & Cunningham, 2013). One reason is because how one measures centralization and density profoundly affects one's results and conclusions (Crossley et al., 2012). For example, centralization is often based on degree centrality (Freeman, 1979), but it is unclear whether this best captures the type of centralization found in dark networks. Measurement problems exist in terms of density as well. For example, because the standard density measure is inversely associated with network size, large and geographically dispersed networks will typically exhibit lower levels of density. A second factor contributing to the opposing views regarding the security-efficiency tradeoff is that most studies have not fully accounted for the multi-relational nature of dark networks (Crossley et al., 2012) or have failed to outline the types of relationships under examination (Lindelauf et al., 2009). Most have focused on a single type of relation, usually communication ties, but dark network actors are embedded in a range of relationships. A final reason is that a majority of studies do not account for the environment in which these covert networks operate. Covert networks are hardly static. They not only change in response to their own operational goals but also to the strategic choices of their opponents.

In this paper we consider how the structure of dark networks can vary in response to both its own goals and the strategies adopted by authorities. It proceeds as follows. We begin by examining the strategic tradeoffs that terrorists and other insurgent groups face. These groups generally seek (or at least should seek) to balance operational efficiency and security, which we operationalize in terms of network centralization and interconnectedness, respectively. This leads to a series of hypotheses as to what we might expect as we observe a dark network over time. Next, we turn to this paper's empirical setting: namely, terrorism and insurgency in Indonesia and the strategic approaches adopted by the Indonesian authorities in their attempts to combat these dark networks. We then discuss the data and methods used

in our analysis. We then present the results, which show that the process by which dark networks adopt various network structures is far more complex than much of the current literature suggests. We conclude by discussing various limitations of our study and suggestions for future research.

Literature Review

Network Centralization

Operational efficiency is largely affected by the ability of insurgencies to mobilize people and resources (McCormick, 2005; McCormick & Owen, 2000). Some scholars suggest centralized networks are positively associated with operational efficiency (Baker & Faulkner, 1993; Morselli, 2009) and are more effective in mobilizing people and resources because they facilitate an efficient decision-making process (Enders & Jindapon, 2010), which enhances strategic planning and creates accountability and standards among network members (Tucker, 2008). They can also facilitate the transfer of resources due to shorter path lengths between leaders and other network actors (Lindelauf et al., 2009). Thus, it is not surprising that several relatively successful dark networks have been considered centralized networks built around charismatic leaders. Enders and Sandler (2006), for example, suggest that the centralized nature of Aum Shinrikyo in the 1990s facilitated its ability to successfully launch a sarin gas attack on the Tokyo subway, while the decentralized structure of Al Qaeda has reduced its ability to attain and launch a CBRN attack.¹ To be sure, many of these characterizations have been largely qualitative in nature and lack standard social network analysis measures.² Nevertheless, they do suggest that centralization is often positively associated with the command and control of dark networks.

Centralization can be a mixed blessing, however. Research suggests that less centralized organizations are able to adapt more quickly to rapidly changing environments (Arquilla, 2009) and are less vulnerable to the removal of key members (Bakker, Raab, & Milward, 2011; Sageman, 2003, 2004). Many dark networks, in particular terrorist networks, are often assumed to adopt cellular and distributed forms of network structure (Carley, Dombroski, Tsvetovat, Reminga, & Kamneva, 2003). This allows small cells to operate relatively independently with lower operational costs, which in turn allows them to more easily adjust to a rapidly changing environment than can hierarchically-structured networks (Kenney, 2007). Moreover, less centralized networks are more likely to withstand shocks, such as the capture of a key member, because much of the remaining network

goes untouched and is capable of continuing operations. However, dark networks that are too decentralized may find it difficult to mobilize resources. Moreover, they run the risk of having individuals or small cells go “rogue” and conduct operations not aligned with their operational interests. This suggests that an optimal level of centralization exists for covert networks and it is likely to change over time. One could argue that dark networks will shift toward the centralized-side of the continuum when mobilization and the transfer of resources is its primary focus (e.g., just prior to an attack). On the other hand, they are more likely to decentralize when adaptability takes precedence, such as in the aftermath of an operation. In addition, network centralization is almost certainly a function of environmental context (Everton, 2012b). In relatively friendly environments where adaptability is less crucial and the risk for losing key actors is low, covert networks will probably be more centralized. However, if the environment becomes more hostile, they will move toward the decentralized end of the spectrum. For example, anecdotal evidence suggests that prior to 9/11 al Qaeda was somewhat centralized, but after it came under attack from coalition forces, it adopted a much more decentralized organizational structure (Sageman, 2008). In any case, these factors suggest that cross sectional analyses are ill equipped to fully understand network dynamics.

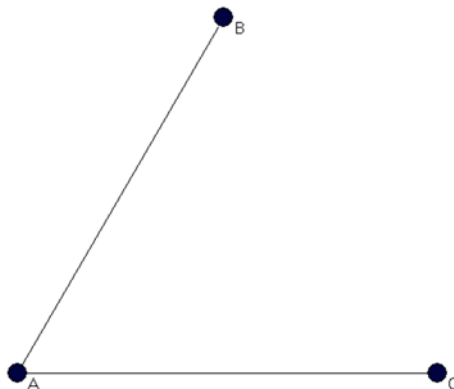
Network Innerconnectedness

There is little debate that groups recruit primarily through their social ties. For instance, Lofland and Stark’s (1965; see also, Stark, 1996) study of conversion to the Unification Church discovered that those who ultimately joined tended to be those whose ties to group members exceeded their ties to

nonmembers. Similarly, Stark and Bainbridge (1980) found that while the door-to-door efforts of Mormon missionaries were relatively unsuccessful, when missionaries met non-Mormons in the homes of Mormon friends, they enjoyed a success rate close to 50 percent. Why? Because such meetings occurred only after lay Mormons had built close personal ties with these non-Mormons and essentially brought them into their networks. A meta-analysis by Snow and his colleagues (Snow, Zurcher, & Ekland-Olson, 1980) and McAdam’s (1986; see also, McAdam & Paulsen, 1993) examination of the 1964 Freedom Summer campaign uncovered a similar dynamic: Successful social movements recruit primarily through their social ties (Snow et al., 1980, p.791). And finally, Sageman’s (2003, 2004) analysis of the global Salafi jihad (GSJ) discovered that 83% of members were recruited through friendship, kinship, or mentorship ties.

Because security is of primary concern for dark networks, they tend to recruit along lines of trust (Passy, 2003). Not doing so can be dangerous, as Ramzi Yousef, one of the 1993 World Trade Center bombers, learned the hard way. As long as he recruited through strong ties, he successfully evaded the authorities, but when he enlisted an unfamiliar South African student, his luck ran out. After Yousef asked the student to take a suspicious package to a Shiite mosque, the student called the U.S. embassy, which led to Yousef’s arrest and later extradition to the U.S (Sageman, 2004, p.109-110). Recruitment through strong ties suggests that the networks will become increasingly dense over time as ties form between previously unlinked actors. This is due to the phenomenon that Granovetter (1973) referred to as the “forbidden triad” that eventually leads to an increase in group density (Figure 1).

Figure 1: Granovetter’s Forbidden Triad



Dense networks consisting of numerous strong ties bring an important benefit to dark networks: They minimize defection because they are better able to monitor behavior (Finke & Stark, 1992, 2005; Granovetter, 2005), appropriate solidary incentives (McAdam, 1982, 1999; Smith, 1991), and solve coordination problems (Chwe, 2001). Dark networks that minimize defection are generally more successful than those that do not. In fact, they often “prefer” having members killed over having them defect because “if one activist decides to defect, the whole organization is vulnerable to the defector’s subsequent actions” (Hafez, 2004, p. 40), and they typically have to alter their plans and lie low for an unspecified amount of time (Berman, 2009, p. 29).

Security concerns not only lead members of dark networks to recruit primarily through strong ties, but they also lead them to limit their ties with outsiders because it helps minimize the presence of ideas and other countervailing influences that could challenge a group’s worldview. However, while limiting external ties can improve a group’s security, dark networks that are entirely isolated from the outside world are unlikely to sustain their movement over the long term (Jackson, Petersen, Bull, Monsen, & Richmond, 1960) because they need links to other groups in order to gain access to important information and other material and nonmaterial resources (e.g., weapons, materials, new recruits). As others have noted, external ties are vital for any group or organization attempting to survive in a rapidly changing environment (Uzzi, 1996, 2008; Uzzi & Spiro, 2005), and this is simply more acute for insurgent groups because they face not only a constantly shifting environment, but one that is hostile at that.

Hypotheses

Because dark networks seek to maintain an optimal level of centralization as well as balance between internal and external ties, we should expect such levels to vary in light of operational goals and events on the ground. Of course, some changes in network structure occur not by design but unwittingly. An important insight of social network theory is that the individual choices that actors make (e.g., forming or dissolving a tie) can sometimes cause changes in network structure of which they did not intend or are even aware (Maoz, 2011). Nevertheless, as noted above, we expect dark networks to move toward the centralized-side of the continuum when mobilization of resources is the group’s primary focus, such as just prior to an attack, but are likely to decentralize when adaptability and flexibility take precedence, such as in the aftermath

of an operation. This can be stated more formally as follows:

Hypothesis 1a: Because of the need to mobilize resources for an operation, dark networks will become more centralized just prior to an attack.

Hypothesis 1b: Because of a need to be adaptable after an operation, dark networks will seek to become less centralized after an attack.

Pre- and post-operation considerations may also affect their relative number of external ties. In particular, just prior to an operation, they may increase the number of their external ties, while after an operation, they may seek to sever them:

Hypothesis 2a: Because dark networks often need to access external resources in order to carry out operations, they will increase the relative number of their external ties prior to an attack.

Hypothesis 2b: Because immediately after an operation dark networks have less need to access to resources, they will decrease the relative number of their external ties shortly after an attack.

However, a dark network’s relative number of external ties and centralization level will not only adapt in order to meet its operational goals, but it will also adapt to its external environment, in particular the efforts of authorities to disrupt it. Counterinsurgents have a wide variety of strategies at their disposal for disrupting dark networks. Roberts and Everton (2011) have outlined a variety of strategic options available to those seeking to disrupt insurgencies and other types of dark networks. They divide strategies into two broad types: kinetic and non-kinetic. *Kinetic* strategies involve aggressive and offensive measures that seek to eliminate or capture network members and their supporters, while *non-kinetic* strategic approaches are more holistic and use a variety of non-coercive means, such as institution building, psychological operations (PsyOps), rehabilitation and reintegration programs, information operations (IO), and the tracking and monitoring of key network members (Everton, 2012a), in order to sever the ties between the local population and the insurgency, ultimately draining it of its material and nonmaterial resources. For different reasons we expect that (successful) kinetic and non-kinetic approaches lead dark networks to become increasingly isolated. Kinetic approaches accomplish this by causing the environment in which

dark networks operate to become more hostile, while non-kinetic approaches do so by cutting dark networks off from the local population:

Hypothesis 3a: Because kinetic operations create a hostile environment, dark networks will become increasingly isolated in response to kinetic operations.

Hypothesis 3b: Because non-kinetic operations seek to sever ties between dark networks and the local population, dark networks will become increasingly isolated in response to non-kinetic operations.

It is less clear what effect kinetic and non-kinetic operations will have on the centralization level of dark networks, so at this time we offer no hypotheses regarding the effectiveness of each strategy, nor is it clear what is desirable. On the one hand, causing dark networks to become increasingly centralized may allow them to mobilize resources, but at the same time it will increase their vulnerability to targeted attacks. On the other, causing dark networks to become less centralized may diminish their ability to carry out attacks, but at the same time, it will make them more difficult to monitor and disrupt. We now turn to a brief overview of Indonesian militancy, which serves as the empirical setting for testing these hypotheses.

Empirical Setting: Indonesia

In the early 1950s, a series of rebellions against the newly independent Indonesian state began in several parts of the country (Conboy, 2006, p. 5). The establishment of an Islamic state, along with other motivations such as socio-economic reform, brought many of these rebellions together under the movement known as Darul Islam (DI), which was led by Soekarmadji Maridjan Kartosoewirjo until his capture in 1962. The movement subsequently faced many challenges through the 1960s, such as numerous defections, a leadership vacuum, and contentious debates regarding strategy, all of which inspired several efforts to reestablish a more cohesive movement in the 1970s and in the 1980s. The most well-known product of these efforts, Komando Jihad (KJ), consisted of several members of the old DI-guard; it aimed to re-launch a revolution against the state despite its complicated relationship with the newly established Suharto regime (Conboy, 2006).

DI's influence and its early offshoots on today's militant groups in Indonesia cannot be understated. Almost every jihadist organization in the country since the 1950s has its roots in DI, including the

majority of groups active over the last decade, such as Jemaah Islamiyah (JI) and Noordin Top's network. Its influence, according to the International Crisis Group's Sidney Jones (2009), stems from a host of factors, such as personal and kinship relations that stretch across generations and are deeply embedded in militant circles today, its employment of tactics such as the use of Fa'i,³ its strategy of developing a secure area of operation from which it could fight the state,⁴ and its leadership and involvement in conflicts, such as the Soviet-Afghan War (1979-1989), the communal conflict in Ambon and Poso, and the conflict on the island of Mindanao in the southern Philippines, which helped establish ties among militant organizations within Indonesia and across the region.

The group from the DI-genealogy receiving the most attention since September 11th has been JI. Originally formed as a breakaway faction of DI, it has its roots in the Soviet war in Afghanistan. The organization's founders, Abdullah Sungkar and Abu Bakar Ba'asyir, were prominent members of DI and among the first to send Indonesian fighters to Camp Sadda in Pakistan around 1985, where many future JI leaders learned skills they would eventually bring back with them. The organization, which was formally established in 1993, initially aimed to create an Indonesian Islamic state, a goal that was eventually expanded into the establishment of a regional caliphate. JI grew increasingly violent through its support and participation in Indonesian communal conflicts in late-1990s and early-2000s. It is best known for the October 2002 Bali bombings that resulted in 202 deaths and attracted headlines across the globe. Indonesian authorities severely cracked down on JI in the aftermath of the bombings and many of its key leaders were detained or killed.

All this appears to have created a leadership vacuum into which Noordin Mohammed Top stepped. A member of JI, Noordin began to sever his ties from JI in 2003 after he acquired explosives leftover from the 2000 Christmas Eve bombings (Everton & Cunningham, 2012). Along with a core set of JI members, he used his newly acquired resources for his nascent network's first operation: the 2003 JW Marriott attack. For the next two years his network, which would go by several names, launched several successful attacks against "Western targets" in Indonesia. He drew from a deeply embedded network of actors, many of whom were DI members or members of its offshoots, in order to continue operating in the face of increased counter-terrorism operations. His success eventually landed him on the FBI's Seeking Information-War on Terrorism List in 2006. After a three-year lull in attacks, he and his associates carried out

simultaneous bombings against the Ritz-Carlton and Marriott hotels in August 2009. These bombings led to further stepped-up police operations and his subsequent demise in the following month. Not long after Noordin and a few of his key associates were killed, his network essentially disintegrated (Everton & Cunningham, 2013).

Noordin's death should not be seen as an absence of a terrorist threat in Indonesia. In 2010, for example, a group of jihadists unsuccessfully tried to establish a safe haven in Aceh to launch attacks and to establish an Islamic state in the country (International Crisis Group, 2010). Moreover, a group established by Abu Bakar Ba'asyir in 2008, Jemaah Ansharut Tauhid (JAT), has joined JI as a powerhouse organization in Indonesia. In fact, many JI members and former Noordin associates joined JAT after its creation. The organization seeks the establishment of an Islamic state and largely operates above-ground; however, several of its members were implicated for participating in Noordin's 2009 attack, for providing recruits for small-scale operations in the country, and for being directly involved in the 2010 Aceh project. Finally, it appears smaller groups of less experienced actors, often with the support of JI and JAT, have emerged as a serious terrorist threat in Indonesia although they have largely focused on carrying out local attacks against law enforcement (International Crisis Group, 2011).

Indonesian authorities have responded to the rise of Islamic militancy in two primary ways, which provide us with something of a natural experiment for testing the effect that strategies have on a network: One was the formation of *Detachment 88* (Det 88), the Indonesian counter-terrorism squad; the other was the establishment of the *Jakarta Centre for Law Enforcement Cooperation* (JCLEC), a joint initiative between the Indonesian and Australian governments. Det 88 was formed in July 2003 shortly after the first Bali bombing and is funded, equipped, and trained by the United States and Australia. Since its inception, it has achieved several notable successes, including the arrest or killing of hundreds of terrorist suspects, including Azhari Husin, Noordin Top's close associate and primary bomb-maker, and Noordin Top himself in late-2009. However, Det 88's tactics have increasingly come under attack from several influential Indonesian and international organizations for purportedly adopting a "shoot first" mentality and for possible human rights violations, such as the torture of suspected terrorists (Priamarizki, 2013; Roberts, 2013; "Elite Indonesian Police Unit," 2013). The elite squad has reportedly killed 50 terrorism suspects since 2010, which has only further contributed to domestic and international skepticism regarding their rules of engagement.

Indeed, it appears that Det 88 may have adopted the coercive practices of earlier Indonesian counterinsurgency efforts by the military, which were successful against DI in the 1950s but were misapplied in later counterinsurgency efforts (Kilcullen, 2010).

Det 88 is in stark contrast with what is taught at the JCLEC, which was founded in 2004 and located in Semarang, Indonesia, and seeks to be a resource for Southeast Asian governments combatting transnational crime and terrorism. It provides a forum for academics and other experts to examine the Southeast Asian situation, as well as allow practitioners to keep up to date with the latest developments on combatting terrorism and transnational crime (Solomon, 2007). To this end, it offers a wide-range of training programs, seminars, and workshops on topics such as money laundering, human trafficking, cyber-crime, computer forensics, crisis negotiation, informant handling and interviewing techniques, organized crime, and Islamic law and politics (Jakarta Centre for Law Enforcement Cooperation, 2005-2010). The center also works closely with regional law enforcement agencies that are looking to enhance their enforcement capacity and approach (Ramakrishna, 2009). In short, it seeks to offer a more holistic approach to combatting the Indonesian terrorist threat, which is sorely needed in Indonesia (International Crisis Group, 2012).

Data and Methods

The Noordin Top network serves as the case study for exploring the relationships among dark network structure, resilience, and counter-terrorism strategies over time. His network, arguably more so than any other organization operating within Indonesia over the last few decades, demonstrated a remarkable ability to withstand both endogenous and exogenous shocks. We utilized relational data drawn from two International Crisis Group (ICG) reports: "Terrorism in Indonesia: Noordin's Networks" (2006) and "Indonesia: Noordin Top's Support Base" (2009). We supplement these with open source data in order to generate time codes by month from January 2001 through December 2010, which allows us to account for when actors entered the network and if and when individuals were arrested or killed. The 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 five networks from several subnetworks each containing 237 individuals. Specifically, we

created a *trust network*, which is an aggregation of one-mode classmate, friendship, kinship, and co-religious subnetworks.⁵ We constructed a second network, which we call the *operational network*, from four one-mode networks that were derived from corresponding two-mode networks, namely logistics, meetings, operations, and training events. Our third network is a one-mode *communication network*, which captures the pattern of communications between Noordin's network members. The fourth is Noordin's *business and finance network*, a one-mode network that was derived from a two-mode network indicating the business and financial affiliations of the members of Noordin's network.⁶ Finally, we created a *combined network*, which, as its name implies, combines the *trust*, *operational*, *communication*, and *business and finance networks* in order to obtain an overall picture of Noordin's network. We consider all but the business and finance network in the descriptive portion of our analysis below,⁷ but focus only on the combined network for the confirmatory analysis portion.⁸

In order to analyze these networks longitudinally, we assigned time codes to each actor in the network that indicated when they entered and left Noordin's *combined network*. In assigning these 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.

Our dependent variables are various measures capturing the centralization and connectedness of Noordin's network over time. Social network analysis calculates network centralization based on variation in actor centrality (Wasserman & Faust, 1994). More variation yields higher network centralization scores; less variation yields lower scores. Because the standard centralization score (Freeman, 1979) estimates variation by comparing each actor's score to the score of the network's most central actor, the larger the centralization index, the more likely it is that a single actor is central (Wasserman & Faust, 1994, p. 176). An alternative measure recommended by Coleman (1964), Hoivik and Gleditsch (1975), and Snijders (1981) is variance

of actor centrality scores found in the network. It compares each actor's score to the average score, which means that the larger the centralization index, the more likely that a group of actors (rather than a single actor) are central. A similar measure, standard deviation, also uses the average score of all actors but is preferable to variance because it returns us to the original unit of measure. In our analysis below, we use both standard centralization and standard deviation scores, both of which can be calculated for any measure of centrality. We include two measures of centralization in this paper: degree and betweenness. Because degree centrality counts the number of ties of each individual actor, centralization measures based on degree capture the extent to which one or a handful of actors possess numerous ties while others do not. By contrast, because betweenness centrality estimates the extent to which actors in a position to control the flow of resources through a network, centralization measures based on betweenness indicate the level to which one or a handful of actors are in a position to broker the flow of resources in a network.

Multiple measures are available for measuring a network's innerconnectedness with density and average degree being the most common. As noted above, however, the standard density measure is problematic because it is inversely associated with network size, and while this limitation can be corrected by using average degree centrality (de Nooy, Mrvar, & Batagelj, 2011; Scott, 2000), if a network adopts a cell-like structure, it can be locally dense but globally sparse. We sidestep these issues by comparing the network's external connectedness with its internal connectedness, using Krackhardt's (1994) E-I Index, which measures the ratio of ties a group has to non-group members to group members:

$$\frac{E - I}{E + I} \quad (1)$$

where E equals the number of external ties and I equals the number of internal ties. Thus, if a group has all external ties, the index equals 1.0; if it has all internal ties, the index equals -1.0; and if there are an equal number of internal and external ties, the index equals 0.0. We expect a dark network's E-I index to be less than those of light networks, all else being equal. Indeed, we expect it to always be negative. Of course, here we do not compare a dark with a light network but instead examine a particular dark network over time. Thus, we expect its E-I index to become increasingly negative as pressure is brought to bear on the network.

We include two variables in order to capture the various strategies adopted by Indonesian authorities during the period under analysis: (1) one that measures the formation and continued existence of Det 88, and (2) one that measures the formation and continued existence of the JCLEC. Although Det 88 was formed in July 2003, it did not reach its operational capacity of 400 members until mid-2005; thus, we include a variable that grows at a rate of 16 members a month, beginning in July of 2003 until reaching 400 members in July of 2005. We rescaled the variable by dividing it by 100 in order to make interpreting the coefficients easier. The JCLEC was established in July 2004, but it took time for it to offer courses that attracted large numbers of students. Thus, drawing on course attendance data included in the JCLEC's annual reports (Jakarta Centre for Law Enforcement Cooperation, 2005-2010), we created a variable that reflects the average number of students who attended JCLEC courses in the previous six months. In other words, although the center was established in July of 2004, the six-month moving average for that month was zero since no students attended a JCLEC course in the previous six months. However, because 49 students attended a course in July of 2004, the six-month moving average for August 2004 equaled 8.167. As we did with the Det 88 variable, we divided the moving average by 100 in order to make the variable's effects easier to interpret.

Examining network structure over time requires the inclusion of variables to account for important temporal and event effects. The model includes two variables to control for the curvilinear effect that time appears to have on the various centralization variables (but not the EI Index – see Figures 3 through 7): we have included both a *month* and a *month-squared* variable. For the EI index, we only included a *month* variable. Four additional variables control for critical events and periods. A dummy variable 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. An additional dummy variable measures the effect of Noordin's ability to acquire surplus explosives from the 2000 Christmas Eve Bombings in Indonesia. This *explosives* variable covers the time from which Noordin obtained the explosives in December 2002 to the time in which they were used for the network's first attack in August 2003. We also have included a series of *pre and post-operation* dummy variables that capture the three-month period immediately preceding and 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. Because Noordin's

network was only directly involved in the bombings after the first Bali bombing, the pre and post operation dummy variables for all but the first Bali bombing are combined into one pre-operation variable and one post-operation variable, while the pre and post operation variables for the first Bali bombing are included separately.

In order to tease out how the Noordin Top terrorist network adapted and changed from 2001 to 2010 in reaction to endogenous and exogenous factors, our analysis includes both descriptive methods and ordinary least squares (OLS) multivariate regression. Because social network assumptions differ from those of standard OLS approaches, we use bootstrapping methods to estimate standard errors, an approach commonly used with social network data (Borgatti, Everett, & Freeman, 2002; Prell, 2011).

Results

Figures 2 through 6 below present graphs of the centralization and E-I Index scores for Noordin's alive and free trust, operational, communication, and combined networks. Specifically, the figures graph the centralization (degree and betweenness), normalized standard deviation (degree and betweenness), and E-I index for each of the various networks. Moving from left to right the vertical dark gray lines indicate key points in the life cycle of Noordin's network: 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). Comparing the degree centralization (Figure 2) and degree standard deviation (Figure 3) scores of the network yields some interesting insights. It appears that in terms of degree centralization, the network grew increasingly centralized early in its existence, and then after a slight dip in 2004, remained relatively constant, at least up until the point that Noordin was killed. This was not the case in terms of degree standard deviation, however. It appears there is a quick run up in centralization early in the network's career, but then it drops back to where it began before climbing slightly in late-2006. The network then shifts back to a downward trend until around early-2007, recovers slightly, and then remains relatively constant until Noordin's death in 2009. The comparison of these two sets of graphs suggests that while Noordin formed and maintained numerous ties to group members, thus driving up degree centralization (Figure 2), his inner circle did not, which could explain why except for the jump in

2004, degree standard deviation remained relatively stable over the time period under examination (Figure 3). The coefficients for the time variable included in Table 1 below (“month”) are consistent with these results. In particular, the coefficient for standard (i.e., Freeman) degree centralization is positive and statistically significant, indicating that after

controlling for other factors, degree centralization increased over time. By contrast, the coefficient for standard deviation is negative but statistically insignificant, suggesting that after controlling for other factors, degree standard deviation remained relatively constant from 2001 to 2010.

Figure 2: Degree Centralization of Alive and Free Noordin Top Network

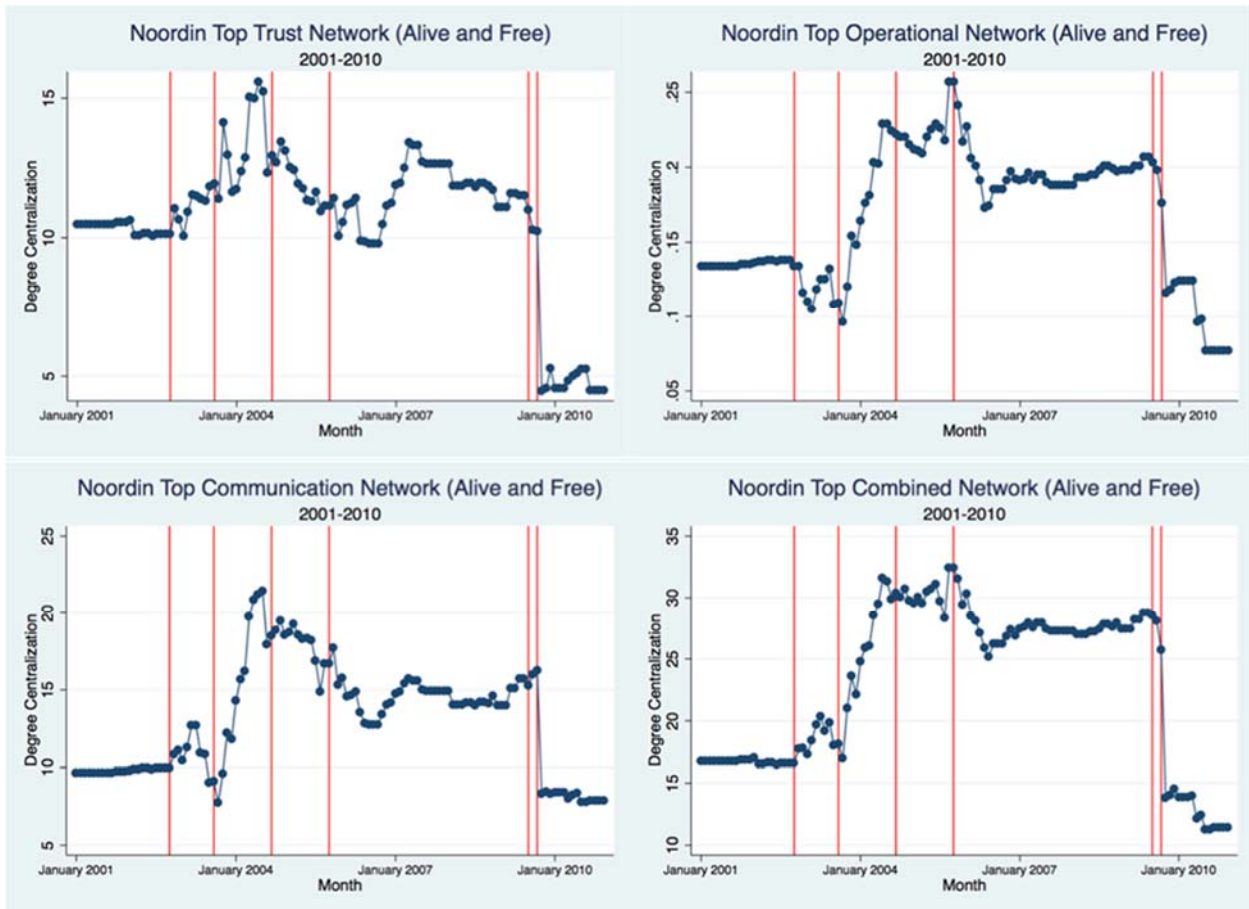
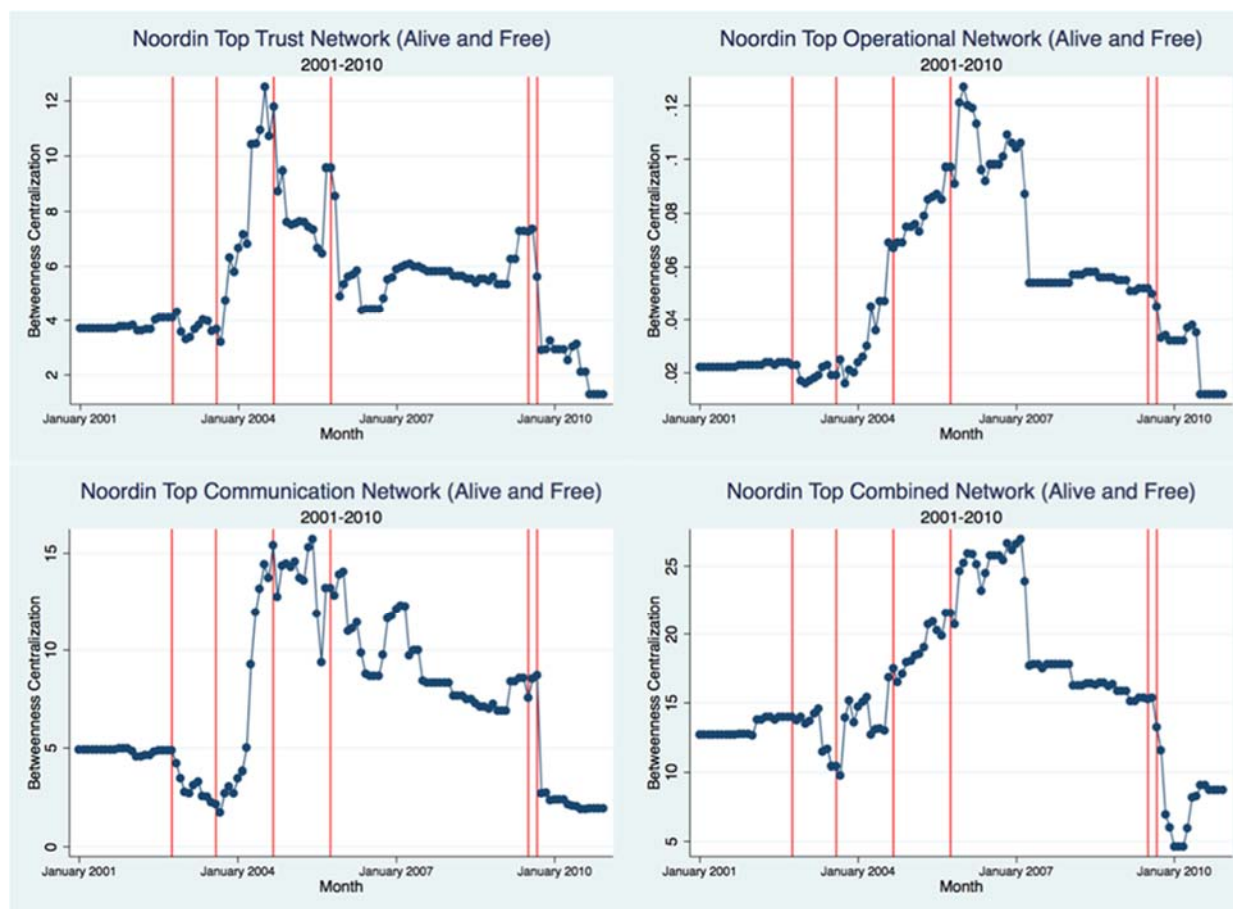


Figure 3: Degree Standard Deviation of Alive and Free Noordin Top Network



We do not see a similar relationship between betweenness centralization (Figure 4) and betweenness standard deviation (Figure 5). Here the two sets of scores display similar patterns, suggesting that both Noordin and his key operatives located themselves in brokerage positions within the network. The coefficients for the time variable

included in Table 1 below are consistent with these results as well. The coefficients for both betweenness centralization and betweenness standard deviation are positive and statistically significant, suggesting that after controlling for other factors both increased over the time period under investigation.

Figure 4: Degree Centralization of Alive and Free Noordin Top Network

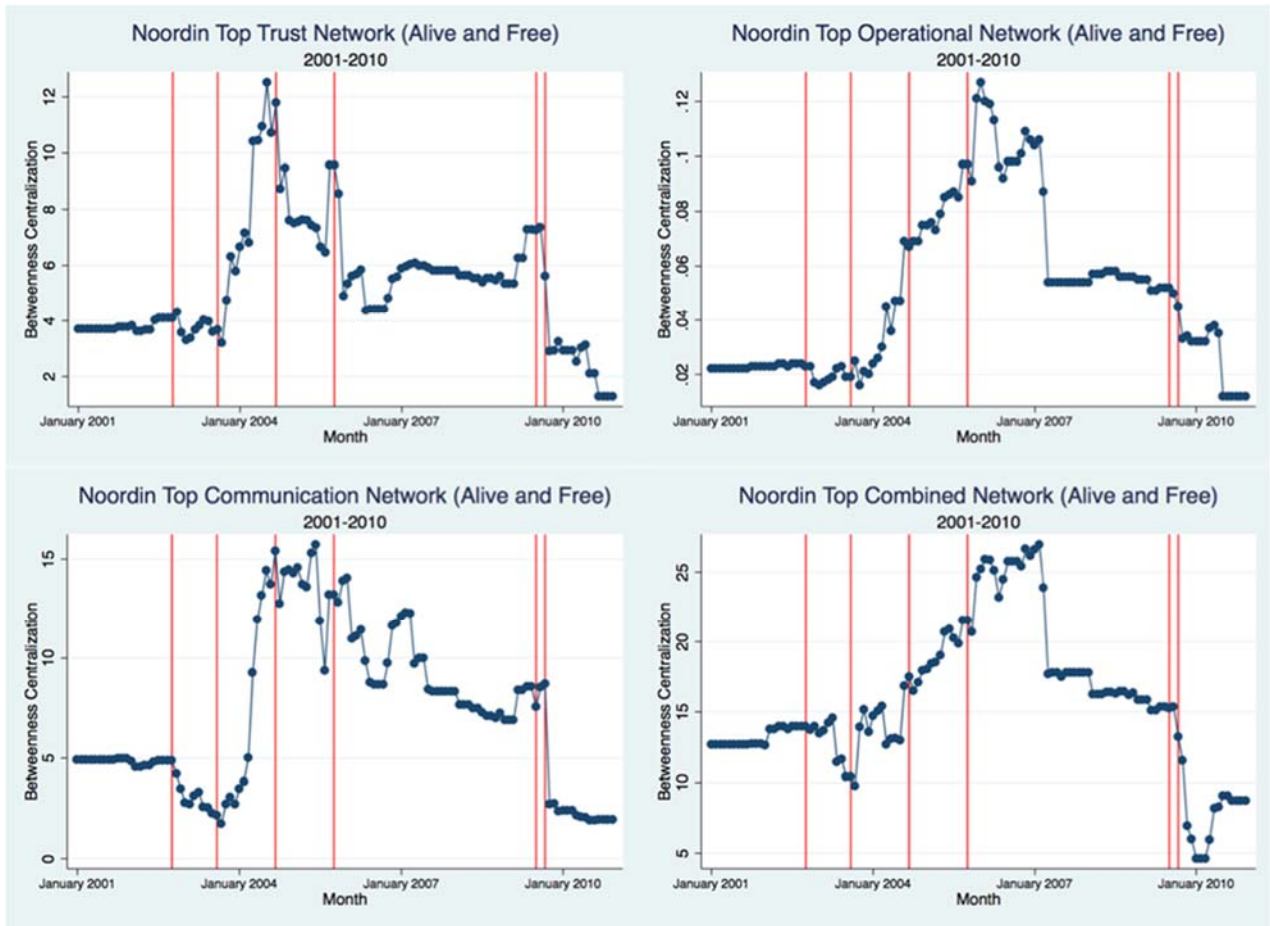
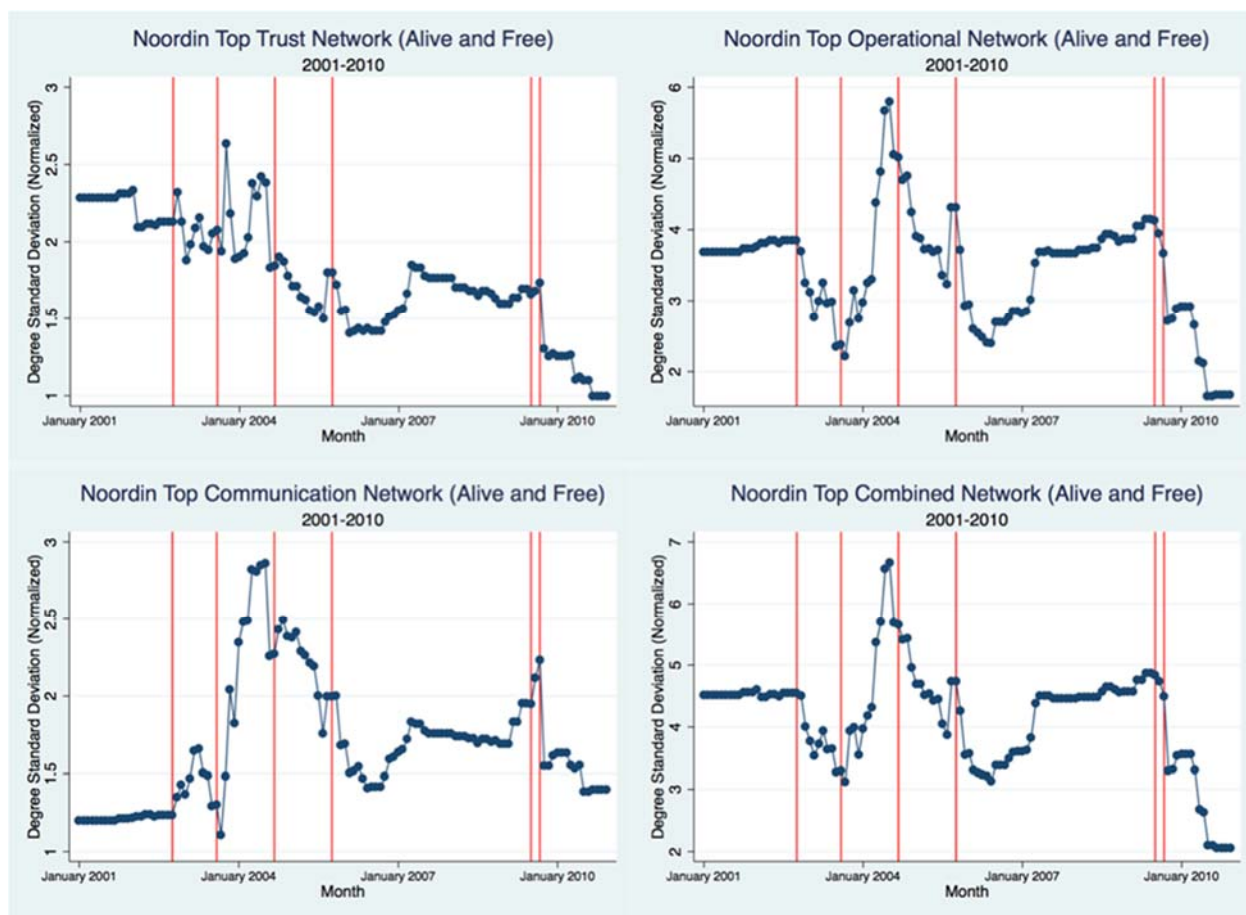


Figure 5: Betweenness Standard Deviation of Alive and Free Noordin Top Network



The E-I Index (Figure 6) shows that the combined network became increasingly inward for most of the period under consideration. Indeed, the network exhibited a pattern of establishing external ties prior to most of the Noordin-led attacks, excluding the 2005 Bali bombings. This trend likely reflects a need for information or other types of resources such as bomb-making materials and money. On the other hand, the network also turned increasingly inward, again with the exception of the

2005 attacks, following the Noordin-led attacks. These changes prior to and after the majority of the attacks highlight that network cohesion is likely to change immediately before and after an attack. What is especially interesting is how just before the July 2009 attacks, Noordin began forming ties to actors outside of his immediate circle because it raises the possibility that Noordin may have been careless in forming these ties, which may have contributed to his death two months after the July attacks.

Figure 6: E-I Index of Alive and Free Noordin Top Network

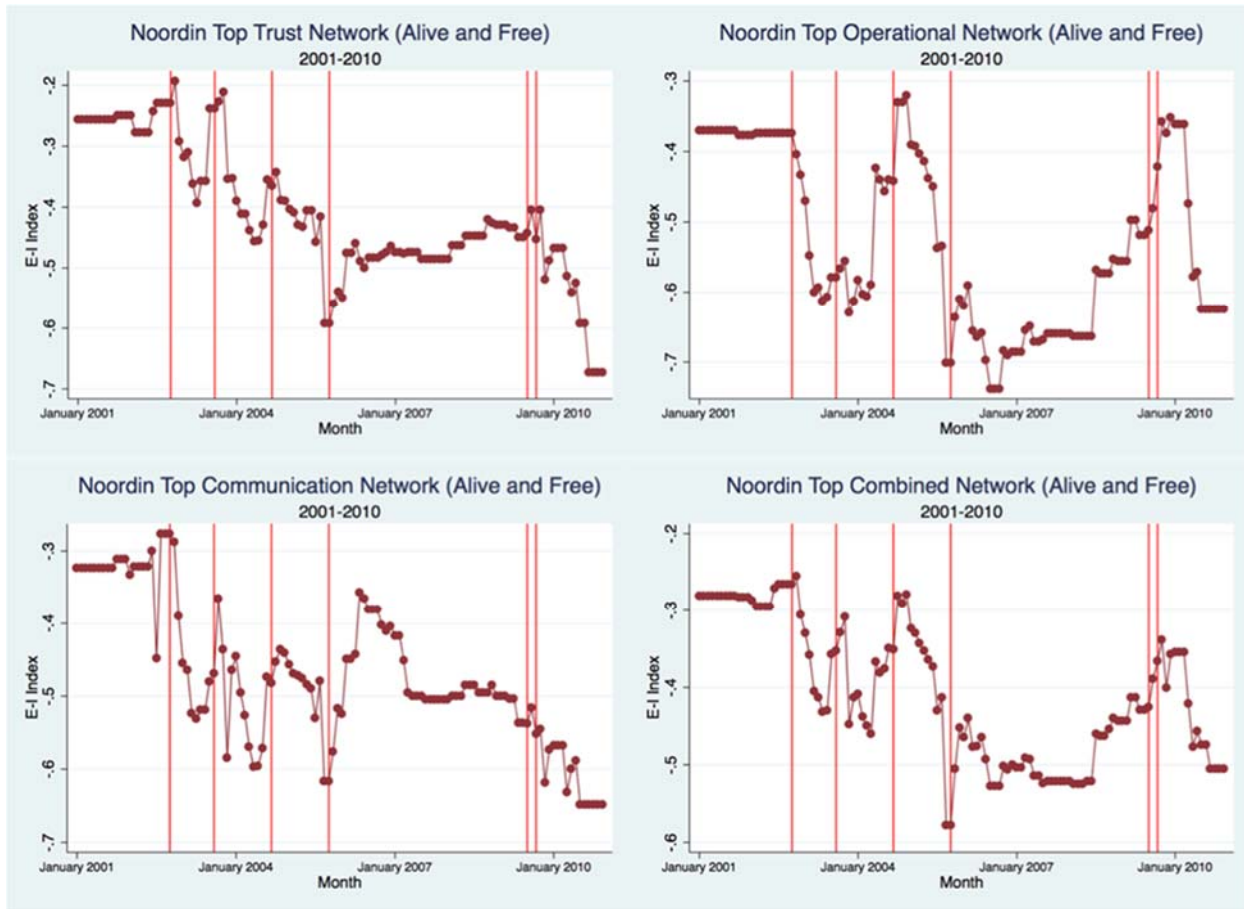


Table 1 displays the results of our multivariate regression analysis. The tables contain models with and without the *month* and *month squared* variables due to high collinearity between the two time variables. Because our table contains five dependent variables for both sets of models, along with ten independent variables for the models with the *month* and *month squared* variables and eight independent variables for those without, it is impossible to discuss all of the nearly 100 coefficients. Thus, our comments will tend to focus on the models *without*

the two month variables and we will concentrate on overall patterns and focus on those coefficients that are both substantively and statistically significant (McCloskey, 1995; Ziliak & McCloskey, 2008). The table presents many interesting findings. For example, the adjusted R² for all of the models are extremely high and indicate that they account for a substantial amount of the variation in the dependent variables, as well as provide a sense of confidence that our models adequately explain the variability in our dependent variables.⁹

Table 1. Multivariate Regression Results for Noordin Top Combined Network (Alive and Free)

	Degree			Centralization			Betweenness			EI Index
	Freeman	Std. Deviation	Freeman	Std. Deviation	Freeman	Std. Deviation	Freeman	Std. Deviation		
Intercept	17.821***	4.523***	44.611	12.504***	-339.603**	1.341***	-39.538***	-0.302***	12.626***	
Detachment 88	3.651***	-0.029	-0.107	2.354***	3.212***	0.151***	0.123***	-0.032***	0.006	
JCLEC	-4.802***	-0.221	-1.050***	-2.474**	5.476***	-0.028	0.480***	-0.052*	-0.111***	
Month	1.687***		-0.164		1.462***		0.158***		-0.047***	
Month2	-0.001***		0.000		-0.002***		-0.000***		0.000***	
Pre Bali I (2002)	-1.241***	0.018	-0.001	1.456***	1.700***	0.031	-0.014	0.036***	0.068***	
Post Bali I (2002)	-0.357	0.188	0.160	1.341***	1.656**	0.038	0.010	0.056**	0.080***	
Explosives	-0.311	-1.090***	-1.135***	0.083	0.678	0.003	-0.067	-0.089***	-0.033	
Pre Ops	1.934**	0.443*	0.307	-1.930*	-0.658	-0.174***	-0.098*	0.032*	0.025*	
Post Ops	1.551**	0.113	0.111	-0.197	-0.203	-0.038	-0.056	0.071***	0.076***	
Key Deaths	-11.922***	-1.319***	-1.864***	-9.999***	-4.648***	-0.639***	-0.269**	-0.066**	0.018	
Observations	118	117	117	117	117	116	116	115	115	
AIC	468.354	187.350	169.283	588.325	502.130	-51.878	-111.474	-376.270	-396.953	
BIC	490.519	209.447	199.667	610.423	532.514	-29.849	-81.184	-354.311	-366.759	
Adjusted R2	92.77	54.24	62.04	65.62	84.07	67.48	81.17	73.68	78.73	

Note: Coefficients are unstandardized; bootstrap standard errors used to estimate significance

* p < .05

** p < .01

*** p < .001 (two-tailed)

Looking at the pre-operational and the post-operational behavior of the network, the network did become increasingly centralized prior to an attack in terms of the degree centralization measures but not in terms of the betweenness centralization measures, lending some support for hypothesis 1a. Given that the former measures capture the extent to which a network is centered around actors who possess numerous ties, while latter measures capture the extent to which it is centered around actors who are in positions of brokerage, this result suggests centralization occurs on some dimensions prior to an attack but not on others. Interestingly, the network did not decentralize like we predicted it would after attacks (Hypothesis 1b).¹⁰ In fact, it appears to have continued to centralize in the aftermath of its attacks. This may indicate that Noordin was incapable of adopting a less centralized and flexible structure immediately after an attack, which probably left his network vulnerable during those periods.

Interestingly, the network did drift toward the external side of the E-I spectrum before attacks, which lends support Hypothesis 2a. His network followed the same behavior after attacks as well (Hypotheses 2b), which may have contributed to him being killed. Interestingly, the *Post Bali I* coefficient shows a similar result. That the Bali I network was essentially destroyed in the aftermath of the attack suggests that increasing external ties in a hostile environment could lead to disastrous results. An alternative explanation is that the apparent inability for Noordin to decentralize his network or halt the drift toward more external ties simply reflects an artifact of the way our data are coded. As noted above, we assumed that a tie continued to exist once it was formed, which means that we may not have captured whether some ties were severed (or at least went dormant) after an attack.

As predicted (Hypotheses 3a and 3b) it appears that both Det 88 and the JCLEC caused Noordin's network to become increasingly isolated as indicated by the E-I Index column in Table 1. The results indicate that they contributed to the network's inward looking behavior, which suggests that the network felt the pressure being exerted by the two groups and consequently attempted to increase its security by focusing on establishing and maintaining internal ties while limiting external ones. While isolating an insurgency is generally a counterinsurgency goal, it can also lead to an increase in a group's radicalism (Sunstein, 2009). However, in this case, it appears that Noordin and his followers were already highly radicalized (Griswold, 2010).

The two groups appear to have affected the network's centralization in different ways, however. Det 88 seems to have pushed it to become

increasingly centralized, thereby increasing Noordin's command and control. However, by causing it to become more centralized, it led it to become more and more vulnerable to decapitation-like strategies, which, as we already noted, is exactly what befell Noordin's network. After Noordin and a few of his key associates were killed in the Fall of 2009, the network essentially fell apart. The JCLEC's effect on the network's centralization is less clear. If we focus only on the models that do not include the two time variables, then it appears that the JCLEC's efforts caused the network to become less centralized. This suggests that the JCLEC not only caused Noordin to attempt to limit his personal ties in order to reduce visibility but also to limit his role as a broker in order to create a relatively more flexible structure in terms of the brokerage of resources. Thus, the JCLEC may have helped to reduce Noordin's command and control capabilities, but at the same time, it may have allowed the network to adopt a more flexible structure. The fact that the sign of the JCLEC coefficient flips in terms of the betweenness centralization measures when the time variables are included in the models raises the possibility that while the pressure brought to bear by the JCLEC did lead Noordin to reduce his visibility, it did not lead him to relinquish his position of brokerage.

Discussion and Conclusion

This article has explored the topic of dark network resilience by simultaneously considering the strategic tradeoffs that both dark networks and counter-insurgents face. It demonstrates that both sets of tradeoffs help shape a dark network's structure, which in part affects its resiliency. As it was shown, a dark network's adoption of a network structure is far more complex than what current literature suggests, namely that a network structure at either side of the cohesion and centralization continuums offers potential advantages and disadvantages in terms of network resilience. In the case of Noordin Top, it appears that his network's focus on establishing external ties after its operations provided it possible access to resources but likely became a factor contributing to its exposure and eventual disruption. The network, much like its Bali I predecessors who also focused on establishing external ties after their operation, faced significant losses and needed to reconstitute itself immediately following each operation. This tendency, along with the general adoption of a centralized structure, suggests that Noordin's network adopted a suboptimal structure that ultimately contributed to his demise.

Similarly, the two somewhat contrasting strategic approaches (Det 88 and JCLEC) both appear to have played critical roles in disrupting the network by isolating it from the population. Together, these approaches appear to have placed significant pressure on the network by forcing it to turn inward only until it exposed itself when it needed resources and may have contributed to the network's downfall. At the same time, they potentially provided some short-term advantages for the network. The JCLEC, for example, appears to have reduced Noordin's command and control by making it less centralized; however, it may have improved the network's resiliency by possibly making it more difficult to monitor. Certainly, it is unlikely that the effect of these strategies will be uniform across the various Noordin network aggregations. For example, Noordin's communication network adopted a very different structure than the combined network and the effects of our independent variables on each aggregation (trust, operations, business and finance, etc.) are unclear at this point. Only after further analysis can we tease out how these strategies affected each network.

Clearly, more work is needed with regards to the security-efficiency tradeoff in terms of dark network resilience. One limitation of this analysis was the inability to tease out specific policies and sub-strategies employed by Det 88 and the JCLEC against Noordin's network. For instance, it is highly likely that Det 88 used alternative strategies against its targets, such as PSYOPs, but open-source data are limited in this regard. Future studies should continue to test various strategic options employed against dark networks and how they affect a network's structure over time. An examination of these strategies to various network aggregations, much like the descriptive analysis in this paper, will certainly benefit the field. A second challenge facing this study, which is one many longitudinal studies of dark networks face, is it did not fully account for the endogenous effects and other internal processes that shaped Noordin's network over time. For example, it is highly possible that some of the network's trends toward internal density and greater centralization across time were due to Noordin's personality and decision-making processes. Finally, one should not assume that the behavior of the Noordin Top terrorist network characterizes the behavior of all terrorist networks, let alone all dark networks. The results here simply suggest that it is desirable to see further inquiry into the security-efficiency tradeoff regarding network resilience within other contexts and that future studies should consider both the counter-insurgent and the dark network's strategic point of view. Not only would these studies help researchers

better understand dark network resilience, but they would also aid in the monitoring, disruption, and destabilization of dark networks.

References

- Arquilla, J. (2009). *Aspects of Netwar & the conflict with al Qaeda*. Monterey, CA: Information Operations Center, Naval Postgraduate School.
- Baker, W. E. & Faulkner, R. R. (1993). The social-organization of conspiracy: Illegal networks in the heavy electrical-equipment industry. *American Sociological Review*, 58(6), 837–860. doi:10.2307/2095954
- Bakker, R. M., Raab, J., & Milward, H. B. (2011). A preliminary theory of dark network resilience. *Journal of Policy Analysis and Management*, 31(1), 33–62. doi:10.1002/pam.20619
- Berman, E. (2009). *Radical, religious, and violent: The new economics of terrorism*. Cambridge, MA: The MIT Press.
- Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *UCINET for Windows: Software for social network analysis*. Harvard, MA: Analytical Technologies.
- Carley, K. M., Dombroski, M., Tsvetovat, M., Reminga, J., & Kamneva, N. (2003). *Destabilizing terrorist networks*. Paper presented at the 8th International Command and Control Research and Technology Symposium, National Defense War College, Washington DC.
- Chwe, M. S. (2001). *Rational ritual: Culture, coordination, and common knowledge*. Princeton, NJ: Princeton University Press.
- Coleman, J. S. (1964). *Introduction to Mathematical Sociology*. New York, NY: Free Press.
- Coleman, J. S. (1988). Free riders and zealots: The role of social networks. *Sociological Theory*, 6(1), 52–57. doi:10.2307/201913
- Combating Terrorism Center. (2006). *Harmony and disharmony: Exploiting al-Qaida's organizational vulnerabilities* (pp. 55). West Point, NY: Combating Terrorism Center at West Point.
- Conboy, K. (2006). *The second front*. Jakarta, Indonesia: Equinox Press.
- Crossley, N., Edwards, G., Harries, E., & Stevenson, R. (2012). Covert social movement networks and the secrecy-efficiency trade off: The case of the UK suffragettes (1906–1914). *Social Networks*, 34, 634–644. doi:10.1016/j.socnet.2012.07.004

- de Nooy, W., Mrvar, A., & Batagelj, V. (2011). *Exploratory social network analysis with Pajek* (Revised and expanded ed.). Cambridge, UK: Cambridge University Press.
- Elite Indonesian police unity under fire over torture, unlawful killings (2013, March 30). *South China Morning Post: Asia*. Retrieved from <http://www.scmp.com/news/asia/article/1202787/elite-indonesian-police-unit-under-fire-over-torture-unlawful-killings>
- Enders, W., & Jindapon, P. (2010). Network externalities and the structure of terror networks. *Journal of Conflict Resolution*, 54(2), 262–280. doi:10.1177/0022002709355439
- Enders, W., & Sandler, T. (2006). *The political economy of terrorism*. Cambridge, UK: Cambridge University Press.
- Enders, W., & Su, X. (2007). Rational terrorists and optimal network structure. *Journal of Conflict Resolution*, 51(1), 33–57. doi:10.1177/0022002706296155
- Erickson, B. (1981). Secret societies and social structure. *Social Forces*, 60(1), 188–210. doi:10.1093/sf/60.1.188
- Everton, S. F. (2012a). *Disrupting dark networks*. Cambridge, UK: Cambridge University Press.
- Everton, S. F. (2012b). Network topography, key players and terrorist networks. *Connections*, 31(1), 12–19.
- Everton, S. F., & Cunningham, D. (2012). Detecting significant changes in dark networks. *Behavioral Sciences of Terrorism and Political Aggression*, 5(2), 94–114. doi:10.1080/19434472.2012.725225
- Everton, S. F., & Cunningham, D. (2013). Terrorist network adaptation to a changing environment. In C. Morselli (Ed.), *Crime and Networks* (pp. 287–308). London, UK: Routledge.
- Finke, R., & Stark, R. (1992). *The churching of America, 1776–1990: Winners and losers in our religious economy*. New Brunswick, NJ: Rutgers University Press.
- Finke, R., & Stark, R. (2005). *The churching of America, 1776–2005: Winners and losers in our religious economy* (2nd ed.). New Brunswick, NJ: Rutgers University Press.
- Freeman, L. C. (1979). Centrality in social networks I: Conceptual clarification. *Social Networks*, 1, 215–239. doi:10.1016/0378-8733(78)90021-7
- Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology*, 73(6), 1360–1380. doi:10.2307/2776392
- Granovetter, M. (2005). The impact of social structure on economic outcomes. *Journal of Economic Perspectives*, 19(1), 33–50. doi:10.1257/0895330053147958
- Griswold, E. (2010). *The tenth parallel: Dispatches from the fault line between Christianity and Islam*. New York, NY: Farrar, Straus, and Giroux.
- Hafez, M. M. (2004). From marginalization to massacres: A political process explanation of violence in Algeria. In Q. Wiktorowicz (Ed.), *Islamic activism: A social movement theory approach* (pp. 37–60). Bloomington, IN: Indiana University Press.
- Hoivik, T., & Gleditsch, N. P. (1975). Structural parameters of graphs: A theoretical investigation. In H. M. Blalock (Ed.), *Quantitative sociology* (pp. 203–222). New York: Academic Press. doi:10.1007/BF00192487
- International Crisis Group. (2006). *Terrorism in Indonesia: Noordin's networks* (Asia Report No. 114). Retrieved from http://www.crisisgroup.org/~media/Files/asia/south-east-asia/indonesia/114_terrorism_in_indonesia_noordin_s_networks
- International Crisis Group. (2009). *Indonesia: Noordin Top's support base* (Asia Briefing No. 95). Retrieved from http://www.crisisgroup.org/~media/Files/asia/south-east-asia/indonesia/b95_indonesia_noordin_tops_support_base.pdf
- International Crisis Group. (2010). *Indonesia: Jihadi surprise in Aceh* (Asia Report No. 189). Retrieved from <http://www.crisisgroup.org/~media/Files/asia/south-east-asia/indonesia/189%20Indonesia%20-%20Jihadi%20Surprise%20in%20Aceh.pdf>
- International Crisis Group. (2011). *Indonesian jihadism: Small groups, big plans* (Asia Report No. 204). Retrieved from <http://www.crisisgroup.org/~media/Files/asia/south-east-asia/indonesia/204%20Indonesian%20Jihadism%20-%20Small%20Groups%20Big%20Plans.pdf>

- International Crisis Group. (2012). *Indonesia: The deadly cost of poor policing* (Asia Report No. 218). Retrieved from <http://www.crisisgroup.org/~media/Files/asia/south-east-asia/indonesia/218%20Indonesia%20--%20The%20Deadly%20Cost%20of%20Poor%20Policing>
- Jackson, M., Petersen, E., Bull, J., Monsen, S., & Richmond, P. (1960). The failure of an incipient social movement. *Pacific Sociological Review*, 3, 35–40.
- Jakarta Centre for Law Enforcement Cooperation. (2005-2010). *Annual reports*. Retrieved from http://www.jclec.com/index.php?option=com_doman&task=cat_view&gid=113&Itemid=42
- Jones, S. (2009). Noordin's dangerous liaisons. *Tempo*. Retrieved from <http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/op-eds/jones-noordins-dangerous-liaisons.aspx>
- Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. University Park, PA: Pennsylvania State University Press.
- Kilcullen, D. (2010). *Counterinsurgency*. Oxford, UK: Oxford University Press.
- 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
- Krackhardt, D. (1994). Graph theoretical dimensions of informal organizations. In K. M. Carley & M. J. Prietula (Eds.), *Computational organization theory* (pp. 89–111). Hillsdale, NJ: L. Erlbaum Associates.
- Krebs, V. (2001). Mapping networks of terrorist cells. *Connections*, 24(3), 43–52.
- Lindelauf, R., Borm, P., & Hamers, H. (2009). The influence of secrecy on the communication structure of covert networks. *Social Networks*, 31, 126–137. doi: 10.2139/ssrn.1096057
- Lofland, J., & Stark, R. (1965). Becoming a world-saver: A theory of conversion to a deviant perspective. *American Sociological Review*, 30, 862–875. doi: 10.2307/2090965
- Maoz, Z. (2011). *Networks of nations: The evolution, structure, and impact of international networks, 1816–2001*. Cambridge, UK: Cambridge University Press.
- McAdam, D. (1982). *Political process and the development of Black insurgency, 1930–1970*. Chicago, IL: University of Chicago Press.
- McAdam, D. (1986). Recruitment to high risk activism: The case of Freedom Summer. *American Journal of Sociology*, 92, 64–90. doi: 10.1086/228463
- McAdam, D. (1999). *Political process and the development of Black Insurgency, 1930-1970* (2nd ed.). Chicago, IL: University of Chicago Press.
- McAdam, D., & Paulsen, R.. (1993). Specifying the relationship between social ties and activism. *American Journal of Sociology*, 99, 640–667. doi:10.2307/2781286
- McCloskey, D. (1995). The insignificance of statistical significance. *Scientific American*, April, 32–33.
- McCormick, G. (2005). *The Diamond Insurgent/COIN Model*. Department of Defense Analysis, Naval Postgraduate School. Monterey, CA.
- McCormick, G., & Owen, G. (2000). Security and coordination in a clandestine organization. *Mathematical and Computer Modelling*, 31, 175–192. doi:10.1016/S0895-7177(00)00050-9
- Morselli, C. (2009). *Inside criminal networks*. New York, NY: Springer.
- Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*, 29, 71–98. doi:10.1016/j.socnet.2006.05.001
- Passy, F. (2003). Social networks matter. But how? In M. Diani & D. McAdam (Eds.), *Social movements and networks: Relational approaches to collective action* (pp. 21–48). Oxford, UK: Oxford University Press. doi: 10.1093/0199251789.003.0002
- Prell, C. (2011). *Social network analysis: History, theory & methodology*. Thousand Oaks, CA: SAGE Publications.
- Priamarizki, A. (2013). Counter-terrorism in Indonesia: The end of special detachment 88? *RSIS Commentaries*, 062/2013. Retrieved from <http://www.rsis.edu.sg/publications/Perspective/RSIS0622013.pdf>

- Raab, J., & Milward, H. B. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory*, 13(4), 413–439. doi: 10.1093/jpart/mug029
- Ramakrishna, K. (2009). Governmental responses to extremism in Southeast Asia: 'Hard' versus 'soft' approaches. In A. de Borchgrave, T. Sanderson & D. Gordon (Eds.), *Conflict, community, and criminality in Southeast Asia and Australia: Assessments from the field* (pp. 31–36). Washington, DC: Center for Strategic and International Studies.
- Roberts, G. (2013). Indonesian anti-terror squad killings prompt revenge attacks. Retrieved from http://www.abc.net.au/am/content/2013/s368601_0.htm
- Roberts, N., & Everton, S. F. (2011). Strategies for combating dark networks. *Journal of Social Structure*, 12(2). Retrieved from http://www.cmu.edu/joss/content/articles/volume_12/RobertsEverton.pdf
- Sageman, M. (2003). *Statement to the National Commission on Terrorist Attacks Upon the United States*. Retrieved from http://www.9-11commission.gov/hearings/hearing3/witness_sageman.htm
- Sageman, M. (2004). *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.
- Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.
- Scott, J. (2000). *Social network analysis: A handbook* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Smith, C. S. (1991). *The emergence of liberation theology: Radical religion and social movement theory*. Chicago, IL: University of Chicago Press.
- Snijders, T. A. B. (1981). The degree variance: An index of graph heterogeneity. *Social Networks*, 3, 163–174. doi:10.1016/0378-8733(81)90014-9
- Snow, D. A., Zurcher, L. A., & Eklund-Olson, S. (1980). Social networks and social movements: A microstructural approach to differential recruitment. *American Sociological Review*, 45, 787–801. doi:10.2307/2094895
- Solomon, D. (2007). *Pillars of power: Australia's institutions*. Sydney, Australia: The Federation Press.
- Stark, R. (1996). *The rise of Christianity: A sociologist reconsiders history*. Princeton, NJ: Princeton University Press.
- Stark, R., & Bainbridge, W. S. (1980). Networks of faith: Interpersonal bonds and recruitment to cults and sects. *American Journal of Sociology*, 85(6), 1376–1395.
- Sunstein, C. R. (2009). *Going to extremes: How like minds unite and divide*. Oxford, UK: Oxford University Press.
- Tucker, D. (2008). Terrorism, networks and strategy: Why the conventional wisdom is wrong. *Homeland Security Affairs*, 4(2), 1–18.
- Uzzi, B. (1996). The sources and consequences of embeddedness for the economic performance of organizations: The network effect. *American Sociological Review*, 61(4), 674–698. doi: 10.2307/2096399
- Uzzi, B. (2008). A social network's changing statistical properties and the quality of human innovation. *Journal of Physics A: Mathematical and Theoretical*, 41, 1–12. doi: 10.1088/1751-8113/41/22/224023
- Uzzi, B., & Spiro, J. (2005). Collaboration and creativity: The small world problem. *American Journal of Sociology*, 111(2), 447–504. doi: 10.1086/432782
- Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge, UK: Cambridge University Press.
- Ziliak, S. T., & McCloskey, D. N. (2008). *The cult of statistical significance*. Ann Arbor, MI: The University of Michigan Press.

About the Authors

Sean F. Everton is an Assistant Professor in the Department of Defense Analysis and the Co-Director of the CORE Lab at the Naval Postgraduate School (NPS). Professor Everton earned his MA and PhD in Sociology at Stanford University (2007). He has published in the areas of social network analysis, sociology of religion, economic sociology, and political sociology, and he currently specializes in the use of social network analysis to track and disrupt dark networks (e.g., criminal and terrorist networks).

His monograph on using social network analysis for the crafting of strategies for the disruption of dark networks (*Disrupting Dark Networks*) was published by Cambridge University Press in late 2012.

Daniel Cunningham is an Associate Faculty for Instruction in the Defense Analysis Department at the Naval Postgraduate School (NPS) in Monterey, CA, where he lectures on the visual analysis of dark networks. He is also a Research Associate in the

Defense Analysis Department's Common Operational Research Environment (CORE) Lab and he is the supervisor for the lab's outreach efforts with practitioners. Dan earned his MA in International Policy Studies with a focus in Terrorism Studies at the Middlebury Institute of International Studies (MIIS) in 2009 and has published several articles on dark networks.

Endnotes

-
- ¹ Other examples of successful centralized covert networks include Pablo Escobar's drug trafficking network and Peru's Sendero Luminoso (Shining Path).
 - ² One notable exception is Koschade's (2006) analysis of the first Bali Bombing network.
 - ³ Fa'i is a method used by many groups to obtain money and resources from armed robberies
 - ⁴ A tactic that was unsuccessfully attempted by the 2010 Dulmatin-led group in Aceh (International Crisis Group, 2010).
 - ⁵ A one-mode network consists of a single set of actors and the relationships between them, which can be any type of ties, such as kinship, friendship, etc.
 - ⁶ Two-mode networks either consist of two sets of different actors, such as people and businesses, or one set of actors and one set of events or affiliations.
 - ⁷ The business and finance network is so sparse that it makes little sense to analyze it separately.
 - ⁸ We could have analyzed these networks separately in the multivariate regression section, but the purpose of this analysis is to examine the overall behavior of the Noordin Top terrorist network in terms of network resiliency. The analysis of each sub-network would certainly provide insight into intricacies of the network's resilience, however.
 - ⁹ We used a variety of regression diagnostic plots (e.g., residual vs. fitted plots, proportional leverage plots, leverage vs. squared residual plots) to identify potentially influential cases that if removed substantially changed our regression results. For each model, we then estimated a regression equation that included all cases and one that removed potentially influential cases. Then, using the Akaike information criterion (AIC) and Bayesian information criterion (BIC) measures of fit, we compared the models to one another. The results from the models having the best fit are presented in Table 1.
 - ¹⁰ Figures 2 through 5 appear to indicate that this does not hold for the operations network.