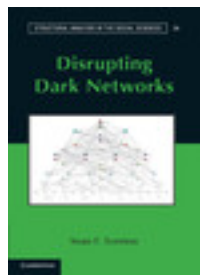

Disrupting Dark Networks

Sean F. Everton

Book DOI: http://dx.doi.org/10.1017/CBO9781139136877

Online ISBN: 9781139136877

Hardback ISBN: 9781107022591

Paperback ISBN: 9781107606685

Chapter

Preface pp. xxv-xxxiv

Chapter DOI: http://dx.doi.org/10.1017/CBO9781139136877.001

Cambridge University Press

Preface

The Problematic Nature of Dark Networks

This book is concerned with the use of social network analysis (SNA) for tracking, destabilizing, and disrupting dark networks. Following Jörg Raab and Brint Milward, dark networks are defined here as covert and illegal networks (Milward and Raab 2006; Raab and Milward 2003), namely, any group that seeks to conceal itself and its activities from authorities. While the term is typically used to refer to groups such as terrorists, gangs, drug cartels, arms traffickers, and so on, it can refer to benign groups as well. For instance, Żegota, the predominantly Roman Catholic underground organization that addressed the social welfare needs of Jews in German-occupied Poland from 1942 to 1945 (Tomaszewski and Webowski 1999), would be considered a dark network because it was covert and, at least from the perspective of the Nazis, illegal. That said, this book implicitly assumes that the theories and methods it discusses will be used for the disruption of dark networks that seek to harm innocent civilians and the societies in which they live.[1]

Social network analysts have long considered the nature of dark networks. Georg Simmel (1906, 1950b), for example, was one of the first to explore their structure in his essay on secret societies, a study that Bonnie Erickson (1981) later expanded and modified. A decade later Malcolm Sparrow (1991) considered the usefulness of SNA for tracking criminal networks, and Wayne Baker and Richard Faulkner (1993) used SNA to examine three price-fixing conspiracy networks in the heavy electrical equipment industry. Since 9/11, analysts have become increasingly drawn to the use of SNA as a tool for understanding dark networks (Reed 2007;

[1] Of course, that does not prevent individuals, groups, organizations, or states from using the techniques discussed herein for ill rather than good. This is a genuine concern and a topic that the book's final chapter addresses.

Ressler 2006), largely because of Valdis Krebs's (2001) analysis of the 9/11 hijacker network. For instance, Sageman (2004) analyzed the network of 172 Islamic terrorist operatives affiliated with the global salafi jihad; José Rodriguez (2005) mapped the March 11, 2004, Madrid bombings; and Ami Pedahzur and Arie Perliger (2006) examined the nature of suicide attack networks. These, of course, are just a few examples; several other notable studies exist (see, e.g., Asal and Rethemeyer 2006; Carley 2003a; Koschade 2006; Magouirk, Atran, and Sageman 2008; Moody 2005; Tsvetovat and Carley 2005; van Meter 2001), many of which we will consider later in the book.

An overriding concern of many of these analysts has been the structure of dark networks. Simmel (1906, 1950b), for instance, argued that since secret societies are organized to conceal themselves and protect their members from detection, they adopt practices and organizational structures that help protect them and their members. He believed that the ideal organizational structure for dark networks was a hierarchy, but Erickson (1981) later showed that while some are, many are not, and that their structure is a function of risk and the group's desire to maximize security. Baker and Faulkner (1993) uncovered similar dynamics in their analysis of price-fixing conspiracies. Using reconstructed communication networks, they found that the conspiracies' structure was driven more by the need to maximize concealment than efficiency, so they adopted decentralized structures. Their findings fit nicely with other studies that have found that because of their adaptability, decentralized networks are generally better suited for solving nonroutine, complex, and/or rapidly changing "problems" or challenges (Arquilla and Ronfeldt 2001; Bakker, Raab, and Milward 2011; Klerks 2001; Krebs 2001; Milward and Raab 2006; Powell 1985, 1990; Raab and Milward 2003; Ronfeldt and Arquilla 2001; Saxenian 1994, 1996). Such structures create problems for those seeking to disrupt dark networks because the networks can adapt quickly to changing environmental pressures. As a case in point, prior to the September 11th attacks, Al Qaeda was a somewhat vertically integrated organization, at least at the command and control level, but since the U.S. invasion of Afghanistan, available evidence indicates that it has become far more decentralized (Raab and Milward 2003:425; Sageman 2008).

In practical terms what all this means is that dark networks are constantly evolving, which suggests that gathering timely and accurate data is always difficult. This difficulty is exasperated by the fact that dark networks actively try to remain hidden, which often renders data on them incomplete (Borgatti, Carley, and Krackhardt 2006; Krebs 2001; Sparrow 1991). That said, there is a surprising amount of detailed information on dark networks, much of it in the open-source literature. The challenge that many analysts have is not finding data but sorting through it. Moreover, the notion that open-sourced information is somehow "second class" is

misguided (Flynn, Pottinger, and Batchelor 2010:23). As former director of the Defense Intelligence Agency, Lieutenant General Samuel V. Wilson has noted (cited in Flynn, Pottinger, and Batchelor 2010:23): "Ninety percent of intelligence comes from open sources. The other 10 percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond"; this means that analysts need to "embrace open-source, population-centric information as the lifeblood of their analytical work" (Flynn, Pottinger, and Batchelor 2010:23).

In recent years the quality and timeliness of social network data have increased due in large part to the improvement of link-analysis programs such as Analyst's Notebook[2] and Palantir,[3] which facilitate the collection of structured and unstructured data. While these programs are not SNA programs per se (see discussion of the difference in Chapter 1), they do include functionality that allows users to export data in formats that dedicated SNA programs can use. For example, Palantir currently exports social network data in formats that can be read by SNA programs such as UCINET,[4] NetDraw,[5] Pajek,[6] and Organizational Risk Analyzer (ORA),[7] and ORA imports Analyst's Notebook files.

Another advance in the collection of social network data is the development of smart-phone-based systems. For example, the smart-phone application Lighthouse[8] uses menu-driven forms to guide the collection of all types of data, including social network data, which then flow from the collection point to analysts in near real time, regardless of location or physical proximity. The system then exports the data into formats ready for geospatial, link, social network, and other types of analysis. In 2010, Lighthouse was used to collect relational, geospatial, and other ethnographic data in the Khakrez District (located in northern Kandahar Province) as part of the village stability operations in Afghanistan.[9] The resulting dataset included up-to-date and accurate relational data

[2] http://www.i2group.com/us/products-services/analysis-product-line/analysts-notebook.

[3] http://www.palantirtech.com/government.

[4] UCINET 6.0 (Borgatti, Everett, and Freeman 2011) is available at www.analytictech.com.

[5] NetDraw (Borgatti 2002–2005) comes as part of the UCINET 6.0 package but can also be downloaded separately at the Analytic Technologies website: www.analytictech.com.

[6] Pajek (Batagelj and Mrvar 2012) is a network analysis and graph drawing program designed to handle extremely large data sets that can be downloaded for free for noncommercial use from the Pajek Wiki website: http://pajek.imfm.si/doku.php?id=download.

[7] ORA (Carley 2001–2011) can be downloaded for free for noncommercial use from the ORA website: http://www.casos.cs.cmu.edu/projects/ora/.

[8] Lighthouse was developed by Captain Carrick Longley with the help of Chief Warrant Officer Chad Machiela: http://lhproject.info/.

[9] *Village stability operations* refers to the program of putting special forces units (e.g., civil affairs units) in rural villages to make it harder for Taliban and other insurgent groups to find safe haven. The villages receive assistance to improve infrastructure development, governance, and security that they can take back to their village.

on several hundred individuals and organizations (i.e., business, kinship, organizational, personal, elder, and tribal affiliations). For example, in three weeks collection efforts identified the community's most central actor as a Taliban sympathizer (his son was in the Taliban) who was (not surprisingly) resistant to efforts by the United States to reduce the Taliban's influence in the area. While this individual's centrality was not "news" to the local forces, analysts not only identified this individual within a shorter period of time than the local forces did, but they also provided the local forces with an array of noncoercive strategies that could decrease this individual's influence by elevating the centrality of others who were more sympathetic to the village stability operations.

Another aspect of dark networks that can create problems for analysts is that they do not necessarily operate independently from one another but instead are often connected through actors who function as brokers between these networks:

> A truism of the network approach is that, at some level, everything is connected to everything else. This is no less true of dark networks. There is increasing evidence of a close connection between Al Qaeda and the failed states of Liberia, Sierra Leone, and Burkina Faso in West Africa. The connection appears based on Al Qaeda's need to exchange cash for diamonds. This is fueled by the pressure from the United States and Western Europe to clamp down on Al Qaeda's use of legitimate banks for international monetary transactions. Diamonds provide a ready currency for Al Qaeda, and the failed states of the region have perhaps provided a safe haven for Al Qaeda's operatives in the wake of 11 September in exchange for arms and money for the warlords of the region. (Raab and Milward 2003:425)

Consequently, accurately specifying a network's boundaries is of the utmost importance, a topic we take up in Chapter 4. Misspecification can lead to the incorrect estimation of metrics and the development of inappropriate strategies and recommendations.

The Social Network Analysis of Dark Networks

To be sure, these three problems – dynamic and evolving networks, the potential incompleteness of data, and fuzzy boundaries (Krebs 2001; Sparrow 1991) – are not unique to dark networks. They arise with light networks as well. It is just that with dark networks, they can be more acute. Does that mean we should abandon the social network approach for disrupting dark networks? No, I do not think so. In recent years SNA has enhanced our understanding of how dark networks organize

themselves (Milward and Raab 2006; Raab and Milward 2003) and has offered potential strategies for their disruption (see, e.g., Krebs 2001; Pedahzur and Perliger 2006; Roberts and Everton 2011; Rodriguez 2005; Sageman 2003, 2004), some of which have been successful. Perhaps the best-known success story is the capture of Saddam Hussein (Wilson 2010), but it has been successfully used to destabilize improvised explosive devices (IED) network (Gjelten 2010) as well as to roll up an insurgency in Iraq (Anonymous 2009).

Nevertheless, there seems to be far too much emphasis on using centrality and brokerage measures (or variations on them) to identify high-value targets within dark networks (Jordan, Mañas, and Horsburgh 2008; Krebs 2001; Pedahzur and Perliger 2006; Roberts and Everton 2011; Sageman 2004; for a similar critique, see Tsvetovat and Carley 2005). While targeting key players is intuitively appealing and might provide short-term satisfaction, it can be misplaced and may make tracking and destabilizing dark networks more difficult than it already is (Arquilla 2008; Schmitt and Perlez 2009; Yasin 2010). As Brafman and Beckstrom (2006) have noted, removing high-value targets in decentralized organizations, which as we previously noted dark networks often are, does not always shut them down but sometimes drives them to become more decentralized, making them even harder to disrupt. This is not to suggest that analysts should abandon the use of metrics that identify key players, but rather that they view them as one set of algorithms among many that can be used to help flesh out a range of strategic options. Indeed, a whole host of nonkinetic (i.e., noncoercive) strategies exist such as institution building, psychological operations (PsyOp),[10] information operations (IO), and rehabilitation and reintegration efforts,[11] many of which have already proved successful. For example, intelligence officers in northern Iraq used SNA to craft a PsyOp campaign that caused an insurgent network in Iraq to turn on itself (Anonymous 2009), and rehabilitation and reintegration programs in Singapore appear to be meeting with some success[12] (Yasin 2010). To be sure, nonkinetic strategies take patience and are often for the long haul, but as Tilly (2005) notes, while the integration of dark networks (not a term he uses) into civil society is necessary, it often takes time. Nonkinetic strategies are hardly new, of course; they have been used successfully in the past (see, e.g., Galula [1964] 2006; Kilcullen 2009, 2010; Nagl 2005), but what SNA brings

[10] The Department of Defense recently dropped the term Psychological Operations (PsyOp) in favor of Military Information Support Operations (MISO) (Maurer 2010). This book uses the former term because of its familiarity.

[11] These strategies are discussed in more detail in Chapter 2.

[12] See, e.g., http://www.singaporeunited.sg/cep/index.php/web/layout/set/print/content/view/full/3037, http://www.rrg.sg/subindex.asp?id=A266_07, and http://www.asiancrime.org/pdfdocs/Singapore_CT_Efforts_Corsi.doc.

to the table are methods for more accurately identifying those institutions, groups, and/or individuals that would be receptive to noncoercive approaches. Unfortunately, there appears to be a lack of awareness of the various nonkinetic strategies available. Thus, this book seeks to fill this vacuum by placing the SNA of dark networks into a larger strategic framework that considers both kinetic and nonkinetic approaches to dark network disruption.

In particular, this book has in mind four primary audiences: (1) scholars who study terrorist and other dark networks but have little or no background in SNA, (2) social network analysts who want to move beyond simple employment of social network metrics in order to see how such metrics can be placed within a strategic framework, (3) students who are looking for a text that not only introduces them to SNA but also applies it to a specific phenomenon, and (4) policy makers who often operate in arenas where terms such as "social network analysis" are bandied about with little genuine knowledge of what the terms actually mean and who would like to expand their understanding of the topic.

Organization of the Book

The book is structured in such a way that it not only introduces researchers to basic social network theories and techniques, but also embeds these theories and techniques in the larger strategic framework that is crucial for tracking, destabilizing, and/or disrupting dark networks. Unlike a number of monographs on social network analysis that focus on a particular phenomenon (see, e.g., Friedkin 1998; Jackson 2008; Kilduff and Tsai 2003; Kontopoulos 1993; Lewis 2009), this book not only explores the theoretical aspects of dark networks, but, following the lead of others (de Nooy, Mrvar, and Batagelj 2005, 2011; Hanneman and Riddle 2005), also illustrates how to use social network software (i.e., UCINET, NetDraw, Pajek, and ORA) to estimate the various metrics illustrated and discussed in the text. To facilitate this, a particular dark network – the Noordin Top terrorist network – serves as a running example throughout the book, from the initial collection of social network data to estimating various SNA metrics to strategies for disrupting dark networks in general (see Appendix 1 for a description of the data).[13]

[13] Prior to his death in September 2009, Top was Indonesia's most wanted terrorist (International Crisis Group 2006, 2009a, 2009b). He began as one of Jemaah Islamiyah's (JI) key bomb makers and financiers before striking off on his own to set up a more violent group that is believed to be responsible for the August 2003 Marriot Bombing in Jakarta, Australian embassy bombing in Jakarta in September 2004, the second Bali bombing of October 2005 (Bali II – JI was responsible for the first Bali bombing in October 2002), and the Jakarta bombings of the Marriott and the Ritz-Carlton in July 2009.

The book demonstrates how to examine the topography of Noordin's network, identify its central actors, uncover any cohesive subgroups, pinpoint its key brokers and bridges, detect classes of structurally equivalent actors, and examine it both over time and geospatially.[14] Drawing on a typology suggested by Krebs (2001:51), four aspects of Noordin's network will be analyzed: his trust, operational, communication, and business and finance networks, as well as the combination of these networks into a single network. Moreover, we will often extract and analyze subnetworks from these four types of networks (five if you count the combined network) based on whether network members are alive, dead, or in jail. In other words, in addition to analyzing Noordin's "Trust," "Operational," "Communication," "Business and Finance," and "Combined" networks, we will explore the "Alive and Free," "Alive," and "Incarcerated" subnetworks of these larger networks, giving us a total of twenty Noordin networks available for analysis. For what should be obvious reasons, we will not analyze all twenty networks in every chapter. To do so would be needlessly repetitive. Instead, in each chapter networks are chosen that, in part, help illustrate the algorithms under consideration.[15]

The book's first two chapters serve as an introduction to the use of social network analysis for the disruption of dark networks. The first chapter provides an overview of the basic terms, concepts, and assumptions of social network theories and methods, while the second outlines the various strategies with which SNA can be combined and a process for doing so. Some may wonder whether these theoretical and strategic discussions, however brief, are necessary. Obviously, I think they are. And that is because they attempt to show that SNA should not be used for disrupting dark networks apart from a basic knowledge of the theories and assumptions lying behind the various methods, as well as the array of strategies available to analysts.

The next two chapters introduce readers to some SNA basics. Chapter 3 seeks to help users become comfortable with the four SNA software packages illustrated in this guide: UCINET, the "granddaddy" of SNA software programs; NetDraw, a program for visualizing social network data developed by the same people who created UCINET; Pajek, a SNA package that integrates metrics and visualization; and ORA (Organizational Risk Analyzer), a relatively new software package that allows analysts to analyze more than social networks. Chapter 4 builds on this chapter and introduces the basics of collecting, recording, manipulating, and visualizing social network data using these software programs.

[14] Other social networks are used to illustrate various aspects of social network analysis as well, but only the Noordin Top network is used throughout the book.

[15] In the real world, of course, analysts will want to examine as many permutations of the dark networks they are analyzing as possible before they sit down to craft strategies for disruption.

The next five chapters examine some of the more common SNA methodologies as well as consider how they can inform crafting strategies for dark network disruption: Chapter 5 looks at a variety of metrics for getting a sense of how the network is structured as a whole (i.e., its topography); Chapter 6 explores a variety of methods for detecting clusters and subgroups within the larger network; Chapter 7 examines how various measures of centrality can be used to detect a network's key and peripheral players; Chapter 8 explores methods for locating actors and ties that broker the flow of information and other resources within and through the network; and Chapter 9 looks at algorithms for identifying actors who are located in similar positions in the social network.

The next two chapters introduce readers to some of the recent advances in SNA that can be of use to dark network analysts. Chapter 10 introduces readers to the dynamic analysis of social networks, a burgeoning and varied field in social network analysis. Here we only brush the surface of this type of the various approaches that fall under this nomenclature. Specifically, we examine approaches for analyzing longitudinal networks and fusing social network and geospatial data. Chapter 11 examines some of the statistical models available for social network analysts – in particular, those that help analysts disentangle genuine from spurious effects.

While, for the most part, Chapters 5 through 11 stand on their own, in many ways they build on one another (especially from a strategic perspective). Thus, it is probably wise to work your way through the book sequentially.

The book's final chapter considers the promises and limitations of social network analysis. SNA should not be seen as a silver bullet in the fight against terrorist and criminal networks but rather one tool among many that can be used for crafting potential strategies. This chapter also addresses the concern that the theories and methods outlined in this book will be used for ill rather than good. While we have little or no control over how such knowledge will be consumed by others, we can still provide guidelines on how we believe such knowledge can be used. Thus, the final chapter explores the ethics of using SNA to disrupt dark networks. It considers a variety of ethical traditions before arguing that the use of SNA for the disruption of dark networks should be guided by the goal of encouraging those practices that allow human beings to flourish.

The book is, for the most part, decidedly nontechnical. The focus is placed on the assumptions lying behind the metrics that are explored. Consequently, mathematical equations are kept to a minimum and only included when I believe they either facilitate comparisons between various metrics or illuminate the metric being considered. For those interested in exploring SNA's mathematical and graph theoretical foundations, there

are plenty of resources available (see, e.g., Brandes and Erlebach 2005; Jackson 2008; Lewis 2009; Wasserman and Faust 1994). The book also does not attempt to provide a comprehensive introduction to all the various theories and techniques associated with SNA. There are a number of available monographs that do just that.[16] Instead, it seeks to bridge the gap between theory and practice by demonstrating how to apply various theories and methods to specific examples. Finally, it adopts the approach used by Everton (2004); de Nooy, Mrvar, and Batagelj (2005, 2011); and Hanneman and Riddle (2005) in that it not only discusses various social network techniques and metrics, it illustrates how to estimate them with worked examples, in this case using UCINET, NetDraw, Pajek, and ORA.[17] The example datasets used in the book, except for the Noordin dataset, are publicly available, and most are provided with the UCINET software package. Nevertheless, all have been gathered and made available at a single website (https://sites.google.com/site/sfeverton18/). Because these programs are regularly updated, it is likely that the various dialog boxes, command menus, and report windows illustrated here will not always match what readers encounter when working with these programs. It is also likely that I will make statements about what the programs can and cannot do that will no longer be true because of updates that occurred after this manuscript was submitted. Nevertheless, most changes should be minor and should not cause the readers too much difficulty. That said, Pajek was significantly updated shortly after this manuscript was completed, so I strongly recommend using the "Book Edition 2" (version 2.05), which can be downloaded at the Pajek website (http://pajek.imfm.si/doku.php?id=download), while using this book and then updating to a newer version afterward.

[16] Readers who are interested in general introductions to social network analysis should consult Degenne and Forsé (1999), Kadushin (2012), Knoke and Yang (2007), Prell (2011), Scott (2000), and Scott and Carrington (2011). Wasserman and Faust (1994) offer a more comprehensive (and mathematical) introduction. Easley and Kleinberg (2010) introduce the topic from the perspective of an economist and network scientist. Robert Hanneman and Mark Riddle (2005) have written a helpful introduction to social network analysis methods using UCINET, while Walter de Nooy, Andrej Mrvar, and Vladimir Batagelj (2005, 2011) have done the same for those interested in Pajek.

[17] Following de Nooy, Mrvar, and Batagelj (2005, 2011) these commands are placed in the margin next to the text discussing the technique/metric in order to make them easier to follow and locate.