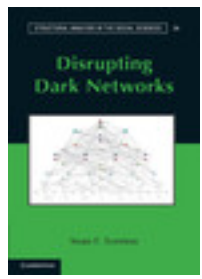

Disrupting Dark Networks

Sean F. Everton

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

Online ISBN: 9781139136877

Hardback ISBN: 9781107022591

Paperback ISBN: 9781107606685

Chapter

2 - Strategic Options for Disrupting Dark Networks pp. 32-46

Chapter DOI: http://dx.doi.org/10.1017/CBO9781139136877.004

Cambridge University Press

2

Strategic Options for Disrupting Dark Networks

2.1 Introduction

Given the time and energy that has been devoted to the collection of data on dark networks (see, e.g., Koschade 2006; Krebs 2001; Rodriguez 2005; Sageman 2004, 2008; van Meter 2001), it is surprising that little attention has been paid to exploring strategies for their disruption (Roberts and Everton 2011). Strategies for combating them are poorly documented in the literature, and with one exception (Lempert et al. 2008), little or no research compares alternative strategies with a view of balancing potential gains and costs. Moreover, it appears to be almost an article of faith that once a dark network's structure has been mapped and its key members identified, one is supposed to capture and eliminate designated high-value targets. However, as noted in the preface, while targeting key players is one option to consider (Walzer 2009:274), other options exist that may offer better alternatives when taking into account costs, human lives, and the consequences for affected communities (see Chapter 12).

This chapter argues that various strategies for countering dark networks need to be considered prior to the use of formal social network analysis. It begins by distinguishing between two general approaches to countering dark networks: kinetic and nonkinetic.[1] The former involves aggressive and offensive measures designed to eliminate or capture network members and their supporters, while the latter involves the use of subtle, noncoercive means designed to reduce a network's effectiveness and impair a combatant's will to fight. This chapter then moves to an overview of the process through which analysts can generate strategies

[1] There is little agreement in the literature on how to describe the alternative approaches to countering terrorism. Some authors use different characterizations such as direct and indirect strategies (Arreguin-Toft 2001, 2005; Fridovich and Krawchuck 2007; Krawchuck ND). Here the focus is on combatant behavior and the level of the coercion involved in their strategies; hence, the terms "kinetic" and "nonkinetic" are used.

for disrupting networks, a process that involves the drafting of working hypotheses, the identification of relations of interest, the aggregation and/or parsing of these networks, the exploratory analysis and interpretation of the networks, and a revisiting of the original hypotheses. The chapter then concludes with a brief reflection on the proper uses of SNA for the disruption of covert and illegal networks.

2.2 Strategic Options for Disrupting Dark Networks[2]

Of the two approaches to combating dark networks, the kinetic approach tends to receive more attention because the capture or elimination of high-value targets attracts headlines and engenders popular support. One only has to recall the media attention (and spontaneous celebrations across the United States) that Osama bin Laden's assassination engendered to know that this is true. The nonkinetic approach, which typically requires patience and skill, tends to attract far less attention, probably because of its subtlety and lack of newsworthiness. Nevertheless, the former U.S. Special Operations Commander, Admiral Eric T. Olson, has tried to shift the emphasis away from kinetic, high-profile raids and toward the use of more nonkinetic approaches. He acknowledges that while kinetic action may be "urgent and necessary" in the short term, he believes that it is merely "a holding action that buys time for non-kinetic approaches to have their effects" (quoted in Roberts and Everton 2011:4). Because of the importance that these two approaches play in counterinsurgency operations, both are explored in greater depth in the following sections.

Kinetic Approach

Kinetic operations target enemy combatants and their supporters in order to neutralize, capture, or eliminate them. They are typically referred to as *targeting strategies* and can be pursued at the individual, group, and organizational (i.e., institutional) levels. Regardless of the level of analysis, they involve the removal of key actors (i.e., individuals, groups, or organizations) or the severing of ties between such actors. When individuals are the target, such as the capture or elimination of Saddam Hussein, Abu Musab al-Zarqawi, or Osama bin Laden, the U.S. military describes such operations as man-hunting (Marks, Meer, and Nilson 2005). When

[2] This section has been adapted from Nancy Roberts and Sean F. Everton. 2011. "Strategies for Combating Dark Networks." *Journal of Social Structure* 12(2):1–32. Accessed at http://www.cmu.edu/joss/content/articles/volume12//RobertsEverton.pdf. Used with permission. Nancy, of course, should not be held responsible for my adaptations.

groups or organizations are the target, they are referred to as group or organizational targeting. Examples of the former include the roundup of specific groups fashioning improvised explosion devices (IEDs) in Iraq (Peter 2008), the disruption of the Syrian recruitment network bringing jihadists into Iraq (Felter and Fishman 2007), and the shutdown of the financial network supporting the Indonesia-based Jemaah Islamiyah (JI) (Abuza 2003); examples of the latter include Malaysia's successful effort to close down Luqmanul Hakiem, a jihadist religious boarding school (Rabasa 2005) and the Al Qaeda–linked Islamic NGO, Pertubuhan al Ehasan, in 2002 (Abuza 2003).

Sometimes military forces function in a consulting role and work "through, by, and with" indigenous forces to build their capacity to conduct effective targeting operations against common enemies (Fridovich and Krawchuck 2007). An example of this approach is when U.S. Special Operation Command forces deployed to Basilan to advise and train the Armed Forces of the Philippines in their fight against the Abu Sayyaf Group (ASG) (Fridovich and Krawchuck 2007; Krawchuck ND; Wilson 2006).

Nonkinetic Approach

The nonkinetic approach is a less aggressive means for countering insurgencies. It involves a more subtle and patient application of power by seeking to undermine insurgencies "more through cooperation and collaboration with partners than through unilateral . . . action, more with the diplomatic and economic tools of national power than with the military, stressing inspiration rather than prescription" (Brimley and Singh 2008:313). Its goal is to secure the population's safety and support while undermining the enemy's influence and control (Galula [1964] 2006; Kilcullen 2008, 2009; McCormick 2005; Wendt 2005) and employs numerous ways to accomplish this goal: institution-building, psychological operations (PsyOp), information operations (IO), rehabilitation and reintegration programs, and the tracking and monitoring of key network actors. Like the kinetic approach, it can target individuals, groups, or organizations.

Institution-Building. This strategy promotes reconstruction in war-torn communities and requires the active involvement of civil affairs forces that provide humanitarian and civic assistance and work in tandem with intergovernmental and interagency partners in the reconstruction process. The emphasis is on building healthy host-government institutions of governance, rule of law, economic development, and transportation infrastructure (Fridovich and Krawchuck 2007; Kilcullen 2009). As we will see in the final chapter, contemporary "just war" theorizing sees

institution-building as a necessary criterion of what it means to fight a "just war" (Allman and Winright 2010).

Psychological Operations (PsyOp). Psychological operations involve the dissemination of information for the purpose of influencing the emotions, perceptions, attitudes, objective reasoning, and ultimately the behavior of foreign nationals (individuals, groups, organizations, governments) so that they are more aligned with one's goals and objectives during times of conflict and peace (U.S. Special Operations Command 2003). They are also employed to counter adversary propaganda and to sow disaffection and mistrust among network members to reduce their will to fight and ultimately induce their surrender. This strategy also includes tactics that attempt to set network members and/or subgroups against each other. One example is the British plan to split the Taliban from within by securing the defection of its senior members and a large number of their supporters. It follows from former British Prime Minister Gordon Brown's decision to focus on courting "moderate" Taliban leaders and "tier-two" foot soldiers who fight more for money and a sense of tribal loyalty than for the Taliban's ideology as well as from the United States' consideration of a divide-and-conquer strategy to peel away some lower-level members of the Taliban and win back the population (Cooper 2009; Rubin 2011).

Information Operations (IO). This strategy uses integrated employment of electronic warfare and computer network operations to combat terrorism.[3] Examples include the disruption of fund transfers, the monitoring of charitable donations, and the detection of money laundering, black market activity, and the drug trade. Activities also include interventions to compromise terrorists' cell phone and online connections and the use of these platforms to locate leaders and their followers.

Rehabilitation and Reintegration. Charles Tilly (2004, 2005) has noted that throughout history trust networks (e.g., insurgencies, trade diasporas, clandestine religious groups, terrorist groups) have often segregated themselves from what they perceive to be hostile or predatory regimes.[4] In so doing they "hoard" various resources (material and nonmaterial) for

[3] In contrast to military doctrine (U.S. Director of Operations 2006), in this book psychological operations are separated from information operations because the latter puts a strong emphasis on technology-centric interventions that involve computer and other sophisticated electronic systems, whereas the former puts a strong emphasis on human factors.

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

themselves. Tilly argues, however, that regimes, in particular democratic ones, cannot survive without the partial integration of trust networks (and their resources) into civil society. The rehabilitation and reintegration strategy seeks to do just that. An example is Singapore's counter-ideological program founded by Muslim scholars who seek to "correct" the thinking of its detainees (Ramakrishna 2005). This program also seeks to extend its influence into the wider Muslim community by giving talks, disseminating publications, and hosting a website in order to "immunize" the minds of Singaporean Muslims against violent radical Islamist ideologies. In addition, the Singapore government is attempting to forge closer ties between Muslims and non-Muslims through the Community Engagement Program, using Inter-Racial and Religious Confidence Circles in neighborhoods, workplaces, and schools. Similar rehabilitation programs also have been introduced to other countries such as Indonesia, Saudi Arabia, and Yemen.[5] While these efforts are encouraging, if recent research on the effectiveness of U.S. faith-based prison programs that seek to reduce recidivism is of any relevance here, then efforts at redirecting or reframing the extremist ideologies of detainees (Juergensmeyer 2001) may not be enough to bring about their lasting transformation. What may also be necessary are "after care" programs that steer former detainees away from the networks that gave rise to their extremism in the first place and toward networks that support their new theological outlook (Johnson 2011).[6]

One reason this strategy is so attractive is because dark networks often suffer considerable damage if one of their members defects. Studies of insurgent groups have found that groups that keep defection to a minimum tend to be more successful than those that do not because, as political scientist Samuel Popkin discovered when he returned to Vietnam in the 2000s in order to ask former Viet Cong insurgents questions he couldn't ask when he was a graduate student in the 1960s, defection can shut an insurgency down for months (Popkin 2007, cited in Berman 2009:29):

> *Popkin*: "If one of your members was killed, how long did it take for the organization to recover?"
> *Former Viet Cong Rebel*: "A few days."
> *Popkin*: "And if a member defected?"
> *Former Viet Cong Rebel*: "Between a week and two months."

[5] For a review of Saudi Arabia's program, see Boucek (2008a, b). The report by Fink and Hearne (2008) on deradicalization and disengagement from violent extremism provides a general overview of topic. See also Horgan (2009) and Jones and Libicki (2008).

[6] The connection between Johnson's work and rehabilitation programs such as these was first suggested to me by a student of mine, Major Justin Duvall.

Why? Because an insurgency's leaders do not know what information has been passed to the authorities, so drop points need to be changed, members have to lie low, and plans have to be altered because they may have been compromised (Berman 2009:29).

Tracking and Monitoring. While it may seem counterintuitive, sometimes the best strategy may be to do nothing. Well, not exactly nothing, but because information on a particular dark network is often incomplete, rather than taking immediate action, it is sometimes better in the short run to track and monitor certain actors with the hope of improving knowledge of the network, which will in turn improve the selection of strategies adopted down the road (Arquilla 2008). As John Arquilla notes

> In the successful strikes against al Qaeda affiliates in Singapore, Morocco, and Saharan Africa, the key doctrinal approach was to wait and watch for a considerable period, then to swarm the targets simultaneously at their moment of maximum illumination. This strategic patience grew out of the understanding that striking at nodes *as* they were identified might actually reduce the ability to detect and track other cells in the networks in question. It is a curious doctrinal point about netwar: the more that is disrupted, the less may be known. (Arquilla 2009:34)

When using this approach, then, analysts will want to draw on those SNA metrics that help identify the individuals, subgroups, organizations, and so on that appear to be worth tracking.

Summary

This section has distinguished between two general approaches to countering dark networks: kinetic and nonkinetic. The kinetic approach pursues aggressive measures designed to eliminate or capture network members and their supporters. By contrast, the nonkinetic approach employs neither bombs nor bullets but instead uses noncoercive means to counter networks and impair a combatant's will to fight. It includes activities such as the reconstruction of war-torn areas, the disruption of electronic fund transfer networks, information campaigns to win over the "hearts and minds" of local populations, efforts at the rehabilitation and reintegration of dark network members into civil society, and the tracking of certain members in order to improve our knowledge and understanding of the network. Table 2.1 summarizes these options.

Of course, a single approach will seldom suffice. Often, multiple strategies will need to be adopted, some focused on the short term, some on the long term. Moreover, analysts need to take into account unanticipated second- (and third- and fourth-) order effects. For example, implementing

Table 2.1. *Strategic options of social network analysis*

	Kinetic	Nonkinetic				
Strategies	Targeting	Institution Building	PsyOp	Information Operations	Rehabilitate/ Reintegrate	Track, Monitor
Level	Individual, Group, and Institutional					

a raid to capture an insurgent in an otherwise friendly neighborhood is its first-order effect, but the raid's second-order effect may be to decrease support for the host-nation government and increase support for the insurgents if done incorrectly. If the second-order effects of a successful but unpopular raid begin to outweigh the first-order benefits, the secondary effects should take precedence in the planning cycle. Simply put, commanders and policy officials must consider kinetic and nonkinetic actions, approaches, and most importantly effects together as a net positive or net negative in order to most effectively craft strategies for disrupting dark networks.[7]

2.3 Crafting Strategies with Social Network Analysis

In practice, using social network analysis (SNA) to craft strategies for the disruption of dark networks is an iterative process that involves both exploratory analysis and confirmatory analysis (i.e., hypothesis testing). Exploratory SNA "involves visualization and manipulation of concrete networks, whereas hypothesis testing boils down to numbers representing abstract parameters and probabilities" (de Nooy et al. 2005:xxv). The general process for doing this is as follows:

- Develop working hypotheses
- Identify and record relationships of interest
- Aggregate (i.e., combine) and/or parse networks of interest
- Analysis and interpretation
- Craft strategies for the disruption of the network

While we focus on each of these steps in more depth later in this book, it is appropriate to discuss each of them briefly before proceeding.

Developing Working Hypotheses

Before attempting to use SNA, researchers need to first develop working (i.e., tentative) hypotheses as to how best to disrupt the dark network

[7] I thank LCDR Kristian Kearton, CW3 Chad Machiela, and LT Bobby Ramirez for pointing this out to me.

they are analyzing. First, they have to decide whether they intend to use kinetic or nonkinetic approaches or a combination of both and then determine which relationships of interest best lend themselves to their chosen strategies. Some, for example, may decide that the best approach is to focus on the network's financial ties, believing that by shutting down or disrupting the flow of funds, it will be difficult for the network to finance operations. Others may conclude that targeting a network's operational ties offers the best opportunity for disruption, assuming that without its key operatives, a network will not have the personnel necessary to carry out operations. Still others may seek to breed distrust among network members in order that it implodes from within (Anonymous 2009). Some may choose not to focus on a network's individual actors at all but instead on its formal and informal organizations, arguing that the network can more effectively be disrupted by focusing on the groups and organizations that helped give rise to and currently sustain the insurgency (Smith 1996). For example, in the fight against radical forms of Islam, analysts could identify central jihadi schools and build alternative schools nearby, ones that promote moderate forms of Islam and instruct students in subjects other than the memorization of the Qur'an (e.g., reading, writing, and arithmetic; Roberts and Everton 2011). This would clearly constitute a long-term strategy, one that aims not so much at disrupting the current contours of a network but one that aims to deprive it of a key resource (McAdam 1982; McCarthy and Zald 1977; Wiktorowicz 2004). In short, there are multiple ways of disrupting dark networks, of which these are only a few examples. The broader point is that before beginning to collect data on a dark network, researchers need to first develop working hypotheses as to how they plan to disrupt the network.

Identifying, Collecting, and Recording Social Network Data

Working hypotheses guide the types of relationships researchers will eventually collect and record. At the individual level these can be friendship ties, school ties, operational ties, religious ties, and so on. At the group level, they can be ties between two institutions because they share a common member.[8] That said, collecting social network data can be a tedious and complicated process. Not only do we have to determine which ties are important, we have to determine a network's boundaries – that is, where it begins and ends. We may decide to analyze a particular network, but identifying which actors are members of the network and which ones

[8] For example, if someone teaches at a particular school and attends a local community of faith, one could argue that a tie exists between the school and the community of faith.

are not is generally easier said than done. "Networks naturally spread out, so no boundary is ever perfect," but we hope "to find a set of actors with relatively good separateness from the rest of the world" from which we can draw reasonable conclusions (Erickson 2001:317). We take up this topic in more depth in the Chapter 4.

Although new tools are being developed to ease the collection of social network data, analysts have typically recorded relational data in matrix form (see Chapter 4). Take, for instance, the following subset of marital ties between Renaissance Florentine families collected and recorded by John Padgett and Christopher Ansell (1993) and used by Breiger and Pattison (1986) (Figure 2.1). A tie was determined to exist if a member of one family married a member of another family. The data are recorded in a square matrix with a row and column for each family. If a marriage occurred between two families, then a "1" appears in the families' common cells (e.g., Acciaiuol and Medici).[9] If not, a "0" appears. As we will see, there are instances where ties are not reciprocal and are recorded accordingly.

As one can imagine, when working with very large networks, recording network data in matrix form can prove challenging and is why social network analysts often turn to other methods when working with large networks. For our purposes here, however, we focus on recording data in matrix form.

Aggregating (Combining) and/or Parsing Networks

Actors are typically involved in more than one type of relation (Hanneman and Riddle 2005). For example, most individuals are embedded in a number of different types of ties, such as friendship, kinship, and economic. Business organizations are no different. They engage in financial and informational exchanges and sometimes form alliances with one another (Saxenian 1994). The same is true with countries. They are explicitly linked through numerous cultural, economic, military, and political ties, and implicitly linked through ties created by transnational corporations, nongovernmental organizations, and international agencies (Meyer et al. 1997). Such multiplexity is important because ties often pull actors in different directions (Simmel [1908, 1922] 1955). For example, our work ties may push us in the direction of making one choice, while our friendship and kinship ties may pull us in another. This suggests that if we want a more accurate picture of a network's dynamics, we often need to combine a number of different relationships before we analyze them. "Indeed it is a basic assumption of those subscribing to the network approach that

[9] Because marriage ties are reciprocal, a "1" not only appears in the Acciaiuol-Medici cell, but also in the Medici-Acciaiuol cell.

	1 ACCIAIUOL	2 ALBIZZI	3 BARBADORI	4 BISCHERI	5 CASTELLAN	6 GINORI	7 GUADAGNI	8 LAMBERTES	9 MEDICI	10 PAZZI	11 PERUZZI	12 PUCCI	13 RIDOLFI	14 SALVIATI	15 STROZZI	16 TORNABUON
1 ACCIAIUOL	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
2 ALBIZZI	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0
3 BARBADORI	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
4 BISCHERI	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0
5 CASTELLAN	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0
6 GINORI	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7 GUADAGNI	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	1
8 LAMBERTES	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
9 MEDICI	1	1	1	0	0	0	0	0	0	0	0	0	1	1	0	1
10 PAZZI	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
11 PERUZZI	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0
12 PUCCI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13 RIDOLFI	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
14 SALVIATI	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
15 STROZZI	0	0	0	1	1	0	0	0	0	0	1	0	1	0	0	0
16 TORNABUON	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0

Figure 2.1. Marriage Ties among Renaissance Florentine Families

behavior cannot be explained in terms of any one single activity" (Breiger 1975, cited in Azarian 2005:39).

This, of course, raises questions of strategy and the manipulation of social network data. For example, if we want to disrupt a dark network's financial operations, we may choose to aggregate actors' financial ties (e.g., ties of financial flows between actors) and their affiliations with institutions that provide financial support to the dark network (e.g., businesses, criminal activities, and/or charities and foundations acting as a financial front to the network). But what if a network's financial operations rely heavily on ties of trust between actors? Then we may want to combine these ties with friendship, kinship, and religious ties, or we may want to first analyze only the network's financial ties and then add the friendship and kinship ties for additional analysis. The aggregation of networks is not the only option open to us, however. Sometimes we may want to parse them, seeking to identify actors who participate in two or more networks of interest (or actors who are active in a particular network and share one or more common attributes). For example, we may be interested in mapping the network of individuals who are involved in both the financing and operations of a particular dark network but not just one or the other. Obviously, there are no clear-cut answers as to how and which networks to aggregate or parse. Such decisions have to be made on a case-by-case basis.

Analysis and Interpretation

Social network metrics play an important role in analyzing a social network's dynamics. Analysts generally use a variety of metrics (rather than just one or two) in their attempts to gain an overall understanding of a network. Metrics are not the only tool available to social network analysts, however. Network visualization is another helpful tool that can help us see patterns that may not be readily apparent by simply looking at tables of metrics (Brandes, Raab, and Wagner 2001; Castilla et al. 2000; Freeman 2000). For example, a visualization that highlights the centrality of actors in a network may better illuminate the degree of variation among actors than a corresponding table of centrality metrics. Little variation could lead analysts to conclude that it makes little sense to pursue a kinetic targeting strategy because there are several high-value targets. Or, sometimes, clustering algorithms provide multiple "solutions" as to the identity of different subgroups within a network, and often the only way to decide between the various alternatives is through network visualization. In short, metrics and visualization are complementary parts of the SNA toolbox. Most SNA programs either come with network mapping algorithms (e.g., Pajek, ORA) or integrate with network visualization programs that do (e.g., UCINET and NetDraw).

Part of our analysis involves interpreting what we have found. We need to ask questions such as:

- What is the network's overall structure? Does it exhibit any characteristics (e.g., density, centralization, cohesion, fragmentation) that might suggest whether it is more or less effective than other networks?
- Are there some relations that appear to be more constitutive to the network as a whole than others (e.g., school ties)? If so, is it possible and desirable to exploit the network at a different level (e.g., the school network)?
- Are there any subnetworks within the larger network? Do some appear more critical or central than others? If so, can they be exploited (e.g., set them at odds with one another)? Can other more peripheral subgroups be targeted for rehabilitation campaigns or infiltration?
- Are there key actors or ties between actors whose removal or isolation (e.g., by being discredited) will render the network less effective? If so, is it feasible to remove or isolate them? Could there be any second-order effects (e.g., causing the network to become more violent, generating hostility among the surrounding community) in pursuing such a policy?
- Do some actors hold structurally equivalent positions in the network with other actors? Since such actors are essentially substitutable for one another, this could indicate potential emergent leaders. That is, when a particular actor is removed, there is a strong probability that they will be replaced with a structurally equivalent actor. This could help identify a particular strategy's second-order effects.
- Are there key actors who could be targeted for the diffusion of misinformation (i.e., a deception campaign) or monitored in order to improve our knowledge of the network?
- Are there peripheral actors that could possibly be enticed to leave the network, making it more vulnerable to disruption or isolation?
- Are there organizations within the network (e.g., schools, businesses, faith communities) that are attractive targets for infiltration or removal?
- How has the network changed over time? What have previous research and case studies told us about how dark networks adapt to exogenous and endogenous shocks?
- Does a spatial analysis of the network yield different insights as to which actors are central and how the network has adapted over time?

- Have we adequately separated genuine from spurious correlations?

Needless to say, the answers we give to these questions and others inform the strategies we craft and the policies we recommend.

Crafting Strategies

At this point it is time to reevaluate our original hypotheses to see whether they need amending in light of what the exploratory analysis and interpretation of the network yielded. Following Admiral Olson's observation that kinetic action is merely "a holding action that buys time for" nonkinetic approaches to have their effects" (quoted in Roberts and Everton 2011:4), we may seek to implement a combination of kinetic and nonkinetic strategies. Or, if General Flynn is correct that kinetic attacks sometimes multiply enemies rather than decrease them (Flynn, Pottinger, and Batchelor 2010:8), we may only consider nonkinetic strategies that will take longer to implement but may yield better results. The broader point is that SNA provides various ways of teasing out the nature of dark networks, which in turn provides us with valuable information as to what strategies may best disrupt them.

2.4 Summary and Conclusion

This chapter has focused on the role that social network analysis should play in the crafting of strategies for the disruption of dark networks. It began with a discussion of the various strategic approaches and then moved to a brief overview of how to use SNA in conjunction with the crafting of strategies. Its goal was to illustrate how SNA can be useful for the crafting of strategic options within the kinetic and nonkinetic approaches.

That said, it recognizes that the use of SNA for such a purpose has its challenges. Three are worth mentioning. As noted in the preface, data on insurgencies and terrorists can be difficult to collect and are often incomplete (Borgatti, Carley, and Krackhardt 2006; Krebs 2001; Sparrow 1991), meaning that analysts have to use caution when crafting strategies. Another is that critics have challenged the use of SNA for military purposes, in particular the use of SNA for targeting purposes (Gjelten 2010). This book shares these concerns and addresses them in more depth in Chapter 12. For now it is sufficient to acknowledge that, as previously noted, not only may lethal targeting increase, rather than reduce, the level of violence, an emphasis on kinetic operations often neglects or minimizes the use of SNA for rebuilding and rehabilitating purposes. Finally,

the use of SNA to generate strategic options should not be confounded with its use for decision making. The latter depends on a whole host of issues – knowledge of context and local culture, and the assessment of risks, costs, and potential for unintended consequences, just to name a few (Moody 2005). SNA should not be seen as a silver bullet or substitute for other critical elements in the decision process. It certainly can inform decisions, but it should not determine them. That is why this book emphasizes the use of SNA for the *crafting* of alternative strategies for countering dark networks, not their selection.