

Disrupting and Dismantling Dark Networks: Lessons from Social Network Analysis and Law Enforcement Simulations

David A. Bright

Researchers using social network analysis have documented the structure of criminal organizations and groups, and have used existing methods and metrics to identify key actors in dark networks (e.g., degree and betweenness centrality). SNA measures focus on the connectivity or relationships between actors. However, actors in dark networks may be key for reasons unrelated to their connectivity. For example, they may play important roles such as obtaining critical resources. The removal of key actors is one strategy that may be used to disrupt and dismantle dark networks, and computer simulations have been used to evaluate the impact of arrests and other law enforcement interventions that seek to mitigate the efficacy of criminal organizations. This chapter assesses the value of such computer simulations and concludes that they offer valuable, if imperfect, insights into the structure and function of illicit networks.

I. The Role of Research and the Science of Dark Network Disruption

While law enforcement agencies utilize SNA methodologies to identify potential targets for surveillance and arrest, researchers across diverse disciplines including the social sciences, mathematics, and computer science study dark networks to develop understandings of their social structure and organization. Researchers have examined many different types of dark networks, including groups involved in price fixing in corporations (Baker & Faulkner, 1993), drug trafficking groups (Morselli & Petit, 2007; Bright, Hughes, & Chalmers, 2012), and terrorist groups (e.g., Krebs, 2002a, 2002b; Rogriguez, 2005; Koschade, 2006; Perliger & Pedahzur, 2011; Harris-Hogan, 2012). Much of this work has focused on descriptions of the structure of dark networks and the identification of key actors.

The results of such research have implications for identifying areas of strength and vulnerability of dark networks. For example, which actor or set of actors should be targeted in order to dismantle and disrupt dark networks? Everton (2012b) has identified two main tasks for researchers interested in investigating strategies for network disruption: (1) exploratory SNA, which includes visualization (mapping) of dark networks; and (2) testing hypotheses (e.g., the predicted impact of law enforcement strategies) using mathematical algorithms to represent abstract parameters (e.g., roles or attributes of actors) and probabilities (e.g., of node removal). Many studies on dark networks have focused on the first, but few have addressed the second.

It is important to note that although SNA and computer simulations can shed light on the effectiveness of specific law enforcement strategies for dismantling dark networks, SNA cannot be a complete replacement for law enforcement decision making. The selection of an appropriate law enforcement strategy requires broad information about the specific context and an assessment of risks and costs, including the potential for unintended consequences (Everton, 2012b; Gerdes, 2014). Although SNA can guide decision making, it cannot be used as the sole determination of law enforcement strategies. Nonetheless, strategies to disrupt and dismantle dark networks can be informed by a consideration of potential strengths and weaknesses of dark networks research.

Before discussing these attributes, it is necessary to first define some important terms. A “hub” is a node or actor with a great many connections relative to other actors in the network. Network “disruption” refers to the disruption of the activities of the network, as occurs when the arrest of a chemical supplier restricts the manufacturing capacity of a methamphetamine production ring. “Dismantlement” and “fragmentation” are purely structural outcomes that refer to the removal of nodes and/or links from the network resulting in disconnected subgroups and isolated nodes. Although distinct, the concepts are related because dismantling a network is likely to produce disruption, ostensibly when some threshold of fragmentation is realized.

II. Strengths and Weaknesses of Dark Networks

A number of inherent strengths and weaknesses are apparent in dark networks (Williams, 2001; Kenny, 2007; Eilstrup-Sangiovanni & Jones, 2008; Morselli, 2009). Law enforcement agencies must consider these strengths and weaknesses in the design of interventions against dark networks. First, network structure, with branching connectivity across actors, facilitates the flow of information, knowledge, and skills, and the exchange of tangible resources such as drugs, money, and weapons.

Second, social networks have a flexible and dynamic quality that permits the rapid change and responsiveness to threats and risks. Third, network structure facilitates the operation of groups in illicit markets by allowing actors to remain hidden, sometimes even from each other. Fourth, networks provide an optimal structure for the pooling and exchange of resources needed for the commission of crimes that require multiple sequences of activities. Fifth, networks can be self-organizing, and require no central governing authority. Sixth and finally, network actors can “learn” (e.g., about law enforcement strategies) and can pass this learning through the network both spatially and temporally.

On the flip side, dark networks also suffer weaknesses or vulnerabilities, some of which law enforcement agencies can capitalize on in their attempts to dismantle and disrupt dark networks. First, dark networks must strike a balance between efficiency and security (Morselli, Giguère, & Petit, 2007), so an increase in efficiency is likely to result in a countervailing reduction in security. Second, the size of dark networks is restricted because of the level of trust usually required (Gambetta, 2009). Networks that grow too large may compromise the capacity to screen network members and therefore facilitate infiltration by informants, intelligence officers, or undercover officers. Third, highly central nodes may be focal points of power and influence, but they are also highly visible to law enforcement agencies and are therefore vulnerable (Morselli, 2010). Fourth, without any central authority or leadership, the group may be rudderless, leading to inefficiencies and errors. Finally, because of the interconnectivity across actors, removing (e.g., arresting) one actor can bring down a whole network like a house of cards, as law enforcement follows the connections between actors. This final weakness of dark networks has been the focus of attempts to dismantle and disrupt such networks.

There is emerging evidence that dark networks are scale free in structure, and therefore vulnerable to law enforcement interventions that target hubs (Xu & Chen, 2009; Keegan et al., 2010; Bright, Greenhill, & Levenkova, 2014). In scale-free networks,¹ the majority of nodes have proportionately few links, while a small proportion of nodes are “hubs” with a very large number of links. Structural connectivity in scale-free networks is maintained by these highly connected hubs, whose removal can drastically impact network topography. This feature of scale-free networks renders them somewhat resistant to random removal of nodes because probability dictates that such random removal is more likely

¹ Networks can be of several types, including random (exponential), small world, and scale free. For more discussion of types of networks, see Bollobas, 1985; Barabasi, Albert, & Jeong, 1999; Barthelemy & Amaral, 1999; Barabasi & Bonabeau, 2003; Bollobas & Riordan, 2004.

to eliminate less well-connected nodes. In contrast, the simultaneous removal of only a few hubs can quickly lead to network fragmentation.

III. Simulation Studies: Dismantling Dark Networks by Targeting Hubs

SNA and computer modeling have been used to test the effectiveness of law enforcement interventions at dismantling and disrupting dark networks. Although somewhat simplistic compared to the complexity inherent in the real world, simulation research can provide evidence about the relative effectiveness of different types of law enforcement interventions. Researchers running law enforcement simulations should consider four main points:

- *Data source* – Simulation research using real-world data must overcome one of the main challenges confronting researchers in the dark networks field: access to the data. The collection of complete “real world” data sets on dark networks is difficult. For example, interviews with participants in illicit markets are fraught with ethical, legal, and safety concerns, trial transcripts cost money, and access to law enforcement data usually involves lengthy approval processes (Bright et al., 2012). Hypothetical or simulated data sets are a viable alternative, but suffer from lower construct validity compared with the collection of real-world criminal justice data.
- *Selection of law enforcement interventions* – Law enforcement simulations can range from simplified strategies (e.g., target the most connected actors in sequential order) to more complex realistic scenarios such as targeting actors involved in exchange of key resources, seizures and arrests, and the insertion of undercover officers.
- *Simulation studies must specify outcome measures for network disruption and dismantlement* – Measures of disruption used in previous research include accuracy of a decision task (e.g., Carley, 2006). Measures of dismantlement include the proportion of actors in the largest connected component in the network, the average size of remaining connected components, and the number or proportion of nodes that are isolated from other actors. Alternatively, analysts can formally calculate “fragmentation,” which Borgatti (2006) defines based on the sum of the reciprocals of distances between all actors in a network. Pre- and post-measures of dismantlement variables offer one approach to quantify the efficacy of particular law enforcement strategies.

- *Dark network adaptation* – Dark networks will change or evolve across time in response to shifting market conditions and law enforcement pressure and interventions (Morselli & Petit, 2007; Bright & Delaney, 2013). Eilstrup-Sangiovanni and Jones note that “a fluid structure is said to provide networks with a host of advantages including adaptability, resilience, and capacity for rapid innovation and learning, and wide scale recruitment” (2008, p. 8). Dark networks will recruit new members as needed, sometimes to replace actors who have been arrested, or to gain access to particular skills and knowledge. Given the dynamic nature of networks, it is reasonable to expect that networks will respond to law enforcement interventions in an adaptive fashion, for example by replacing actors removed/arrested.

Research using law enforcement simulation methodology has addressed each of these four issues in different ways. Some research has not incorporated network adaptation, preferring instead to simplify the simulations by setting adaptive complexity aside. For example, Xu and Chen (2003) used simulation methodology to examine terrorist, methamphetamine trafficking, and gang networks. After concluding that these networks exhibited scale-free structure, the researchers conducted two simulations. The first removed nodes with high degree centrality (hubs) sequentially; the second removed nodes with high betweenness centrality (brokers) sequentially. Three outcome measures served to assess efficacy: (1) the fraction of nodes remaining in the largest connected component following each removal, (2) the average size of the remaining components following each removal, and (3) the average path lengths in the network following each removal. Xu and Chen (2003) concluded that targeting either hubs or brokers was an effective means to degrade network structure, but found strategies that emphasize brokers over hubs more efficient.

Similarly, Keegan and colleagues (2010) examined the resilience of an on-line gaming network (a proxy for an illicit network) and a drug trafficking network derived from criminal justice data. They compared the removal of nodes in random order with sequential removal of nodes by degree centrality scores. Outcome measures used were the proportion of nodes in the largest remaining connected component and the proportion of the network that was isolates. While removing the top 5 percent of nodes as ranked by degree centrality effectively dismantled the networks, removing 5 percent of nodes chosen at random failed to yield comparable results.

Bright, Greenhill, and Levenkova (2010) applied a computer simulation approach to two case studies of drug trafficking networks to evaluate the impact of law enforcement interventions focused on the removal

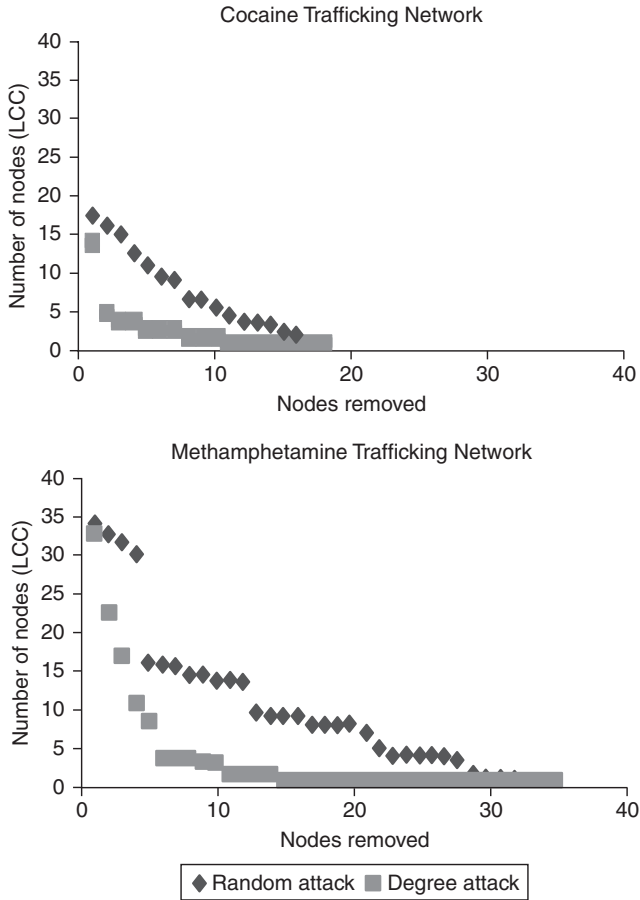


Figure 3.1. Number of nodes in largest connected component.

of hubs. The real-world data was extracted from criminal justice sources. The researchers adopted a design similar to Keegan’s and conducted simulations that removed nodes at random, as well as separate tests that removed nodes sequentially based on degree. Outcome measures were the number of isolates and the number of nodes in the largest remaining connected component. As Figures 3.1 and 3.2 show, removal of hubs reduced the size of the largest connected component more rapidly and produced more isolates than random node removal in both test networks. Thus, this study supported the findings of previous research, which suggest that law enforcement interventions can trigger the structural collapse of dark networks by removing well-connected actors – a finding that we would expect if dark networks are indeed scale free.

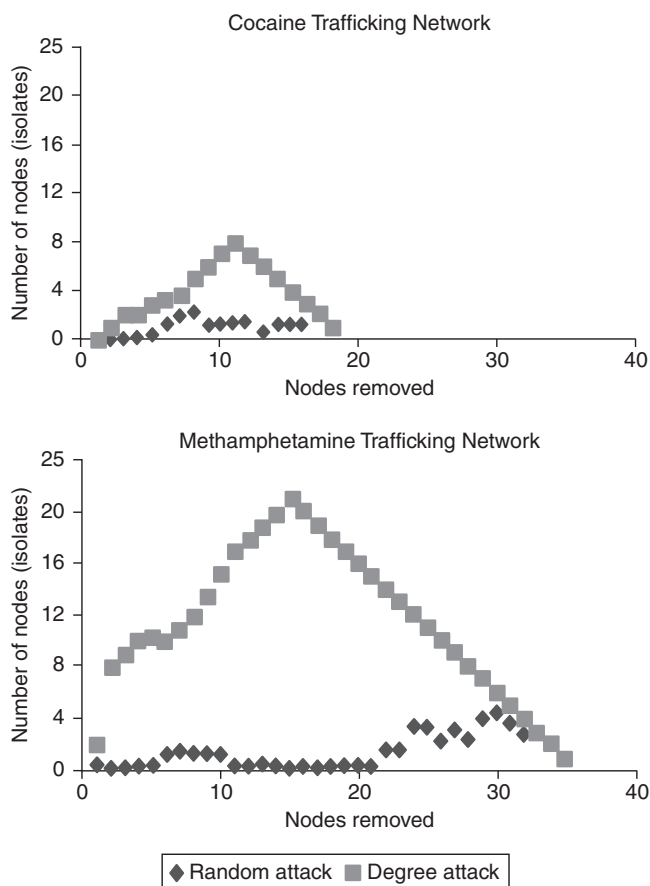


Figure 3.2. Number of isolates.

However, the simulations and the centrality measures that underlie them only consider agents' structural characteristics, and leave aside their intrinsic attributes (Robins, 2009; Schwartz & Rouselle, 2009). This assumption is unrealistic because actors in dark networks often possess a range of characteristics or play particular roles that are critical to the commission of illicit activities, but that may be unrelated to centrality scores. For example, Bright and colleagues (2012) identified seven roles played by actors in methamphetamine trafficking networks (see Table 3.1). Similarly, Mancuso (2014) identified six functional roles in Nigerian sex trafficking networks, and in terrorist networks, some actors may have critical skills in bomb making, or detailed knowledge of ideology. Gerdes (2014) argues that extremist groups may sometimes deliberately insulate such individuals from the broader group in the interests of

operational security. Thus, across different types of dark networks, some actors may have intrinsic characteristics that make them more likely to assume leadership roles (Carley, 2006b; Carley, Reminga, & Kamneva, 1998), and centrality scores may not always accurately characterize such individuals' importance. Some key nodes are likely sparsely connected to the remainder of the network.

IV. Actor-Level Characteristics Versus Centrality Scores

Given that law enforcement agencies are interested in the most cost-effective allocation of their resources (e.g., for surveillance and arrest), should targeting efforts focus on the most connected actors, on the actors who play critical roles, or actors who are both well connected and play critical roles? Some scholarship has addressed this question. For example, Carley (2006) used simulation to compare three strategies aimed at disrupting dark networks: removal of central actors, removal of emergent leaders, and random removal. The outcome measure was accuracy in a simulated decision task, in which impaired performance indicates network disruption. Although the networks proved difficult to disrupt, the research suggested that removing emergent leaders produced the largest effect.

Bright and colleagues (2014) conducted four different law enforcement simulations in which actors were removed as though they were being arrested by law enforcement agencies. The four simulated interventions were: (1) sequential removal of the nodes that ranked highest in degree centrality; (2) sequential removal of nodes who played important functional roles in the network; (3) sequential removal of nodes based partly on centrality scores and partly on the roles played by actors; and (4) the random removal of nodes. In these simulations, the impact on the network was measured in two ways: the first was a purely structural measure, namely a count of the number of nodes in the largest component, and the second measure combined structural and functional factors into a "disruption function" that measured the number of nodes in the largest remaining connected component in combination with a measure of these nodes' role-based importance in the network.

The disruption function takes high values when the network remains well connected *and* contains actors who play relatively important roles. As Table 3.1 summarizes, the function weights each node by the inverse of the number of actors who performed the same role. For example, there were two managers, so they each received a weighting of 1/2. There were seven wholesale dealers, so each of them received a weighting of 1/7. Bright and colleagues (2014) assumed that more specialized roles were

Table 3.1. *Role-based weightings*

Role	Nodes with that Role	Nodal Weight
Manager/Assistant Manager	K18, K28	1/2
Possession of specialist skills	K10, K36	1/2
Clan lab “branch manager”	K12, K24, K31	1/3
Corrupt official	K33, K34, K35	1/3
Wholesale dealer	K1, K13, K15, K23, K26, K27, K32	1/7
Resource provider	K5, K6, K7, K8, K9, K11, K14, K22	1/8
Worker/“labourer”	K2, K3, K4, K16, K17, K20, K21, K25, K29, K30	1/10
Unknown role	K19	0

Source: From Bright et al., 2014.

less numerous in the network, and that such roles would be higher in demand and lower in supply in the broader illicit market for personnel. Weightings, therefore, served as proxies for the importance of the role and for difficulty illicit networks might encounter if they needed to replace individuals lost to death, arrest, and other forms of personnel turnover.

Figure 3.3 shows that random targeting was relatively ineffective, while the most effective strategies were the removal of nodes by degree centrality and the mixed strategy (centrality and role weighting). For the purely structural approach depicted in the figure’s upper panel, the degree and mixed strategies showed similar performance, and both outperformed targeting by role weights alone and random targeting. For the disruption measure depicted in the figure’s lower panel, the best performance was again attained by both the degree strategy and the mixed strategy. Random targeting was the most ineffective strategy. Targeting based solely on role weights again occupied the middle ground; it did worse than either the degree-based or mixed strategies, but better than the random approach.

Overall, these findings support the conclusions of studies that adopt a purely structural approach. Although law enforcement agencies receive marginal benefit by considering role weights in combination with measures of nodal centrality, the performance differences between the “mixed” and degree-based approaches were negligible. Any approaches that neglect to consider centrality scores are, however, unlikely to succeed. Attempts to disrupt the network by simply removing managers and specialists did not perform especially well.

Much of the research on dismantling and disrupting dark networks neglects to incorporate network dynamics and the illicit organizations’

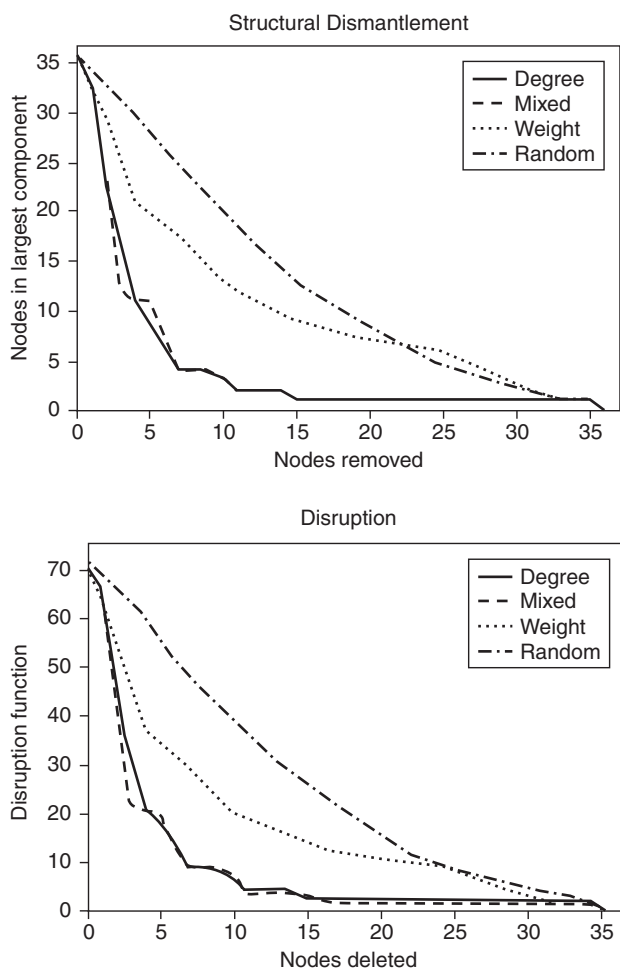


Figure 3.3. Outcome measures for four law enforcement simulations (Bright, Greenhill, & Levenkova, 2014).

propensity for organizational learning. Too many researchers assume that, aside from the loss of nodes, criminal networks remain static in the face of multiple, sequential arrests of members. While such assumptions render the simulations easy to run and interpret, overly static models lack construct validity and generalizability. The next section, therefore, describes efforts to utilize dynamic network analysis (DNA) (Carley et al., 1998; Carley, Lee, & Krackhardt, 2002; Carley, 2006a) and other similar approaches to model dark networks' ability to adapt to law enforcement interventions.

V. Network Dynamics and Adaptation

Research in dynamic network analysis (DNA) dates to at least 1998, when Carley and colleagues first used the accuracy of decision making – a non-structural variable – to measure the effects of structural interventions on networks. This research found covert networks with cellular organizational structures both difficult to disrupt and very adaptive. Subsequent research by Tsvetovat and Carley (2003) simulated interactions between law enforcement and terror groups. Specifically, the law enforcement group used knowledge about the terrorist group to select actors in that group for removal or isolation. Dark network performance on decision tasks remained relatively stable, despite the removal of key actors. Other actors quickly moved in to fill the vacated roles, thereby allowing the simulated terror group to adapt to a targeted decapitation campaign.

While the paucity of real-world data on dark networks has restricted the number of longitudinal assessments of adaptation in criminal networks, a handful of noteworthy studies rely on over-time data obtained from criminal justice sources in lieu of the simulated data underlying the work of Carley and her collaborators. For example, Xu, Marshall, Kaza, and Chen (2004) examined the stability of two dark networks across time and found changes at both the actor level and the global network level. Group density and cohesion for both networks increased across time. The centrality scores for one of the leaders fluctuated. Specifically, closeness centrality increased, while degree and betweenness decreased, suggesting that it became easier for him to connect with other actors in the network while maintaining few direct connections and therefore being less visible to law enforcement.

In another study on network dynamics, Helfstein and Wright (2011) examined structural change in a terrorist network over time. They concluded that the connectivity of network actors became denser across time, with an increased number of links between actors over time, probably as a reflection of the need for increased collaboration as an attack date loomed. Iwanski and Frank (2014) examined the evolution of a co-offending network of drug offenders and found somewhat contradictory results. The co-offender network initially showed tightly knit clusters of offenders involved in the same crime type, but this clustering became less prominent over time, even though the clusters were actively involved in recruiting new, younger offenders into the network.

Morselli and Petit (2007) examined a drug trafficking network that was under law enforcement surveillance for two years. Because law enforcement seized illicit drug imports but made no arrests until the end of the investigation period, this operation provided the conditions to study the network's responses to general pressure from law enforcement, rather than targeted decapitation. Initially, betweenness and degree

centralization were 80 percent and 70 percent, respectively, but after the first seizure these statistics dropped to 44 percent and 30 percent, suggesting that drug confiscation caused the network to become less centralized around a few well-connected actors.

Law enforcement's actions also precipitated changes in centrality scores for some actors. For example, as one actor's degree and betweenness score decreased across time, the scores for two other actors increased. As law enforcement continued to seize drug shipments, the influence and authority of the first actor waned, and the influence of the latter two waxed, suggesting that power shifted in the network directly because of the law enforcement interventions. Thus, illicit organizations respond adaptively to law enforcement interventions other than node removal through arrest.

A study by Bright and Delaney (2013) documented changes in a criminal network across an eight-year period divided into four two-year time periods (T1–T4). Network density remained relatively stable across the first three time periods (12–16 percent), but then increased in the fourth time period as the result of a shift toward securing financial profits and away from security. Between T3 and T4, the network expanded its involvement in wholesale and retail distribution of illicit drugs, reflecting attempts to increase sales and profit at greater risk of discovery.

This study also documented changes in centrality scores and roles. For example, one actor was connected to less than 5 percent of the network at T1, but to more than 70 percent of the network by T4. In contrast, one actor who was initially central and held direct ties to more than 50 percent of the network at T1 was connected to less than 10 percent of the network by T4. These patterns suggest significant changes in the power and authority in the network across time, and may reflect the shift from a small network focused on methamphetamine distribution within a close group of friends, to a larger, profit-motivated network.

Similarly, network members' roles evolved in response to law enforcement's efforts. For example, at T1 a large number of actors supplied their private residences as clandestine methamphetamine production laboratories. These homes initially offered a reasonably secure location for drug production, but when law enforcement discovered some of the labs, investigative attention on residential areas intensified, causing members of the production ring to move their remaining manufacturing facilities to isolated bush lands free from law enforcement surveillance. Because of these changes, "premises suppliers," a common role in the network at T1 and T2, were nearly absent from the network by T4.

Some actors were recruited to the network specifically because they could provide access to particular resources. For example, following law enforcement interventions that attenuated stocks of precursors, there was a pressing need to access alternate precursor chemical supplies.

In response, an individual was recruited into the network specifically because he could obtain large amounts of a precursor chemical.

When viewed in aggregate, the studies described in this section suggest that criminal networks evolve and change over time in response to a wide assortment of factors. Market dynamics, law enforcement interventions, and organizational learning among members of dark networks all have the potential to trigger adaptation. Moreover, networks recruit new actors to replace lost personnel, causing changes in actor connectivity over time, as well as shifts in agents' functional roles. Criminal networks do not remain static, and do not simply stand still as law enforcement interventions play out.

VI. Conclusions

In summary, SNA and computer simulations have much to offer the field of dark networks. Researchers have demonstrated the potential of purely structural approaches to intervention, such as node removal through arrest. In static studies, such decapitation strategies performed almost identically to mixed strategies that considered both structural and functional information (e.g., agents' job description), and outperformed both random interventions and mitigation strategies that *only* considered agents' functional roles.

However, the results of dynamic studies that model the adaptability of criminal networks complicate the picture. Carley and colleagues have used simulated data to demonstrate that dark networks quickly adapt to fill any organizational holes left by decapitation strategies. Similarly, the few available longitudinal studies of real-world criminal networks suggest that dark networks undertake a host of adaptations over time and do so in response to market factors and organizational learning, as well as law enforcement interventions.

Moving forward, researchers should synthesize the rigor of Carley and colleagues' simulation-based approach to dynamic network analysis with real-world data. This conclusion speaks to the need for interdisciplinary research, for example, involving computer scientists and criminologists. These efforts should incorporate criminal adaptation, model a range of realistic law enforcement interventions, and investigate the applicability of various outcome measures for disruption and dismantlement. Such research, some of which is presented elsewhere in this volume, holds the key to determining the generalizability of static assessments' conclusions about the efficacy of structurally oriented campaigns of targeted decapitation.