

Target outlet: Illicit Networks Conference 2011

Last modified: September 5 2011 (version 6)

Words: 6478

Word limit: 6000-8000

Dismantling criminal networks: can node attributes play a role?

David A. Bright¹, Catherine Greenhill², Natalya Levenkova²

¹ Drug Policy Modelling Program, National Drug and Alcohol Research
Centre, University of New South Wales

² School of Mathematics and Statistics, University of New South Wales

Correspondence to:

Dr David Bright
Research Fellow
Drug Policy Modelling Program
National Drug and Alcohol Research Centre
UNSW Sydney
NSW 2052
Australia
E: David.Bright@unsw.edu.au
T: +612 9385 0105
F: +612 9385 0222

Abstract

Internationally, there is recognition of the need to more clearly understand drug markets and the criminal syndicates that operate within them, in order to target drug law enforcement interventions in the most effective ways. The current project aims to fill some of the gaps in knowledge about the structure of drug trafficking networks using SNA, and to evaluate the impact of different types of law enforcement interventions directed at drug trafficking networks. We build on earlier work in which judges' sentencing comments were used to build a network map of a drug trafficking syndicate which operated in Australia in the 1990s. As well as producing a network map, this study was also able to identify the role that each individual played within the syndicate. We wish to explore the effectiveness of different hypothetical intervention strategies that aim to dismantle the network. First we investigate the structure of the network and show that it shares some properties of scale-free networks. Then four enforcement scenarios will be tested via simulation: (1) interventions which target individuals based on degree centrality; (2) interventions which target individuals based on role, (3) interventions which combine the first two strategies, and (4) random intervention. The results offer some guidance to intelligence and operational law enforcement when determining which individuals to target, and specifically the impact of targeting individuals based on high degree centrality and roles within the networks, as compared with a baseline (random) intervention.

Criminal groups involved in the trade of illicit commodities (e.g., drugs, arms, people) and in terrorist activities contribute to health and social harms in the Australian and international communities. Internationally, there is growing recognition of the need to more clearly describe the operation of criminal networks, and to empirically investigate the effectiveness of law enforcement strategies aimed at dismantling criminal networks.

Particularly since the 2001 terrorist attacks in New York, there has been a growing focus in law enforcement and research communities on conceptualising criminal groups as networks. The shift to thinking about criminal groups as networks promises to improve our understanding of such groups and enhance law enforcement interventions. In particular, the effectiveness of law enforcement interventions against criminal networks may be improved by research which describes the structure of such networks, and identifies factors which influence the resilience and vulnerability of criminal networks to law enforcement interventions.

While much network research has focused on the position of nodes within the overall structure of networks (e.g., using centrality scores), some scholars (e.g., Robins, 2009) have argued that network analysis should include information about individual level factors (e.g., skills, attributes, demographics). We will examine a case study of a criminal network using both centrality scores and the roles played by individuals in the network. We will use simulations to investigate different strategies for dismantling the networks, and apply two “measures of disruption” to evaluate the effectiveness of these strategies. The motivation for this work is to explore which factor or combination of factors law enforcement should focus on when targeting nodes with the aim of dismantling the network. The current study adds to the series of strategic cases, against which other cases can be compared. It follows work by

Morselli & Petit (2007) on heroin importation in Canada, and Natarajan (2006) on heroin trafficking and dealing in New York.

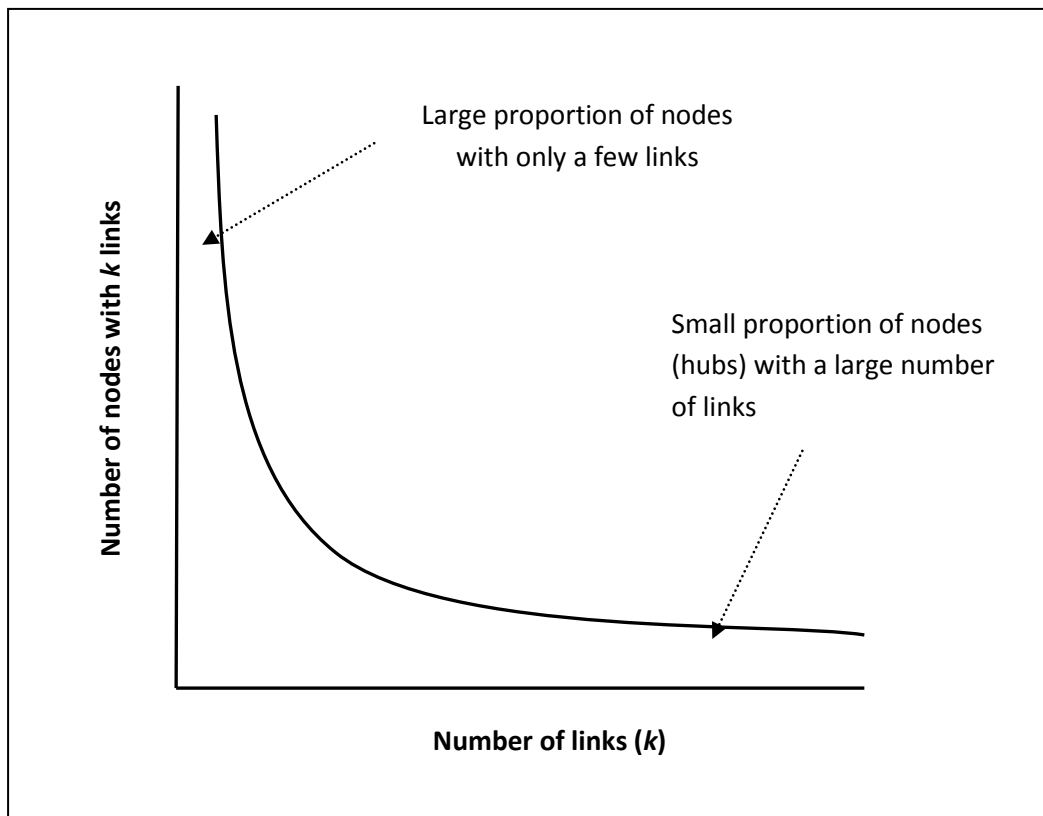
Network structure.

Existing theoretical accounts and empirical results suggest that networks (of any type, where the nodes are students in a school, organic chemicals in cells, or cables in an electricity grid) can be divided into two types: exponential and scale-free (Albert, Jeong, & Barabasi, 2000). Exponential networks (also called Poisson networks) are structurally homogenous, with the majority of nodes having approximately the same number of links. Scale-free networks on the other hand are inhomogenous- the majority of nodes have proportionately few links, and a small minority of nodes have a very large number of links (known as hubs).

In exponential networks, nodes show some variation in the number of links they possess as compared to the average node (i.e., the peak of the bell curve), but it is very unlikely to find nodes with a very much larger or smaller number of links compared with the average node.

In a scale-free network, a plot of the number of links (k) to number of nodes with k links would follow a “heavy-tailed” distribution: many nodes have a small number of links (the left of the graph) and a few have a very large number of links (the right of the graph).

Figure 1: Nodes and links in scale free networks.



Examples of scale-free networks include the world wide web, the physical structure of the internet, metabolic processes in cells, and (at least some) social networks. For example, sexual relationships in Sweden (Liljeros, Edling, Amaral, Stanley, & Aberg, 2001), networks of people connected by email (Ebel, Mielsch, & Bornholdt, 2002), and networks of scientific papers connected by citations (Redner, 2005) have all been shown to be scale-free networks.

Implications of scale-free structure for network vulnerability.

Scale-free networks with heterogeneity in degree distribution imply that network connectivity is maintained by a few highly connected hubs whose removal can drastically alter network topography. These hubs are typically on many of the paths between other pairs of nodes in the network. The structure of scale free networks make them resistant to accidental or random failure (Albert, et al., 2000; Bollobas & Riordan, 2004; Crucitti, Latora, Marchiori, &

Rapisarda, 2003). This is because the random removal of nodes will take out mainly less connected ones because they are far more numerous. The elimination of nodes with few connections will not exert a large impact on network topography. However, the simultaneous removal of only a few hubs (representing a small proportion of the entire network) can collapse an entire networked system (Bollobas & Riordan, 2004; Newman, 2010).

While in many areas (e.g., internet topography, World Wide Web networks) the focus is on ensuring resilience, in the study of criminal networks, real world policy implications flow from identifying areas of weakness which can be exploited by law enforcement agencies. Despite the implications for the vulnerability of criminal networks to law enforcement interventions, there has been very little previous research on dismantling criminal networks. Morselli & Petit (2007) evaluated the impact of a surveillance and seizure operation on a drug trafficking network. The project evaluated the impact of this intervention on network structure. By virtue of the type of law enforcement intervention involved, it did not examine the impact of removal of nodes as there were no arrests until the intervention was concluded. Nonetheless, Morselli & Petit (2007) found that over time and law enforcement pressure, the centralization of the network decreased and that one node that was initially highly central became less so over time. As an aside, this research also demonstrated that multiple seizures which imposed large financial losses on the network, and changed the network structure, did not impede the capacity of the network to arrange importations- importations that eventually failed due to the high level of surveillance of the network.

Using simulation methodology, Xu and Chen (2009) examined terrorist, meth trafficking, and gang networks. They found that these networks had scale free properties, and also exhibited characteristics of 'small world' networks (i.e., high clustering compared to random graphs

with the same average degree centrality). They simulated attacks on hubs (nodes with high degree centrality) and attacks on bridges (nodes with high betweenness centrality). Network fragmentation following sequential node-removal was indicated by measuring: the fraction of nodes in the largest connected component, average size of remaining components, and average shortest path lengths between pairs of nodes. They found that both hub and bridge attacks were effective in dismantling the networks; though all three networks were more sensitive to attacks targeting bridges than hubs.

Keegan, Ahmed, Williams, Srivastava, & Contractor (2010) examined the resilience of on-line gaming (1600 nodes) and drug trafficking (110 nodes) networks – and compared random failure with attacks targeted at hubs (i.e., sequential removal of nodes by degree centrality scores). They found that the on-line gaming network had a scale-free structure. As measures of network fragmentation, they used: the fraction of nodes in the largest connected component, and the fraction of nodes which were isolates. They found similar resilience to degree and random attack when fewer than 1% of nodes were removed. However, removing 5% of nodes by attacking hubs fragmented the network; in contrast, the removal of 5% of nodes by random failure did not lead to fragmentation.

One criticism of this previous work is that it does not take into account the attributes of individuals in the networks (e.g., Robins, 2009; Robins & Kashima, 2008). Instead, each node is treated as being identical separate and apart from centrality scores. However, nodes can be critical for reasons unrelated to centrality. For example, they may have exclusive access to resources/knowledge (e.g., chemicals), play crucial roles (managing clan lab site) or be a critical link between the licit and illicit worlds (e.g., baggage handlers, corrupt police). Robins (2009) describes five levels of factors relevant to networks: individual level factors,

dyadic level factors, node positioning network effects, localised network structural features, and global network features. Individual level factors include capacities such as skills, expertise, information and knowledge. Robins argues that network analysis should include not just an analysis of traditional features such as centrality scores, but should also explore features of individuals within the network.

Some previous research has examined the roles of individuals within criminal networks. For example, Natarajan (2006) conducted a “role analysis” of a heroin importation network in addition to more traditional network analyses, finding several roles in the network including retailers, sellers, brokers, and secretaries. Similarly, Bright, Hughes, & Chalmers (in press) used a role analysis of a methamphetamine network, finding several roles including workers, specialists, wholesale level dealers, and managers. However, previous research has not examined the impact on network typology of law enforcement interventions which target nodes based on centrality scores (*node positioning effects* under Robins framework) and/or functional roles performed by individuals in the network (*individual level effects*, according to the framework outlined by Robins). Therefore, the current study will investigate whether, when the aim of law enforcement is to dismantle the network, law enforcement should target individuals based on centrality scores or based on their role in the network, or perhaps some combination of the two.

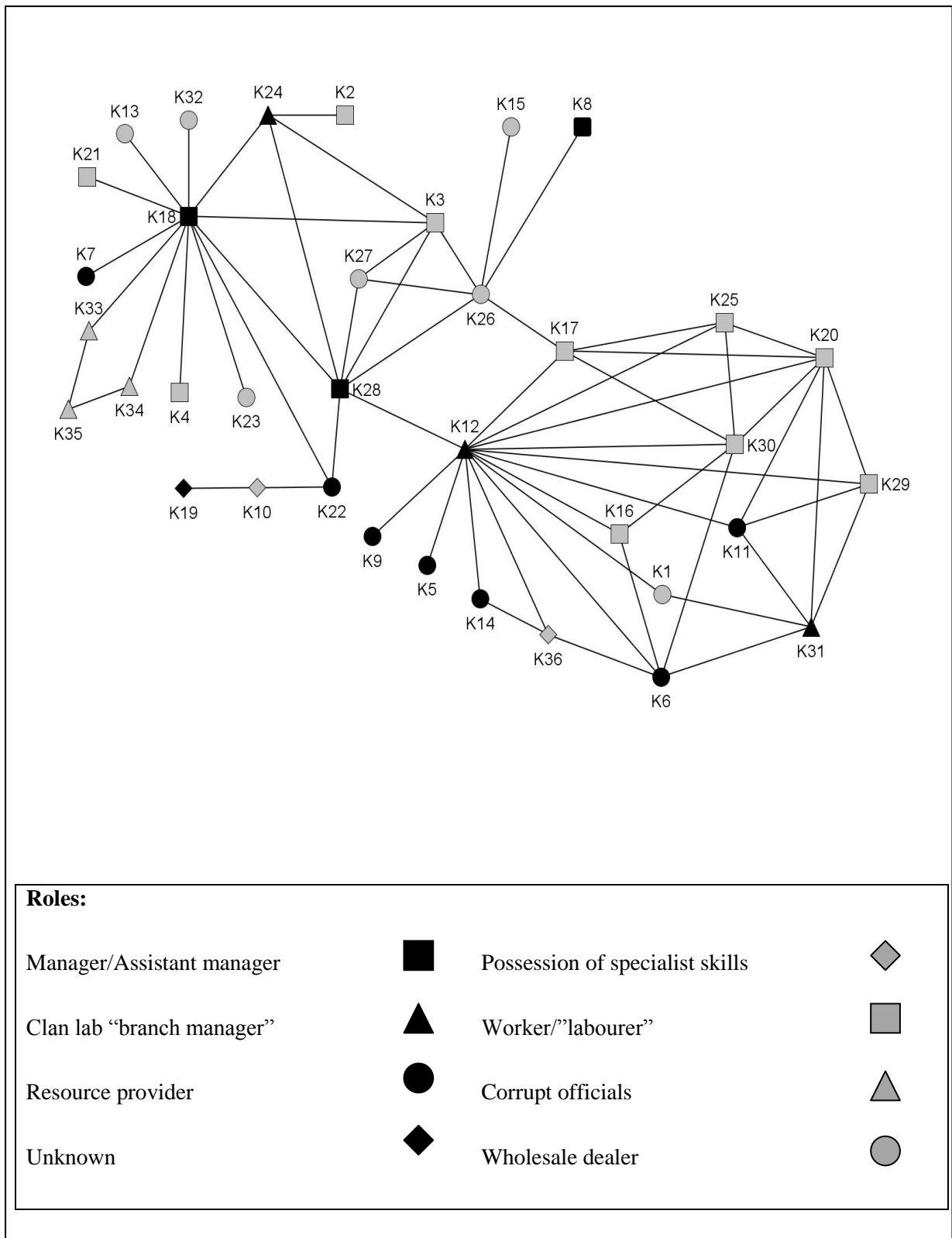
Method

For criminal networks, the collection of complete data sets in realistic contexts is difficult. For example, trial transcripts cost money, and gaining access to law enforcement data there is likely to involve a lengthy approval process. Judges’ sentencing comments offer a viable alternative and we have used this source in previous research on criminal networks (e.g.,

(Bright, Greenhill, & Levenkova, 2010; Bright, et al., in press). In criminal cases, judges' sentencing comments convey the judges' justifications for a sentencing decision. They typically include the name of the person sentenced and a summary of the established facts in the case (behaviours, locations, names, dates) including the names of criminal associates.

For the current study, we used an existing data set described in a previous paper (Bright, et al., in press). The method used to extract and analyse the data was as follows: A search was conducted on the NSW Lawlink website for criminal cases between 1999 and May 1999 using two search terms ("methamphetamine" and "methyamphetamine"). Cases were included if they involved the manufacture and distribution (including importation) of the drug. 61 cases found which met the inclusion criteria. Each case read by one of the researchers (DB). The review resulted in the identification of three groups involved in manufacture/trafficking/importation of methamphetamine. We selected the largest group for further analysis. Eleven cases were identified which made reference to individuals connected with this group. SNA and network mapping was conducted using Visone and UCINET. Previous research using the same data set identified seven roles for 35 of the 36 network members (we did not have sufficient information on one individual, so one node is without a role; Bright, et al., in press). Individuals who designated tasks to others, provided the funds for parts of the drug trafficking operation, or to whom other individuals reported were classified as managers. Individuals who managed the operation of clandestine laboratory sites were designed as clan lab managers; those responsible for selling methamphetamine in single to multiple kilogram lots were classified as wholesale dealers; individuals who sourced chemicals and equipment required for the manufacture of the drug were labelled resource providers; those who possessed specialist knowledge and skill in the manufacture of methamphetamine were labelled specialists; individuals who were paid a wage to complete

Figure 2: Network map of the methamphetamine trafficking network showing roles.



tasks or follow orders were designated workers/labourers; and those who occupied government positions and received bribes to behave in corrupt ways were labelled corrupt officials.

We used two methods to test whether the two networks exhibited scale-free structure: First, we compared mathematical properties of the network to random graph equivalents. And second, we constructed log-log graphs and compared with a line of best fit.

Next, to examine the impact of law enforcement interventions, we conducted four sets of simulations. A computer simulation needs numerical data in order to perform its calculations. Therefore, in order to take the role of each node into account, these roles must somehow be quantified. Our approach to this was to assign a weight to each node, where the weight is inversely proportional to the number of individuals in the syndicate with the same role. Hence the weight measures how difficult it might be to replace that individual, were they to be removed from the network. For example, there are two managers in the network, so they are both assigned a weight of 0.5. There are 10 workers in the network, so they all receive a weight of 0.1. The node with unknown role was assigned a weight of 0. The weights of each node are shown in Table 1.

Table 1: Roles and weights assigned to nodes in the network.

Role	Nodes with that role	Weight of each of these nodes
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

In each simulation, at each time step a node of the current network is chosen according to some rule and deleted from the network. The four different rules we used in the simulations were as follows:

- (1) degree attack, where the node of highest remaining degree centrality score was selected for removal;
- (2) weight attack, where the node with the highest remaining weight was removed from the network;
- (3) a mixed strategy, which is described in more detail below, and
- (4) random attack, where nodes are targeted in a random order.

In the case of a tie (e.g. for maximum degree, or for maximum weight) a node with the maximal value was chosen randomly. We performed 100 runs of each simulation, starting with the methamphetamine network at time 0.

The degree attack and weight attack can be combined to produce a family of mixed strategies. For a given constant c between 0 and 1, we define the score of a node v in the current network to be

$$S(v) = (1 - c) d(v) + c B w(v)$$

where $d(v)$ denotes the degree centrality of node v in the current network, $w(v)$ denotes the weight of node v , and B is a constant chosen so that on average, over the initial network, the two terms make equal contribution. (For the methamphetamine network we used $B = 124/7$.) When $c = 0$ we obtain degree attack, and when $c = 1$ we obtain weight attack. For intermediate values of c we have a combination of the two. We investigated several values of c and found that, for the given network, setting $c = 0.1$ gave the best results. So we only report on the mixed strategy with $c = 0.1$, which is our third strategy.

Although it could be argued that random removal of nodes might simulate “random” law enforcement interventions (e.g., stop and search; border detection), it is better conceived as a baseline comparison for targeted intervention. Random removal is relatively easy as no knowledge of the network structure, is required and if some individuals are hard to locate—with random strategy, any person will suffice as a target (Carley, 2006).

The vulnerability of dark networks to being dismantled by law enforcement can be measured in various ways. In earlier work (Bright, et al., 2010) we investigated the following measures of fragmentation for the degree targeting and random targeting simulations: the number of nodes in the largest connected component, the number of isolated nodes, the maximum degree centrality, and the number of connected components. For each of these measures, degree targeting significantly outperformed random targeting.

In the current study we have chosen to work with two functions. A connected component in a network is a maximal set of nodes such that all pairs of nodes in the set are joined by a path in the network. The first function $n(G)$ is the number of nodes in the largest connected component of the current network G . This measure (and the other fragmentation measures mentioned above) only considers the topological structure of the network, and ignores individual attributes of the nodes, such as role. But we wish to investigate how individual attributes, such as roles, can affect the choice and performance of intervention strategies. Therefore it is desirable, and arguably appropriate, to include role information in our method for measuring the success of the intervention strategies. This led us to investigate another function, which we call the disruption function. For the current network G the disruption function is given by

$$n(G) + K w(G),$$

where $w(G)$ is the maximum, over all connected components, of the sum of the weights of the nodes in that component. Note that the disruption function takes both topological and individual-level data into account. The constant K is chosen so that when G is the initial network, the contribution from both terms is equal. (For the methamphetamine network, this is achieved by setting $K = 36/7$).

For each of our four simulations, both of these measures were calculated after every node deletion in each run, and then averaged over the 100 runs. The values for the four simulations were then plotted together in a graph, for each of the two measures.

Results

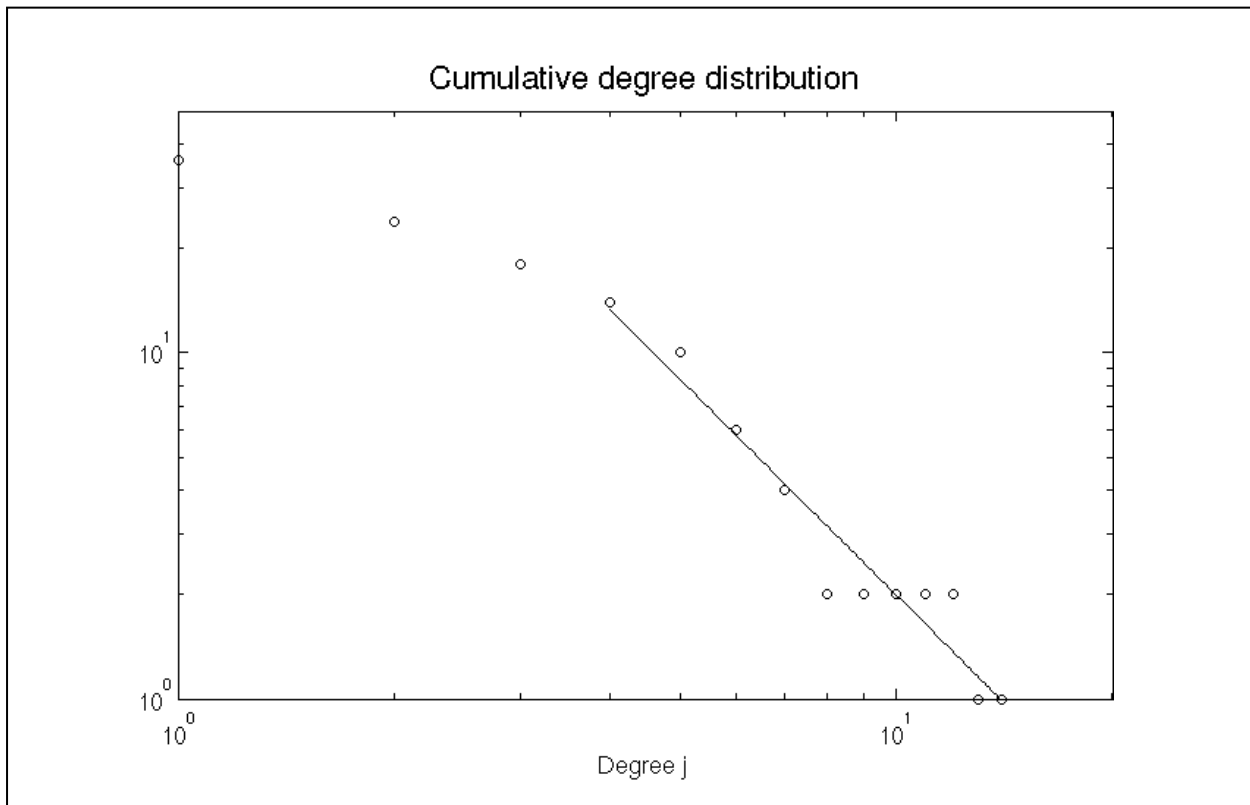
Network structure

One way to examine the mathematical properties of real world networks is to compare them with their random graph equivalents. Random graphs are constructed by making connections between nodes using a pre-set probability p . For example, if $p = 0.5$ then, for each pair of nodes in the network, there is a 50% probability that they will be connected. To produce equivalent random graphs against which to compare our real world networks, the probability is calibrated to give the same average degree in the random graph as for the real world network. In the methamphetamine trafficking network, there were 36 nodes, 62 edges, and an average degree centrality score of 3.444. We used probability $p = 0.09841$ to give the same average degree in the corresponding random graph. The resulting graph is an “exponential network” in the sense of (Albert, Jeong & Barabasi, 1999). In this random graph, the probability that there is a node with degree centrality of 14 is less than 7.6×10^{-5} (less than an 8 in 100 thousand chance), and the probability that there exists a node with degree 14 and a node with degree 12 (as in the real-world network) is less than 3.09×10^{-7} (an approximately 3 in 10 million chance). So the methamphetamine trafficking network was very far from being like an exponential network.

To further test whether the network could be said to be scale-free, we plotted the cumulative degree distribution for the network on a log-log scale and compared the result with a line of best fit. The cumulative degree distribution has points of the form: $(j, \text{number of vertices of degree at least } j)$ where j ranges from 1 up to the maximum degree centrality score of the network. When estimating a line of best fit, we chose to ignore the first three data points. In fact, very few real-world networks display a power-law distribution over the entire degree sequence and researchers usually only claim power-law behaviour for the tail of the degree distribution (that is, for the high-degree nodes). In this case, our aim was to compare the tail of our distribution with a power-law distribution.

Since our network is quite small and there are gaps between the high degrees, the cumulative degree distribution "flatlines" at a couple of places. The reader may form their own opinion as to whether they believe that the data points lie approximately on the given line of best fit.

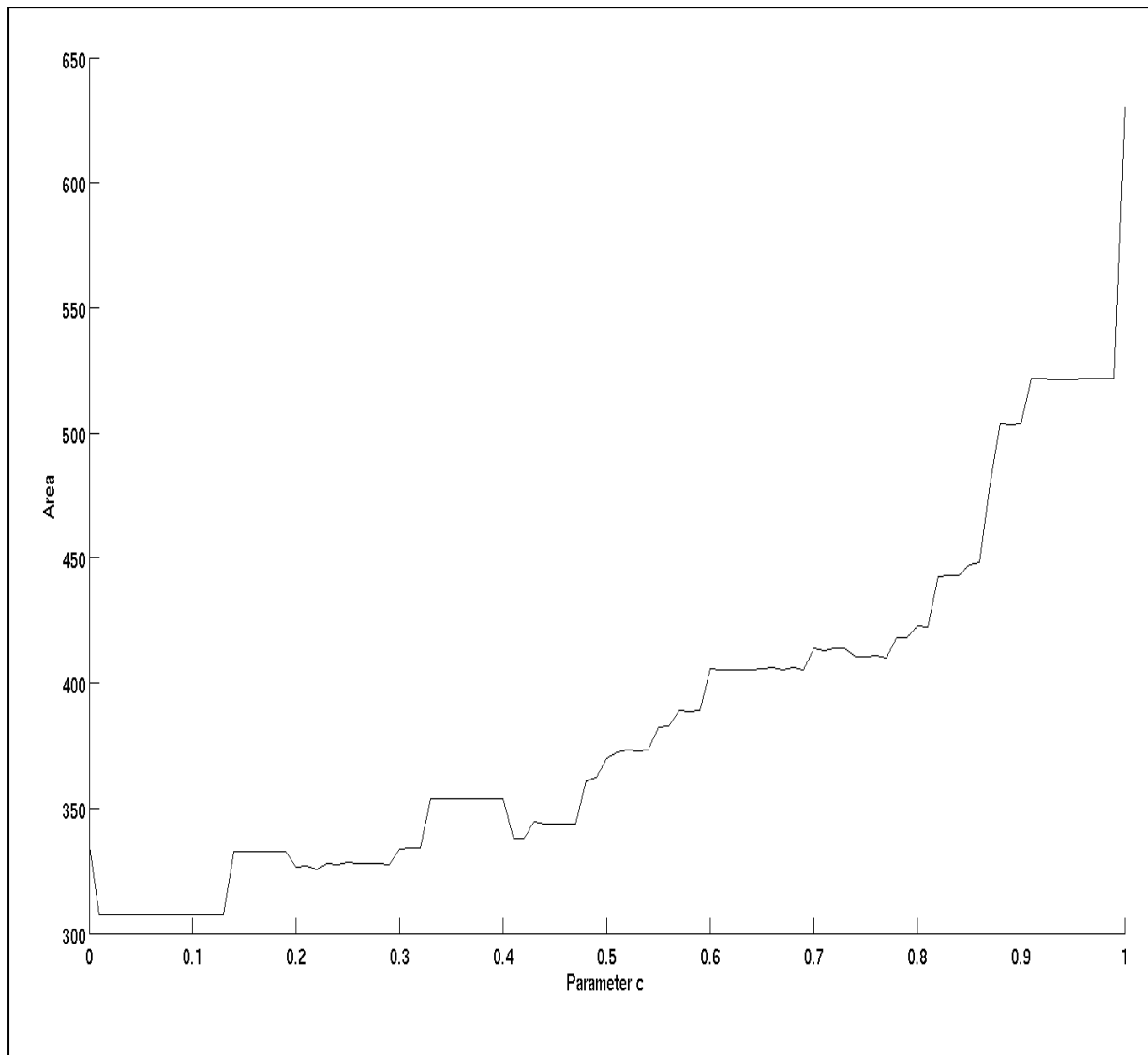
Figure 3: Log-log plot: methamphetamine trafficking network.



Law enforcement simulations

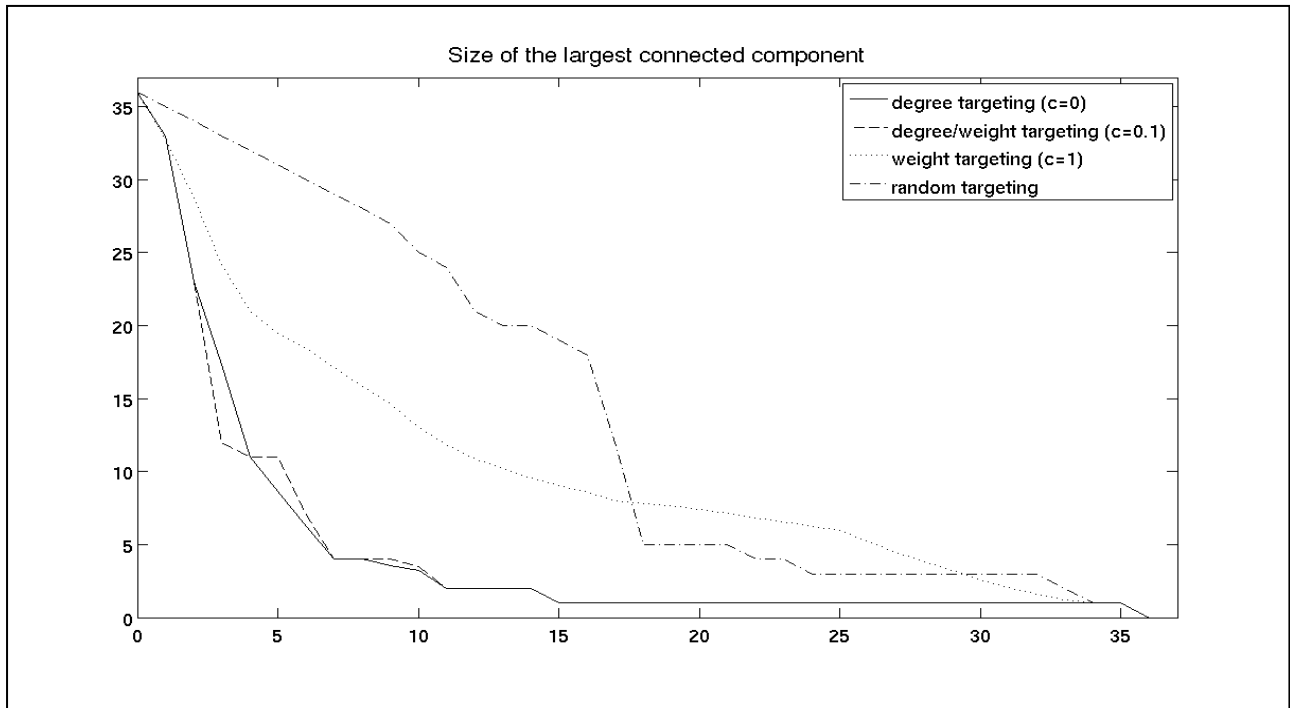
First we investigated the dependence of the disruption function on the parameter c , in order to find a near-optimal value of c (at least for the given network). The average area under the curve of the disruption function was calculated for many different values of c (see Figure 4). Again, the average was taken over 100 runs of the simulation. We see that values of c around 0.1 give the best result, and therefore we chose to work with $c = 0.1$ as a convenient value.

Figure 4: Average area under the disruption function, for various values of c



Next we performed 100 runs of each of our simulations, and measured fragmentation of the network at each step by calculating the size of the largest connected component. Figure 4 shows the average size of a maximum component at each step of the four simulations. The average is taken over 100 runs of each simulation.

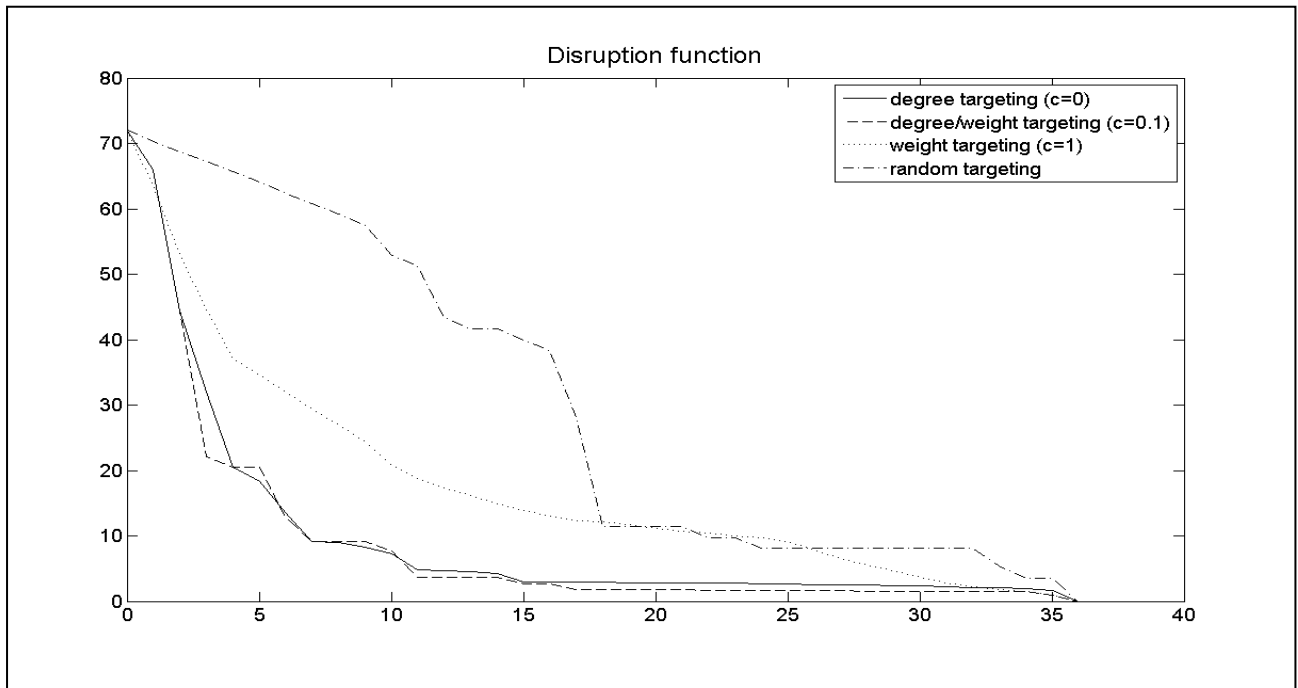
Figure 5: The four simulations, measured by the size of the largest connected component



Just by viewing this plot, we see that random targeting is ineffective compared with the three other strategies. The best strategies appear to be degree targeting and the mixed strategy. This can be quantified by comparing the area under each curve. These areas are 514.50 for random targeting, 376.55 for weight targeting, 159.98 for degree targeting and 158.86 for the mixed strategy. This confirms the visual impression that the degree targeting and mixed strategy have a similar performance, and that both outperform the other two strategies (targeting based on role only, and random targeting).

Finally we performed 100 runs of each of our simulations, calculating the disruption function of the network at each step. Figure 6 shows a plot of the average value of this function over the four simulations. Again, the average is taken over 100 runs in each simulation.

Figure 6: The four simulations, measured using the disruption function



Viewing the plot, we see that the best performance is obtained using the degree targeting and mixed strategies, with these being very similar. In fact, the curve for the mixed strategy lies below the curve for the degree strategy most of the time, which suggests that the mixed strategy performed the best overall. The random strategy is far worse than all the others. The effectiveness of targeting based on role only falls between random targeting and the degree/mixed interventions. We quantify this by calculating the area under each curve, giving the following areas: 1098.35 for random targeting, 630.49 for weight targeting, 335.64 for degree targeting and 307.48 for the mixed strategy. This confirms that the mixed strategy was the best in this case.

Discussion.

The current study aims to examine whether criminal networks show evidence of being scale-free in structure, and to estimate the differential effectiveness of different law enforcement strategies aimed at dismantling criminal networks.

Network structure.

We performed some calculations to compare the degree distribution of the methamphetamine network with the expected degree distribution of a random graph with the same density of links. We believe that our calculations show that the methamphetamine network is not an “exponential network”, as the nodes of high degree are extremely unlikely to exist in a random graph with the same average degree. By default, this suggests that the network is likely to be of the scale-free variety (Albert, Jeong, & Barabasi, 2000). From the log-log plot of the cumulative degree distribution there may be some evidence for scale free structure, but this is inconclusive mainly due to the small size of the network.

Law enforcement interventions

In our simulations, the degree targeting strategy proved very effective at fragmenting the network, with respect to both measures (size of largest component, and the disruption function). This is consistent with previous research (e.g., Keegan, et al., 2010). It is somewhat surprising that the mixed strategy achieved an improvement over degree targeting when measured using the maximum component size, since this is a purely topological measure.

We believe that this improvement is an artefact of the properties of the methamphetamine network, as we now explain. Careful study of Figure 5 reveals that the curve for the mixed

strategy dips below the curve for the degree targeting at the third step (after the third deletion). By the fourth deletion the two curves meet and thereafter the curve for degree targeting is always below or meeting the mixed strategy curve. So the improvement obtained by the mixed strategy is entirely due to the choices made in the 3rd step of the simulation.

Under both strategies, the first two nodes which are deleted are always K12 and K18 (in that order). The reader may check that after these deletions, there are 22 nodes in the maximum connected component of the remaining network. Then the degree targeting strategy will randomly choose a node of highest remaining degree, namely K20 or K28 (both of degree 7). Each of these nodes is chosen with probability 1/2 and is deleted, leading to a network with maximum connected component of size 21 or 18. The average over 100 runs of the maximum component size at this step will be close to 19.5 (which equals the average of 21 and 18). However, at the third step the node with the highest score in the mixed strategy is K26. Hence this node will be deleted at the third step, leading to a network with a maximum connected component size of 11. This fairly dramatic improvement (reducing the size of the largest component from 22 to 11 in one step) is due to an important structural property of this particular criminal network. As can be seen from Figure 2, deleting the links from K17 to K26 and from K12 to K28 will disconnect the network into two pieces, of roughly equal size. This can also be achieved by deleting one node from each of these two links, such as K12 and K26. In graph theory terminology, the set containing K12 and K26 is a *cut set*, meaning that deleting these nodes creates a disconnected graph. It is a very useful cut set for fragmenting the network because each remaining component is much smaller than the original network (around half the size). By chance, the mixed strategy manages to delete such a cut set in the first three steps, thereby producing a steep drop in the size of the largest connected component.

It is clear from Figures 5 and 6 that random targeting is much less effective than degree targeting, irrespective of whether effectiveness is measured using the size of the largest connected component or the disruption function. To quantify this, we calculated the ratios of the areas under the curve for random targeting versus degree targeting. This ratio equals 3.22 with respect to the maximum component size measure (Figure 5), and equals 3.25 with respect to the disruption function (Figure 6).

The mixed strategy performed (slightly) better relative to the degree strategy. The ratio of the areas under the curve for the degree targeting versus mixed strategy was 1.006 with respect to the maximum component size measure (Figure 5) and was 1.092 with respect to the disruption function (Figure 6). This is not unexpected given that the disruption function takes role information into account when measuring fragmentation.

Overall, law enforcement strategies which targeted nodes based on centrality scores and on a combination of centrality scores and roles of individuals were most effective. Law enforcement interventions which use role information only and which do not consider centrality scores were relatively ineffective at dismantling the network. Interestingly, adding role information to centrality scores increased the effectiveness of law enforcement interventions in dismantling the network when the outcome measure incorporated the roles or ease with which individuals could be replaced (the disruption function).

Recall that we worked with the value $c = 0.1$ since this gave optimal performance for the given network, as shown in Figure 4. It is noteworthy that this value of c is quite small,

meaning that the mixed strategy only takes role information into account to a limited extent. This could be an artefact of the particular network studied.

Policy/Practice implications.

The results of the study suggest that in effectively targeting criminal networks, law enforcement should consider both node level features (such as the roles played by individuals in the network) and node topography features such as centrality scores. In fact, the results suggest that only using role information to determine nodes to target is less effective than using either centrality scores or centrality scores in concert with individual attributes (such as roles). The results underscore the utility of measures of centrality in choosing individuals to target when the aim is to dismantle criminal networks.

To make cost-effective arrests, law enforcement agencies require resources which facilitate the gathering of quality intelligence, sophisticated SNA, and interventions targeted at vulnerable areas (i.e., hubs). These processes are resource heavy. In recent media interviews (Australian Broadcasting Corporation, 2010), ACC chief executive and ex-officers suggested that law enforcement is currently under-resourced to engage effectively in these endeavours. Also, there may be political pressure on law enforcement agencies to seize drugs and money, make arrests etc as indicators of success, rather than to engage in prolonged intelligence gathering, costly investigations, and interventions designed to dismantle a criminal network. If future research supports the results of this preliminary research, it would suggest that resources directed into longer term intelligence gathering, SNA of criminal networks (i.e., including calculation of centrality measures and node level attribute information), and targeting vulnerabilities within criminal networks, may produce cost-effective results (but this needs further economic study).

Furthermore, there are no clear and accepted methodologies which measure the effectiveness of law enforcement interventions aimed to dismantle criminal networks. On the other hand, trends in seizures and arrests are routinely reported and are often used (somewhat erroneously) as measures of law enforcement effectiveness. This surfaces the need for the development of alternate performance indicators which can accurately reflect other law enforcement goals such as the dismantling of criminal networks.

Limitations

There are a number of important caveats regarding this study, and for the generalisability of the results to real-world criminal networks. There are a number of limitations of the study. Firstly, all criminal networks research suffers a range of limitations including: Networks are multimodal (include people, events, locations, resources), the current study looked at connections between people only; simple and static connections. Criminal justice/law enforcement data can include intentional misinformation (e.g., aliases) and inaccuracies (e.g., typos). Law enforcement and criminal justice data, such as that used in this study, are often incomplete. Also, degree centrality scores for particular nodes may be artificially inflated by the amount of information gathered on particular nodes during the investigation, and may not reflect the extent of “real” connectedness. The network that we studied is very small, with only 36 nodes. There are many ways to quantify role information and to measure fragmentation of a network: we feel that the choices that we made were logical, however other choices may also be valid and may lead to different results.

Secondly, the simulations assumed that no new connections are made in response to node removal. Dark networks are resilient (Ayling, 2009; Bakker, Raab, & Milward, 2010; Carley, 2006) and can respond or adapt to law enforcement interventions in a number of

ways: by replacing nodes, replacing links, by laying low, recruiting new members, joining other groups, or through the emergence of new leaders (Carley, Lee, & Krackhardt, 2002). In fact, even if all well connected nodes are removed, just a few remaining nodes might re-establish communication (Williams, 2001). The simulation did not take account of this possibility. Thirdly, the aims of law enforcement are diverse. In this project we evaluated the extent to which law enforcement interventions (arrests) can dismantle a criminal network. However, law enforcement may seek to accomplish goals other than dismantling a network. For example, the aim may be to incapacitate the network so that the groups can no longer act illicitly, or to breach trust within the network such that the network disintegrates via internal distrust and conflict.

Nonetheless, the simulation methodology we employed here can provide insights into the structural and functional damage that can be done to dark networks by targeted removal of nodes. It has the potential to demonstrate the utility of targeted node removal as a law enforcement intervention, especially compared with the removal of less well connected nodes such as drug couriers, wholesale dealers or other individuals who are easily replaceable and are not well connected with other nodes in the network, but may simply be more “visible”. In addition, it provides a potential method for measuring the effectiveness of law enforcement interventions which aim to dismantle criminal networks.

Future research.

Research looking at the vulnerability and resilience of criminal networks is in its infancy. This paper represents an important progression in the literature, but more research is needed. Improved strategies may be obtained by taking more information from the network into account, such as looking for small cut sets which achieve a steep drop in the size of the

largest connected component. Furthermore, alternate methods to measure connectedness, for example frequency of contact (e.g., number of phone calls) could be used to quantify strength of relationships. There is also a need to replicate this work with larger, more complex networks, and with a variety of criminal networks (terrorist networks, arms traffickers, people smugglers/traffickers etc). Insights may be gained from performing simulations on random scale-free (or other) networks, using some random distribution of role data. Future research should utilise dynamic modelling which incorporates network responses/adaptation (e.g., previously unconnected nodes connect; recruitment), and individual/node-level characteristics (e.g., resilience, adaptability). Finally, the current paper utilised a relatively unsophisticated method of quantifying role information. Future research should utilise more detailed data sources and attempt to use more sophisticated node attribute data (see Robins, 2009; Robins & Kashima, 2008).

References

- Albert, R., Jeong, H., & Barabasi, A.-L. (2000). Letters to Nature: Error and attack tolerance of complex networks. *Nature*, *406*, 378-382.
- Albert, R., Jeong, H., & Barabasi, A. L. (1999). Diameter of the World-Wide Web. *Nature*, *401*, 130-131.
- Australian Broadcasting Corporation. (2010). Four Corners. (authors to add full reference)
- Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice*, *37*(4), 182-196.
- Bakker, R. M., Raab, J., & Milward, H. B. (2010). *A preliminary theory of dark network resilience*. Unpublished manuscript.
- Bollobas, B., & Riordan, O. (2004). Robustness and Vulnerability of Scale-Free Random Graphs. *Internet Mathematics*, *1*(1), 1-35.
- Bright, D. A., Greenhill, C., & Levenkova, N. (2010). *Attack of the Nodes: Scale-Free Criminal Networks and Vulnerability to Targeted Law Enforcement Interventions*. . Paper presented at the 2nd Illicit Networks Workshop.
- Bright, D. A., Hughes, C. E., & Chalmers, J. (in press). Illuminating dark networks: A social network analysis of an Australian drug trafficking syndicate. *Crime, Law, and Social Change*.
- Carley, K. M. (2006). Destabilization of covert networks. *Computational and Mathematical Organization Theory*, *12*, 51-66.
- Carley, K. M., Lee, J., & Krackhardt, D. (2002). Destabilizing networks. *Connections*, *24*, 79-92.
- Crucitti, P., Latora, V., Marchiori, M., & Rapisarda, A. (2003). Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, *320*, 622-642.

- Ebel, H., Mielsch, L.-I., & Bornholdt, S. (2002). Scale-free topology of e-mail networks. *Physical Review E*, 66(3), 035103.
- Keegan, B., Ahmed, M. A., Williams, D., Srivastava, J., & Contractor, N. (2010). Dark Gold: Statistical Properties of Clandestine Networks in Massively Multiplayer Online Games. In *Proceedings of the Second IEEE International Conference on Social Computing*, (Minneapolis, USA), August 2010.
- Liljeros, F., Edling, C. R., Amaral, L. A. N., Stanley, H. E., & Aberg, Y. (2001). The web of human sexual contacts. *Nature*, 411(6840), 907-908.
- Morselli, C., & Petit, K. (2007). Law-Enforcement Disruption of a Drug Importation Network. *Global Crime*, 8(2), 109 - 130.
- Natarajan, M. (2006). Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data. *Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data*, 22(2), 171-192.
- Newman, M. E. J. (2003). Random graphs as models of networks. In S. Bornholdt & H. G. Schuster (Eds.), *Handbook of Graphs and Networks: From the Genome to the Internet*. Weinheim: Wiley-VCH.
- Redner, S. (2005). Citation statistics from 110 years of Physical Review. *Physics Today*, 58, 49-54.
- Robins, G. (2009). Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects. *Trends in Organized Crime*, 12(2), 166-187.
- Robins, G., & Kashima, Y. (2008). Social psychology and social networks: Individuals and social systems. *Asian Journal of Social Psychology*, 11(1), 1-12.

Williams, P. (2001). Transnational Criminal Networks. In D. F. R. John Arquilla (Ed.), *Networks and netwars: the future of terror, crime, and militancy*. Santa Monica: RAND.

Xu, J., & Chen, H. (2009). Untangling Criminal Networks: A Case Study. *Intelligence and Security Informatics* (pp. 958-958).