2018 ACTA UNIVERSITATIS CAROLINAE PAG. 115–135
PHILOSOPHICA ET HISTORICA 2 / STUDIA SOCIOLOGICA

SINISTER CONNECTIONS: HOW TO ANALYSE ORGANISED CRIME WITH SOCIAL NETWORK ANALYSIS?[1]

TOMÁŠ DIVIÁK
Department of Sociology, Faculty of Arts, Charles University & Department of Sociology, University of Groningen, and Interuniversity Center for Social Science Theory and Methodology, The Netherlands
E-mail: tomas.diviak@gmail.com

ABSTRACT

Networks have recently become ubiquitous in many scientific fields. In criminology, social network analysis (SNA) provides a potent tool for analysis of organized crime. This paper introduces basic network terms and measures as well as advanced models and reviews their application in criminological research. The centrality measures – degree and betweenness – are introduced as means to describe relative importance of actors in the network. The centrality measures are useful also in determining strategically positioned actors within the network or providing efficient targets for disruption of criminal networks. The cohesion measures, namely density, centralization, and average geodesic distance are described and their relevance is related to the idea of efficiency-security trade-off. As the last of the basic measures, the attention is paid to subgroup identification algorithms such as cliques, k-plexes, and factions. Subgroups are essential in the discussion on the cell-structure in criminal networks. The following part of the paper is a brief overview of more sophisticated network models. Models allow for theory testing, distinguishing systematic processes from randomness, and simplification of complex network structures. Quadratic assignment procedure, blockmodels, exponential random graph models, and stochastic actor-oriented models are covered. Some important research examples include similarities in co-offending, core-periphery structures, closure and brokerage, and network evolution. Subsequently, the paper reflects the three biggest challenges for application of SNA to criminal settings – data availability, proper formulation of theories and adequate methods application. In conclusion, readers are referred to books and journals combining SNA and criminology as well as to software suitable to carry out SNA.
Key words: social network analysis; network models; criminal networks; covert networks; organized crime

In recent years, there has been a huge influx of interest in networks in basically every scientific field and also in our everyday language. Networks are now studied in such various fields as computer science, physics, biology, and social sciences such as economics and sociology (Newman, 2010). Some researchers even speak of a brand new field of study – network science (Robins, 2015). In social sciences, the term network has been connected to globalisation, social media, and more generally to a fundamentally new

[1] The preparation of this journal article was supported by the Charles University funding scheme Progres Q15.

https://doi.org/10.14712/24647055.2018.7

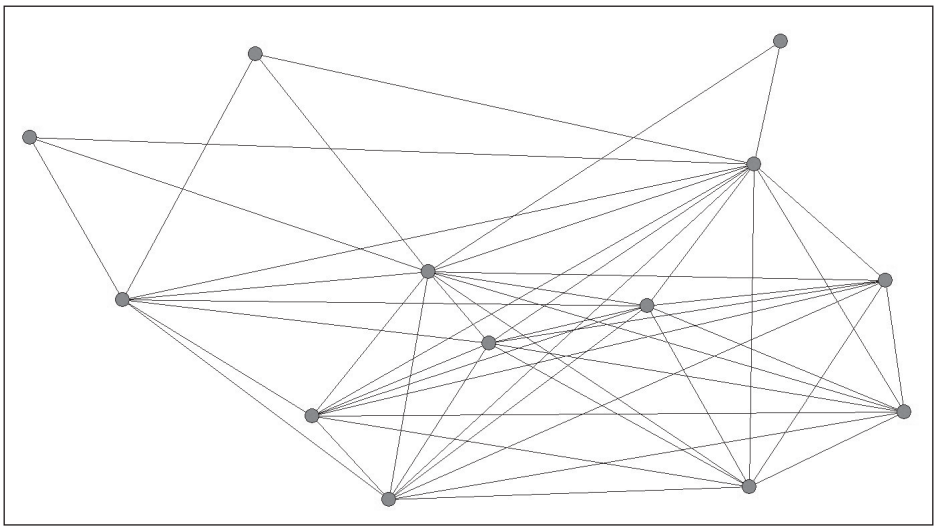

Figure 1: A graph of a network with nodes (points) and edges (lines)

form of social organization. Networks are supposed to be fluid, flexible, dynamic, global, and omnipresent, yet it is often not clear, what exactly these networks are, how they are defined or how should we think about them. Amidst the "network revolution" the term *network* has been used so widely, that it could be considered a buzzword. Even though there have been earlier attempts to marry network perspective with criminology and criminal intelligence (Krebs, 2002; Sparrow, 1991), some researchers argue that criminology might have been left a little bit behind this network trend (Papachristos, 2014). However, the network perspective has much to offer for criminology and especially for the study of organized crime. This paper introduces the network thinking into the criminological research and points out potential benefits of this synthesis.

It is important to clarify what is meant by networks here. The concept of network may be rather broad. The network is defined here as a set of actors and a relation among them, indicated by a collection of dyadic ties (see Figure 1). This is a definition commonly used in social network analysis (SNA). And since all the forms of organisation are based on human interactions and relations, they can be subsumed under networks (Carrington, 2011; von Lampe, 2009). Within this conceptualization, networks capture "the least common denominator" of organized crime – human relations (McIlwain, 1999). Networks in this sense are thus an instrument which can capture any hypothetical form the organized crime can take – be it hierarchy, market or ethnic communities (Le, 2012). Social network analysis methods can then empirically describe and test to which extent they are hierarchical or decentralized, stable of fluid, or in general – how they are structured or in other words, *how* are they organized. After all, this is a major question in the whole field of organized crime studies (von Lampe, 2009).

Criminal networks are special cases of so-called covert networks[2]. The underlying assumption is that covert networks are defined by the need of actors involved in them to remain concealed (Oliver, Crossley, Everett, Edwards, & Koskinen, 2014). Such an environment and context, where it is principal to hide, modifies interactions and relations (Morselli, 2009: 8). The focal point of studying criminal networks is first trying to determine how interactions and relations among a group of offenders intertwine and build up to create a network, and then analyse this with the use of SNA. In this paper, we introduce the most important concepts in SNA, from the basic terminology, through descriptive measures of networks to advanced network models. We will also illustrate criminological applications of these concepts.

Basic terminology

We define network as a set of nodes and ties[3] among them (Borgatti, Everett, & Johnson, 2013; Hanneman & Riddle, 2005; Wasserman & Faust, 1994)[4]. *Nodes* can represent any entity, but in social sciences, they usually represent social actors. Specifically, in the study of organized crime, nodes represent offenders such as traffickers, terrorists, gang members etc. Nodes can carry various *attributes*, for example they may have different genders (binary attribute), possess different skills (categorical attribute), have different attitudes towards various things (ordinal attribute) or be of different wealth (continuous attribute). *Ties* are what connect them; the collection of all ties between the nodes in the node set defines the *relation*. This definition encompasses a broad range of phenomena. Relations may be either undirected or directed. Undirected relations are by definition mutual such as being at the same place at the same time (co-attendance), being members of the same organization (co-membership) or sharing a background (e.g. being university classmates or relatives). Directed relations allow for specifying from which node to which other the tie goes. These often represent flows of resources (e.g., money or drugs) or communication (e.g., who calls whom). Generally, in cases of one actor sending a tie to another and the other potentially sending or not sending it back (so-called reciprocity), the ties are defined as directed, whereas in cases the reciprocity is "automatic", ties should be defined as undirected. In addition to directionality, ties may also vary in their strength or value. The simplest case is a network of binary ties, where a tie is either present or absent. Like other variables, tie variables can be dichotomous (the simplest case just mentioned), ordinal, discrete, or continuous. An important distinction further is between positive (friendship) and negative (enmity) relations. All these distinctions have implications for

[2] For a deeper discussion on the relation of covertness and legality of various networks, see (Milward & Raab, 2006)we try to understand and interpret why and how dark networks manage to survive despite massive control efforts by nation states, thus demonstrating a high degree of resilience. We approach this question from an organizational perspective looking at the (organizational.

[3] The term "node" is interchangeable with the term "vertex" and in social sciences with the term "actor" (in the cases where nodes represent actors). Similarly, the term "tie" is sometimes interchanged with the term "edge" or "arc" (arc refers to a directed tie).

[4] There are many more network concepts and measures than those described here. For further reference, see the introductory text by Borgatti, Everett, & Johnson (2013) or an intermediary book by (Robins, 2015).

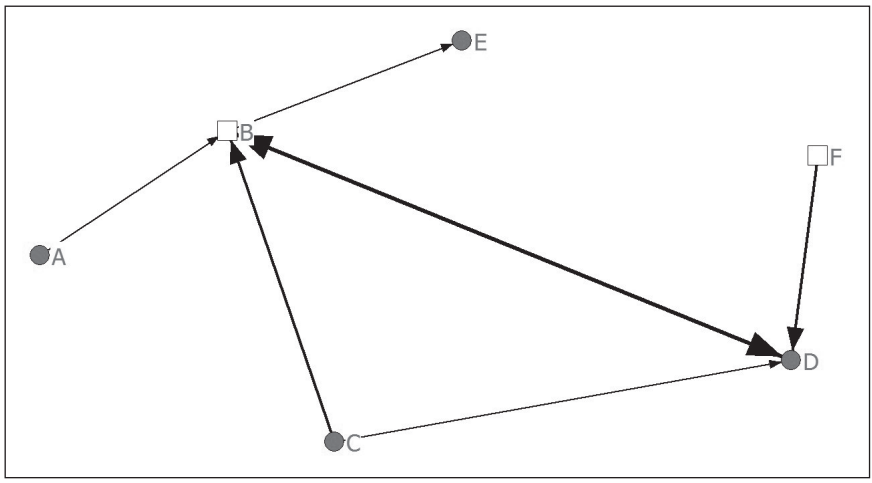

Figure 2: An example network with 6 nodes with a binary attribute displayed with different colors and shapes (white squares = female, grey circles = male) and 7 directed weighted ties among them (the B to D tie is reciprocated, i.e., goes in both directions)

which methods to use and how. Most methods have been developed for relations with dichotomous tie variables. All these aspects of network can be visually represented in network graphs. These visualizations are also known as sociograms and they have been invented by Jacob L. Moreno (1934), the father of sociometry – a precursor to SNA.

The information on criminals and ties among them is based on the available data. Collecting the data can be a daunting task as observing a group of people who by definition try to avoid any detection excludes usual ways of collecting data in social sciences. Therefore, we usually analyse secondary data on criminal networks. This data may come, for example, from police investigation and surveillance, trial testimonies, court documents, archives, other research or from media reports. All these sources have different liabilities and advantages – police data may not be accessible, testimonies may be purposefully distorted by defendants, archival data may be incomplete and media reports may have questionable validity. What is important is to be wary of the shortcomings of the data we use and be as careful as possible with their procession and analysis. We will come back to the issue of data in this field in the last part of this paper.

Centrality measures[5]

Centrality measures are probably the most well-known and the most widely used concept within the SNA (Morselli, 2009: 38). Centrality measures are a set of methods which are used to identify the most prominent nodes in the network (Freeman, 1978). This is obviously very important in the context of criminal network analysis, as the most central actors are suitable targets for monitoring and subsequent disruption of the network,

[5] Overview of centrality measures can be found in a paper by (Borgatti, 2005).

which is of great interest for law enforcement (Sparrow, 1991). Furthermore, organizing activities of central actors often explain the organization of the whole group, its ability to adapt to a changing environment, profit or survive in the face of disruption (Bright et al., 2012; Morselli, 2009; Oliver et al., 2014). There are tens of different centrality measures and while it is by far not necessary to compute all of them, it is also never redundant to compute more than one. Even though they relate to the same concept (that is the relative importance of a node within a network), each of them approaches this concept from a different angle and thus they are complimentary to each other. Here, we will take a look at just two of these measures, which are arguably the most important and also the most frequently used; degree and betweenness.

Degree captures the simplest intuitive notion of an important actor – it is such a node, which has the most ties to other nodes. The high number of direct contacts allows such an actor to access a lot of information and potentially exercise direct control over adjacent actors in the network. Formally, the degree of a node is the sum of its ties. In directed networks, we can distinguish two kinds of degree – indegree and outdegree. Whereas indegree refers to the number of incoming ties (directed towards the node), outdegree refers to the number of outgoing ties (directed from the node). In valued networks, not only the plain number of ties can be computed, but also the sum of their values, so that degree tells us for example how many times has a particular node met with others or how much money has he or she received. In Figure 2, B is the node with the highest degree.

The centrality measure called *betweenness* defines important nodes from a different point of view than degree. Central actors in terms of betweenness are those, who stand between other nodes in the network. Between each pair of nodes within the network, if there is a sequence of connected nodes between them, we can find the shortest sequence known as the *geodesic path*. For example, between nodes A and F in the Figure 3, there are numerous paths leading from one to the other. However, only the path through nodes I and H is the shortest (of length 3) making it the geodesic path between A and F. The betweenness of a node then is the proportion of geodesic paths between all pairs of nodes in the network that pass through this node. Betweenness is very important for relations that have to do with communication or other processes where indirect connectedness is important while long geodesic distances are costly, because then high betweenness means having an important position through which much of the flows will pass. Actors with high betweenness scores are sometimes coined as brokers or gatekeepers – they bridge connection to others in the network and control flows of, for instance, information, goods, in the network. In the network in Figure 3, the node with the highest betweenness is I, whereas A has the highest degree. Brokers may also be crucial for keeping the network connected (Morselli & Roy, 2008).

In some networks degree and betweenness are highly correlated, that is, nodes which have high score in one measure tend to have high score in the other as well. However, this is not necessary – criminal networks in particular are often exceptions to this pattern. Having a high degree may have a significant drawback in such networks, because a high number of ties means a high number of interactions and therefore high visibility which in turn leads to higher chance of being detected – which the actors in criminal networks obviously try to avoid. Some actors may act in such a way that

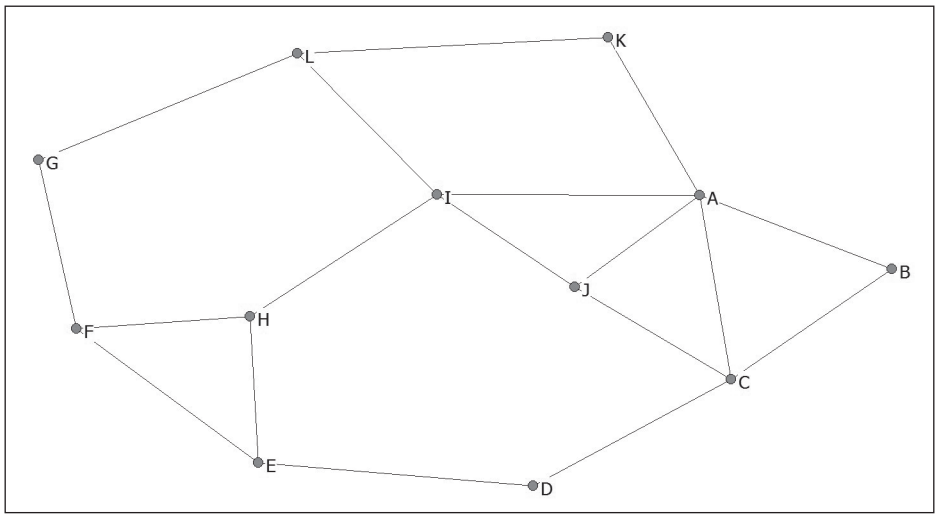

Figure 3: An example network

they try to minimize redundant connections, but compensate for it by assuming key brokerage positions, which allows them to retain control of the most important information, resources, and co-offenders in the network, while being less visible and thus susceptible to detection. This is called strategic positioning (Morselli, 2010). In the case of having high scores in both degree and betweenness, the vulnerability connected with high degree may outweigh the advantages of betweenness (Morselli, 2009). Strategically positioned actors have been observed for example in networks of drug trafficking operations of the Hells Angels gang (ibid.), an Australian drug trafficking network (Bright, Greenhill, Ritter, & Morselli, 2015), or Calabrian N'dranghetta's cocaine dealing activities (Calderoni, 2012). However, in some other cases where it was studied, this phenomenon has not been present, such as in the case of political corruption (Diviák, Dijkstra, & Snijders, 2017) or in another case of drug trafficking network (Hofmann & Gallupe, 2015). These results suggest that while strategic positioning is not universal, it is worth paying attention to it.

A closely related topic to the centrality of actors is the problem of criminal network disruption. Since the law enforcement usually has only limited resources for disrupting criminal networks, it needs to allocate them as efficiently as possible. Disruption is a state of a network, in which it can no longer serve the purpose it was designed to serve (Carley, Lee, & Krackhardt, 2002; Bright, 2015). In a disrupted network, resources and information are unable to flow properly and actors involved in them cannot communicate smoothly and reach a consensus (Carley, Lee, & Krackhardt, 2002). Central nodes within the network, and brokers particularly, have been proven to be suitable targets for such an efficient disruption, as in both simulation and longitudinal studies, removal of a central node caused the most damage to the network in comparison to random node removal or removal based on attributes of nodes (such as possession of skills and resources; Bright, 2015). This fact has been demonstrated in number of empirical studies – in the case of

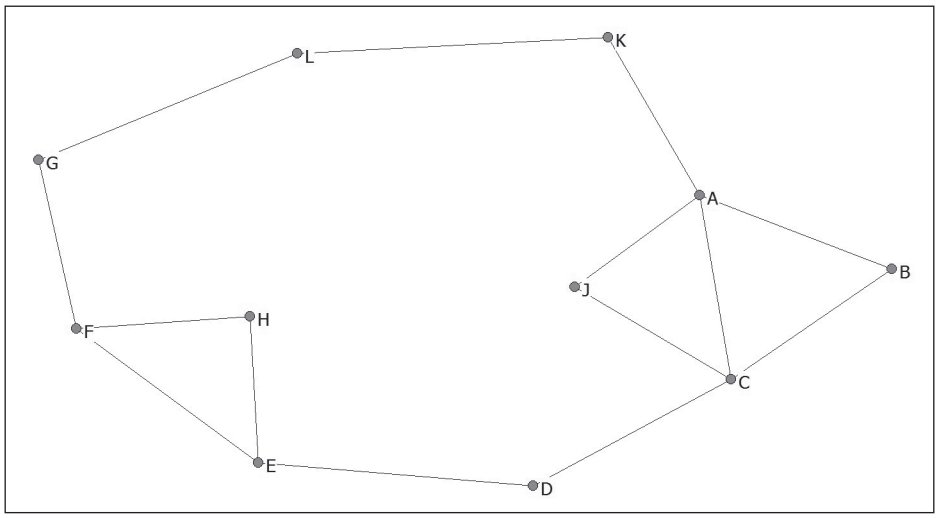

Figure 4: A graph showing the effect of a central node (I) removal

a hacker network (Décary-Hétu & Dupont, 2012), terrorist, drug trafficking, and gang networks (Xu & Chen, 2008), and ringing operations network (Morselli & Roy, 2008). This area of research is very vivid and more research is being done, particularly in relation to network dynamics and their ability to recover from disruption (Bright, 2015; Duijn, Kashirin, & Sloot, 2014).

Cohesion measures

Whereas centrality measures focus on individual nodes within the network, cohesion measures focus on the network as a whole. Specifically, cohesion measures indicate how well connected or cohesive (hence the name) the whole network is. In more cohesive networks, information and resources flow easily, goals can be reached effectively, infiltration and disruption may be more difficult, and norms and identity among the nodes tend to be similar (Borgatti, Everett, & Johnson, 2013: 181; McGloin & Kirk, 2010). Much like in the case of centrality, there are different ways of expressing cohesiveness of a network which are mutually complimentary. Here, we will introduce measures which are based on the number of ties within the network, on the spread of the ties within the network, and on the distance among the nodes.

The intuitive image of a cohesive network is a network in which nodes are well connected to each other. *Density* is a measure which captures this. It is a proportion of ties present in the network relative to the maximum number of possible ties in the network (that is the number of all pairs of nodes). The result ranges from 0 to 1, where 0 means that the network is just composed of all isolated nodes, while 1 means that each node has a tie to each other in the network. This implies that density can also be expressed as a percentage. The average of the degrees is an alternative measure of cohesion. This contains

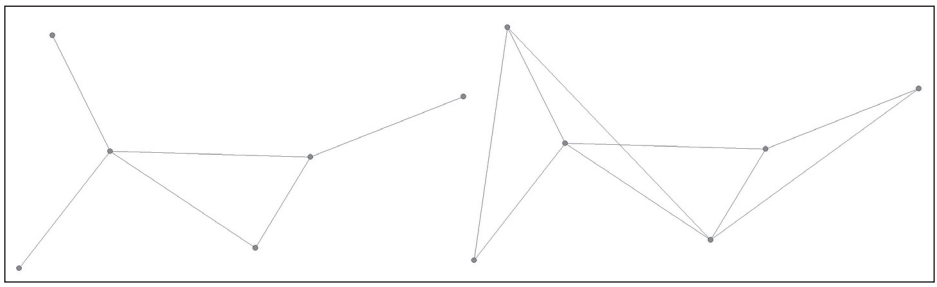

Figure 5: A sparse (density = 0.4) and a dense (density = 0.8) network with 6 nodes

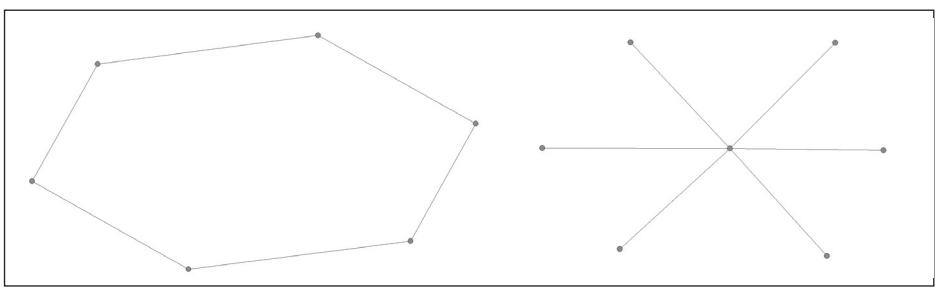

Figure 6: A circle network and a star network

the same information as the density, because the average degree is the density multiplied by the number of nodes minus 1. For most social networks the average degree is a more directly interpretable measure than the density, because it is more directly experienced by the actors. Density is mostly inversely related to the network size – with an increase of the number of nodes, the density tends to decrease (Everton, 2012).

It is not only the sheer number of ties that matters for cohesiveness of the network, but also their spread. In other words, in some cases, ties can be concentrated around a few very central nodes and in other cases, ties may be evenly spread among all the nodes. This is captured by measures called *centralization*. Essentially, centralization tells us to which extent does a particular network resemble a star network, which is a maximally centralized network around one node with ties to all others and no other ties among them. If centralization equals 1, it is a star network, while if it equals 0, then each node in the network has the same number of ties. Similarly to average degree, we can also use the standard deviation of degrees to indicate the spread of ties in the network as an alternative to centralization (Snijders, 1981).

When we defined the betweenness above, we used a concept of geodesic distance to do so. *Geodesic distance* is the shortest path (the smallest number of ties) between a given pair of nodes. In this vein, we can think of a cohesive network as a network with short geodesic distances among the nodes. We can then simply characterize a network with an average geodesic path length. The smaller this average is, the more cohesive the network is in these terms. A measure of variability of geodesic path length is the *diameter* of the network. The diameter is the longest geodesic distance in the network, and indicates how

many steps a piece of information or a resource needs for traveling between the two most remote nodes in the network.

Greater cohesion of the network initially increases its flexibility and the potential for interaction of its actors. However, beyond a certain point, increased cohesion may stifle these advantages (Everton, 2012). This is because both extreme sparsity and extreme density are disadvantageous. On the one hand, very low density leads to insufficient cooperation, coordination, social control among the actors and thus the inability to reach goals. On the other hand, overtly dense network structure leads to too much social control and too much similarity among the actors, which hampers their ability to perform complex tasks and to adapt to varying conditions. This relates closely to what Morselli, Giguére, and Petit (2007) called the efficiency/security trade-off. They argue that "criminal network participants face a consistent trade-off between organizing for efficiency or security" (ibid.: 143). Efficiency indicates that participants in criminal networks interact and communicate with each other frequently by having a lot of ties. But as we have already shown on the strategic positioning, a lot of ties come at a price of being easily detectible and thus vulnerable, undermining the security of the network. If criminals opt for more secure communication design with a lower number ties instead, their ability to efficiently coordinate the whole network decreases. According to Morselli and colleagues (2007), the goal determines whether a network will be structured efficiently or securely. Ideologically driven networks (terrorists) are supposed to be particular at assuring security, as they operate within long time frames preparing to carry out one carefully planned action (typically an attack). To achieve this, they have to remain as secure as possible. The efficiency is a feature of networks driven by financial profit, such as smugglers, traffickers or drug dealers, who operate within short time frames in order to generate profit and thus need numerous ties. This idea challenges the very basic assumption of the field of criminal networks – the primary emphasis on security and covertness of actors within these networks. Testing this hypothesis empirically is currently one of the focal points in the field (Wood, 2017).

Subgroups detection[6]

One common feature of networks created by human actors is the tendency of actors to create smaller groups which are usually more cohesive (i.e., dense) than the overall network (Newman & Park, 2003). This tendency is called clustering. Within such subgroups actors are more likely to share norms, values, resources, and thus actors involved in them are strongly influenced by other members of their subgroup (Borgatti et al., 2013: 181). In criminal networks, subgroups might represent closely cooperating task groups. As with the centrality measures, there are numerous ways to detect subgroups and more and more are being developed[7]. Here, we will take a look at the most frequently used ones; cliques and factions.

---

[6] Other terms, such as "cohesive subgroups", "clusters" or "communities", are used to label this type of sets of nodes within the network. Since the term "community" has other meanings across social sciences, "clusters" may create confusion with cluster analysis and for clarity purposes, we will simply talk about "subgroups" here.

[7] An elaborated and more technical review of these methods was provided by (Fortunato, 2010).

Cliques are formally defined as maximal complete subgraphs. This means that a clique is a group in which all nodes have ties to each other, but there is no other node that also has ties to all nodes in this group. Thus, the density within each clique equals 1, as all the ties which can be there are by definition present. The minimal number of nodes considered is usually three. One important property of cliques is that they can overlap, which means that one node can belong to multiple cliques. This way, cliques stack onto one another resulting in the overall structure of the network (Borgatti et al., 2013) . The definition of cliques implies that in most usual networks, clique sizes are rather small, e.g., going up to four or five nodes. However, if we imagine a subgroup of seven actors, where everyone has ties to everyone else with the sole exception of one null dyad (a pair of actors with no tie between them), it is not a clique, but it still is considerably cohesive (density = 0.98). For this reason, alternative concepts have been proposed. One such alternative is a subgroup called *k-plex*. A k-plex, for a given value of k, is a group in which each node is connected to all other nodes except perhaps a subset of at most k nodes. So, in our earlier example, a group of seven actors with one null dyad is a 1-plex of size 7.

A different and more computationally complex approach to subgroups detection is represented by algorithms for detecting so-called *factions*[8]. The main idea is that a network can be partitioned to subgroups, which internally contain as many ties as possible (so, ideally they are cliques) while between them in contrast, there as few ties as possible. It is up to researcher to determine the number of subgroups to be found this way and frequently, it is useful to try different numbers and compare the results. There are different algorithms and their description is beyond this introductory paper, but all of them essentially rearrange the ties in the network into a predetermined number of subgroups so that the above mentioned criteria of internal density and external sparsity are fulfilled the best way possible. Afterwards, in order to check whether this partition is any good, the partition is compared (e.g., using correlation coefficient) to an ideal one with the same number of subgroups. This is important as the algorithm always produces some solution, no matter how bad it is and no matter if there actually are any subgroups or not (such as in very dense networks). Unlike cliques or k-plexes, factions are mutually exclusive, which means they do not overlap.

The role of subgroups has also been investigated in criminal networks. An influential idea was proposed by (Sageman, 2004) who postulated that jihadist terrorist networks (Al-Quaeda particularly) are organized into what he called a "cell-structure". Basically, the terrorist networks are supposed to be built up from small clique-like subgroups, with only very sparse interconnections between these subgroups. This is a result of a purposeful design, where these small cells allow for carrying out complex tasks, but they also allow for remaining secure from infiltration as within these groups, everyone knows everyone else. Although this idea needs to be empirically tested, some other studies have shown this structure in other networks. An example is the study of British suffragette network, which became more cell structured with their engagement in militant activi-

[8] In statistical physics or computer science literature on networks, the term community is used for these methods instead.

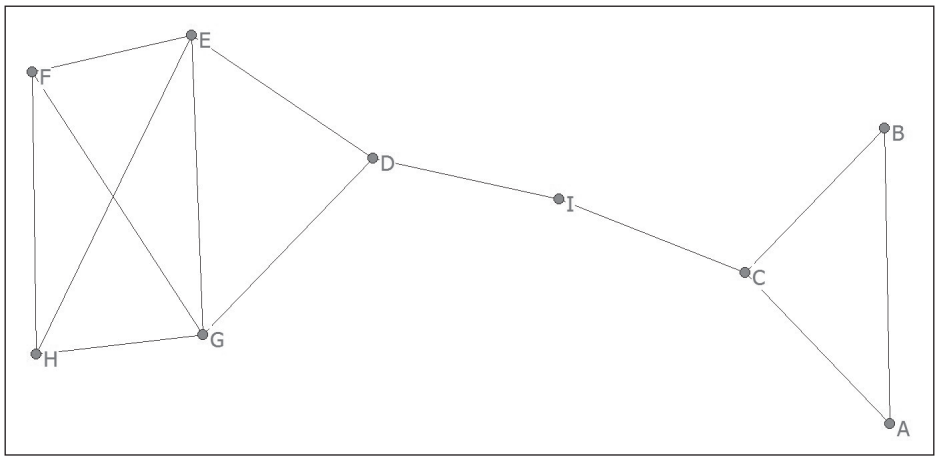

Figure 7: A network with 3 cliques – one contains four nodes (E, F, G, H), two contain three nodes (A, B, C and D, E, G)

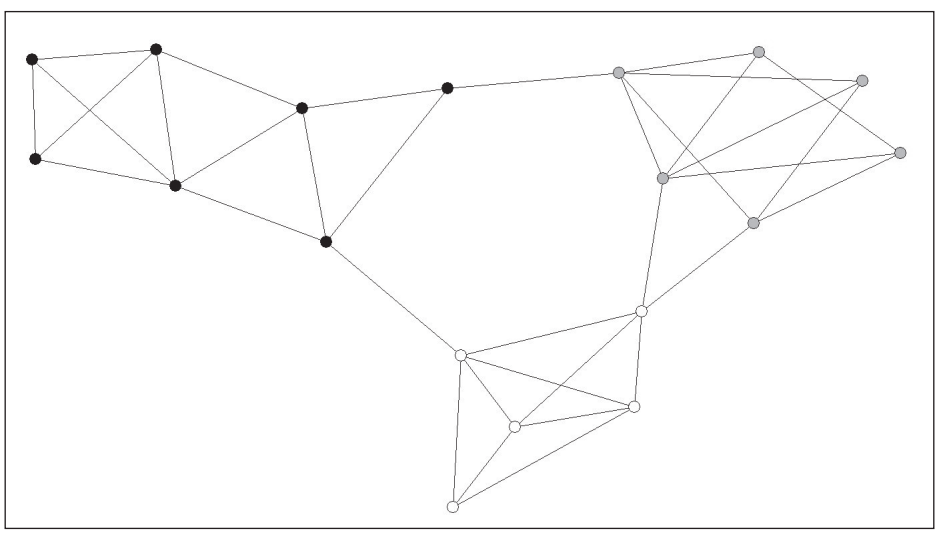

Figure 8: A network with 3 identified factions distinguished with different colors of nodes

ties (Crossley, Edwards, Harries, & Stevenson, 2012). In other studies using the factions approach, subgroups were found to be an important structural feature in Russian mafia outpost in Italy (Varese, 2012) or in Calabrian N'dranghetta, where they corresponded with formal organisation units called "locali" or their unions (Calderoni, Brunetto, & Piccardi, 2017). A sparse subgroup of brokers with high betweenness was identified as crucial for distribution of illegal steroids among other subgroups of professional athletes (Athey & Bouchard, 2013).

Statistical models of networks

Methods we have introduced so far are descriptive measures for the whole structure, substructures, and individual nodes in networks. However, there is also a large set of methods which go beyond description. These network models allow for capturing irregularities in human behaviour and action, assessing the influence of randomness on network structures, testing various hypotheses on processes and mechanisms which form social networks, and for simplifying some highly complex network structures (Robins, Pattison, Kalish, & Lusher, 2007). The development of these models have been vigorous in recent years (Snijders, 2011) and researchers of criminal networks may greatly benefit from this development in order to provide more empirically based explanations of organized crime. Nevertheless, there is a huge gap between descriptive measures and models of networks, which require nontrivial knowledge of statistics and which are both conceptually and computationally more elaborated. Hence, the following section only briefly introduces the most frequently used models, their principles and criminological applications[9].

An immediate question may arise – why should we not just apply standard statistical models we use regularly in social sciences (e.g., various general linear models)? There are two main reasons why standard statistical models are not sufficient to model networks. The first reason is the violation of the assumption of independence of observations. This is a basic assumption of standard statistics, but it is by definition violated with network data – after all, networks are all about interdependencies of nodes. For instance, if we remove a node from a network, its removal also changes centralities of other nodes in the network. The second reason is the requirement of random sampling. In network analysis, we do not usually work with random samples drawn from a population. Instead, we are typically dealing with case studies of a few networks or even just one. However, inference may still be useful in such cases – we are just not trying to infer about a population of networks, but rather aim for inferences about certain mechanisms or processes in our studied cases (Snijders, 2011).

The simplest way to handle these difficulties is to accommodate regular statistical tools for inference to non-independent data. Methods for computation of effects remain the same (e.g., correlation or regression), we only use different way to estimate statistical significance. This is what the *quadratic assignment procedure* (QAP) does. QAP works like permutation tests – it "reshuffles" randomly the labels of nodes in the network many times (usually from one to ten thousand times), which yields a distribution of possible outcomes (say, a correlation between the degree of nodes and their age). If there is just a small fraction of such randomly obtained results which are equal or more extreme than our empirical correlation (5% is equivalent to the p-value of 0.05), we deem the result unlikely to just be a result of chance and therefore we consider it significant[10]. QAP based regression models may be useful, especially in modelling valued networks (Campana,

[9] A very accessible brief overview can be found in respective chapter of Borgatti et al. (2013). More detailed overview of statistical models of social networks with technical details is provided by Snijders (2011).

[10] Detailed, yet very clear description of the whole procedure is given in Borgatti et al. (2013: 126–133) or in Robins (2015: 190).

2016). An example of application of QAP multiple regression is given by (Campana & Varese, 2013), who studied the impact of kinship ties and violence on cooperation among Mafiosi from Russian and Neapolitan mafia groups. They found that both these factors enforce cooperation, though the effect of violence is much stronger than the effect of kinship. Another proof of usefulness of QAP is a study by (Grund & Densley, 2012), who found that ethnically similar gang members tend to commit similar types of offences.

Models using the QAP deal with the network structure by accounting for it with different way of estimating statistical significance. However, the structure itself plays little role as it is not explicitly modelled. We introduce three broader sets of models, which all explicitly model the structure of the network rather than merely control for it. These sets of models are blockmodels, exponential random graph models, and stochastic actor-oriented models.

In networks, two nodes may have ties of the same strength to the same nodes. If we would swap such nodes, the structure of the network wouldn't change. We say that these two nodes are structurally equivalent (Lorrain & White, 1971)[11]. The principal idea behind *blockmodels* is that it is possible to reduce the network structure to mutually exclusive sets of equivalent nodes (called positions) and ties among them (called roles; Diviák, 2017; Doreian, Batagelj, & Ferligoj, 2004). Blocks are pairs of positions and ties between them – this way, we do not only model subsets of nodes (like in the subgroup detection), but also relations among them and thus the structure as well. This reduction yields a simplified picture of the network, which captures its essential features. Since exact structural equivalence is rare in empirical networks, in practice, we usually measure the extent of (dis)similarity of ties between each pair of nodes within the network and subsequently, we apply one of many blockmodelling algorithms. These algorithms are in essence akin to what is known from standard statistics as cluster analysis or classification[12]. They partition the network into positions, within which nodes are similar to each other and between these positions, nodes are dissimilar. Subsequently, the quality of the resulting partitioning (that is the extent of internal homogeneity and external heterogeneity of positions) is assessed with so-called measures of adequacy. The entire procedure of blockmodelling can be done in two general ways. One way is exploratory, which is much like for example in hierarchical cluster analysis, where we try numerous different partitions and algorithms trying to come up with a meaningfully interpretable solution. The other way is confirmatory, where an analogy can be made with latent class analysis, where we start with a theory about how a network should be partitioned and then we investigate, whether this theoretical blockmodel fits our empirical data or not. To give an example, one very well explored blockmodel is the core/periphery structure (Borgatti & Everett, 1999). It consists of two sets of nodes – core and periphery. Core is basically a clique – every member has ties to all others. Peripheral nodes have ties only to the nodes in the core and no ties within the periphery. In criminal networks, this model has been found to capture the structure of the inner circle of the Provisional Irish Re-

[11] There are also other, less restrictive, definitions of equivalence, such as regular or stochastic. For the sake of simplicity, we will consider only the structural variant here. More on the other definitions can be learned in a chapter by (Batagelj, Doreian, & Ferligoj, 2011).

[12] As a matter of fact, clustering algorithms may be used for blockmodelling as well with some adjustments (Robins, 2015).

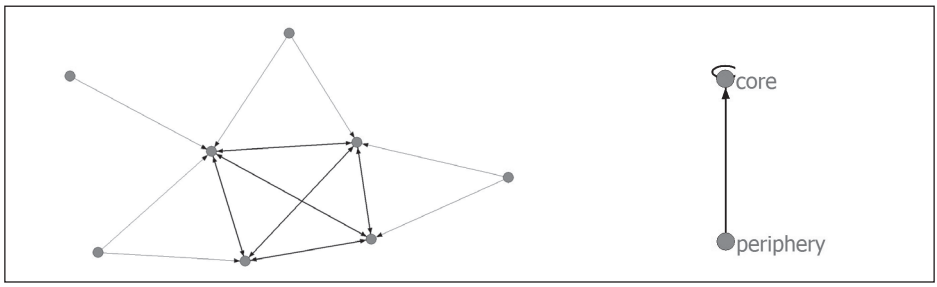

Figure 9: A core/periphery structured network (core is composed of the square of nodes in the middle) and its blocked image graph. Note that the image graph, unlike directly observed networks, contains a self-loop for the core, indicating that it is a cohesive subset, with many ties within the group.

publican Army, where the core consisted of experienced members and was solidified over time (Stevenson & Crossley, 2014). Another case of core/periphery structure was a Czech political corruption affair, where politicians formed a dense core and ad hoc cooperated with businesspeople to manipulate public contracts (Diviák et al., 2017).

A different approach to model the network structure is represented by the *exponential random graphs models* (ERGM)[13]. Instead of grouping nodes on the basis of similarity in their ties, ERGMs are based on the idea that network structure is built by overlapping, intertwining, and cumulating of micro network substructures called configurations. There are numerous hypothetical configurations which can be modelled, ranging from simple ties and reciprocated ties to various forms of triadic closure (see the Figure 10 below). These configurations represent theoretical mechanisms or processes, for example, reciprocated tie represent a tendency of actors to exchange transferred resources in the network or triangle represents a tendency of actors to collaborate if they share a common third collaborator. A contrast between blockmodeling and ERGM is that the former may tend to discover large-scale features of the groups, defined by large subsets of nodes, whereas the configurations in the ERGM are of a local nature. Roughly, ERGMs work in a way similar as logistic regression (Grund & Densley, 2014) – predicting the empirical network based on the presence of ties patterned in configurations. If a resulting parameter is significant and positive, it means that the corresponding configuration is present more than just by a chance in the network and if the parameter is significantly negative, then the corresponding configuration is present less than we would expect randomly. A theoretically interesting benefit of ERGMs is the fact, that they can disentangle the network structure by separating the influence of competing mechanisms (represented by configurations) which may work simultaneously. We may for example have a drug distribution network, which is descriptively highly centralized, but when we fit an ERGM with a star parameter (representing activity of actors) and a triangle parameter (representing closure, i.e., the tendency of two distributors to collaborate if they share a common third collaborator), we may get a result with insignificant star parameter and significant triangle parameter suggesting that the observed centralization is not the effect of frequent

[13] A comprehensive and detailed account for ERGMs is given in a book by Lusher, Koskinen, and Robins (2013).

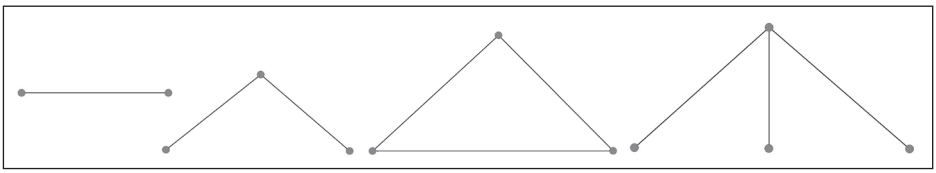

Figure 10: Some basic ERGM network configurations (from left to right) – tie, 2-path, triangle, and 3-star

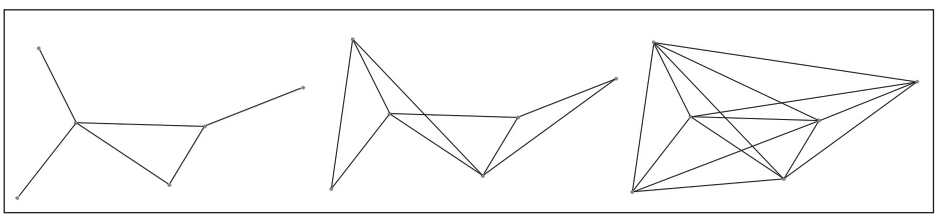

Figure 11: A dynamic network at three time points (from left to right) t1, t2, and t3

activity of particular individuals, but rather, it is a result of working together in closed structures (e.g., in order to keep each other "in check"), which happen to frequently include particular actors resulting in centralization. ERGMs have been used to show that co-offenders in a street gang are more likely to commit illicit behaviour if they share an ethnic background and even more so, when the tendency towards closure among ethnically homogenous gang members is taken into account (Grund & Densley, 2014). Another example is a study of prohibition era Chicago organized crime scene by (Smith & Papachristos, 2016), who found strong effects of both legitimate (e.g., business) and personal (e.g., kinship) ties on criminal activity. Helfstein and Wright (2011) applied ERGMs to test two competing theories about the structure of terrorist networks and found support for neither of them – modelled networks displayed no tendencies towards heavily centralized structures as well as no tendencies towards open non-redundant structures. Instead, they all exhibited strong tendencies towards decentralization and triadic closure. No matter how powerful ERGMs are, they are so far implemented mainly for binary networks. Also, their estimation may be rather lengthy due to simulations used for estimating significance of parameters.

All the models we have introduced so far treat the network structure as static. However, networks are dynamic and change over time. A dynamic network is a network with the same set of nodes measured over multiple periods of time. This allows for tracking the change of the network over time. The question is whether such changes (typically, a creation or dissolution of a tie) are an outcome of random fluctuation or if they are driven by some process. *Stochastic actor-oriented models* (SAOM[14]; Snijders, van de Bunt, & Steglich, 2010) have been developed as a tool to model changes in the network over time.

[14] These models are sometimes referred to as SIENA (Simulation Investigation of Empirical Network Analysis) models due to the name of the software they were first implemented in.

SAOMs are built up on the same underlying principle as ERGMs – network structure is modelled from configurations representing theoretical mechanisms/processes. Changes between two successive time points are decomposed into microsteps – each actor is given an option to create or remove a tie. The probability of an actor creating or dropping a tie is then modelled in a similar way as in ERGMs. SAOMs have been for example applied to show how a drug trafficking network evolves over time towards closed triangles to facilitate trust and simultaneously towards longer distances to assure security (Bright, Malm, Koskinen, & O'Connor, 2014).

Challenges for criminal network analysis

There are three challenges, which every researcher in the field of criminal network analysis as well as the field as a whole has to face (Morselli, 2014). The three challenges are data, methods, and theories. These challenges sometimes constrain the research to some extent on one hand, but on the other hand, finding solutions to these problems may help the development of this area of research and our understanding of organized crime.

The problem of data availability and validity is a severe one. In network context, this becomes especially problematic, because one Achilles' heel of the whole approach is its sensitivity to missing data. This is especially problematic for covert networks. If we miss important actors (such as brokers), the picture of the network may alter drastically and as a result, we will draw invalid conclusions from our analysis. Similarly, if we miss important ties (such as a bridge connecting two otherwise unconnected segments of the network), we may incorrectly deduce that there are two unconnected groups which have no way how to cooperate. It is therefore important to consider the validity, reliability, and quality of possible data sources. Bright and colleagues (2012) compared five different data sources – offender databases, transcripts of physical or electronic surveillance, summaries of police interrogation, transcripts of court proceedings and online or print media. With the exception of online or print media, all these sources are not usually publicly or freely accessible. But even if they are, they are not flawless – some offenders might have not yet been caught and thus they are not in the databases, criminals may limit their communication using cover language (e.g., nicknames) and not mention crucial information in their phone calls, and during interrogation or trials offenders may lie or hold up information to avoid sentencing. While the media-based sources may be freely available, extra caution needs to be taken in order assure data validity. In highly attractive cases (e.g., with the involvement of politicians or other public figures), media coverage may create a spotlight effect and concentrate their reports disproportionately on the well-known offenders. This concentration as a result may lead to a centralized network structure, but the reality may be very different and, again, incorrect conclusions may be drawn. While this spotlight effect can be assessed in modelling (as shown by Smith & Papachristos, 2016), there is no specific way how to deal with it. General advice is to process the data as carefully as possible. This can be helped by content analysis of the sources (van der Hulst, 2009), which allows for transparent coding, recoding, and comparisons of categories. Suspicious as well as solid information may become more visible and the reliability of the procedure can be checked by another independent coder.

Regarding the second challenge, the use of methods, there are two possible ways of improvement of the analytical tools at our disposal. One way is the use of statistical modelling of networks, the other is qualitative analysis as a complement to the SNA. We have briefly covered the basics of statistical modelling of networks and underlined its usefulness and potential for the field of criminal network analysis, which has been predominantly descriptive so far. Mixed methods approach, where various qualitative analysis methods accompany SNA, has also been recently discussed as a way to improve the way we study networks (Bellotti, 2014; Domínguez & Hollstein, 2014). The mixed methods approach is potentially fruitful especially when details can be obtained, from the actors themselves, from well-placed informants, or from intelligence sources on how actors themselves perceive, plan, and reflect their network positions and attributes (Hollstein, 2014). We have talked about strategic positioning from network point of view, but the question is how actors experience such situation (do they really think about reducing redundant connections or are they just trying to not "go too far"?). Furthermore, combining qualitative findings (e.g., from interviews or an ethnographic study) with quantitative results of SNA may either corroborate our results, fill in some gaps or we may even come to a contradiction. Imagine a situation where we are studying networks of mobile phone communication of a criminal group at two points of time. With SNA alone, we may come to a result that at the first time point, the structure was dense and centralized, while in following time point, it changed drastically and became sparse and decentralized. We may conclude that such a change was caused by a lot of actors deciding to terminate their criminal activity in fear of being arrested amidst of ongoing investigation. However, a qualitative analysis of interrogation records or maybe a participant observation may reveal, that it was not the case – the participants just shifted their communication from mobile phones to face-to-face. Thus, mixed methods provides better understanding of the phenomena we study as it brings more insight into the context and meaning of what is going on in the networks we describe formally (Stevenson & Crossley, 2014). The difficulty with mixed methods studies is the fact that they are very demanding in terms of time, money, and skills of researchers (Hollstein, 2014).

The last challenge for network criminology is the theory-building. There are some researchers, who deem the whole field to be rather devoid of theory or primarily driven by data rather than theory (Bright et al., 2012; Carrington, 2011; van der Hulst, 2011). A proper theory should start with the individual action as the individual level is the locus of intentionality (Coleman, 1990; Robins, 2009). While the SNA is all about structures of interactions, they are necessarily based in the individual interaction and relations with others. One relatively new approach to theorizing about social world is analytical sociology (Hedström, 2005; Hedström & Bearman, 2011). Analytical sociology seeks to explain how social structures (in our case, criminal networks) are brought about by individual action and interaction (e.g., cooperation on a criminal task). It emphasizes that social scientists should look for mechanisms in order to formulate useful explanations of social phenomena. "Mechanism approach is that we explain a social phenomenon by referring to a constellation of entities and activities, typically actors and their actions, that are linked to one another in such a way that they regularly bring about the type of phenomenon we seek to explain." (Hedström, 2005: 2). As we can see from this definition, analytical sociology is often concerned with actors and their relations similarly to SNA.

There is a synergy which could be explored further and help network criminologists in theoretical explanations of organized crime.

Conclusion

We have introduced basic concepts and descriptive measures of SNA together with more advanced models of networks and we have illustrated this with various criminological applications. We have also foreshadowed three big challenges for criminal network analysis. In case it motivates for reading further, there have recently been books with studies employing SNA in criminological research. Accessible showcase of a few studies and a reflection of network criminology is given by (Morselli, 2009) in his *Inside Criminal Networks*. Intermediary readers may find more examples in compilations *Crime and Networks* (Morselli, 2014a), *Illuminating Dark Networks* (Gerdes, 2015) and *Disrupting Criminal Networks* (Bichler & Malm, 2015). Cutting edge network papers with criminological background are occasionally published in the *Social Networks* journal (with a recent special issue on criminal networks) and conversely, some criminological journals occasionally publish papers which use SNA, notably *Trends in Organized Crime* (special issue in 2009) and *Global Crime* (special issue in 2013). In case readers are not only motivated to further reading, but also for conducting SNA on their own, there is specialised software, which provides the tools for both visualization and analysis of networks. *UCINET* (Borgatti, Everett, & Freeman, 2002) is relatively user friendly and is accompanied by an introductory book (Borgatti et al., 2013) and an online textbook (Hanneman & Riddle, 2005), there is also *Pajek* (Batagelj & Mrvar, 1996) with slightly different functionalities and a nice book (Mrvar, de Nooy, & Batagelj, 2005), and for those familiar with the R statistical environment, there is a package called *statnet* (Handcock, Hunter, Butts, Goodreau, & Morris, 2003) with a hands-on introduction (Luke, 2015).

Even though the study of criminal networks is in its infancy, its future seems to be promising. This field of inquiry has been steadily cumulating findings from case studies, which have already led to discoveries of some common patterns in criminal networks. This effort may be further supported by the adoption of more sophisticated methods and more profound theories, both of which are being vividly developed in related areas of social sciences. In return, network criminologists offer an uncharted territory with unique research problems which may stimulate new theoretical and methodological endeavour. Lastly, organized crime is a phenomenon with great implications for policy-making and interventions. The network approach can contribute to make these policies and interventions more evidence-based.

REFERENCES

Athey, N. C., & Bouchard, M. (2013). The BALCO scandal: the social structure of a steroid distribution network. *Global Crime*, *14*(2/3), 216–237. https://doi.org/10.1080/17440572.2013.790312

Batagelj, V., Doreian, P., & Ferligoj, A. (2011). Positions and Roles. In J. Scott & P. J. Carrington (Eds.), *The SAGE Handbook of Social Network Analysis* (pp. 434–447). SAGE.

Batagelj, V., & Mrvar, A. (1996). *Pajek – Program for Large Network Analysis.* Retrieved from http://vlado.fmf.uni-lj.si/pub/networks/pajek/

Bellotti, E. (2014). *Qualitative Networks*. London: Routledge.
Bichler, G., & Malm, A. (2015). *Disrupting Criminal Networks*. Boulder ; London: Lynne Rienner Publishers.
Borgatti, S. (2005). Centrality and network flow. *Social Networks*, *27*(1). Retrieved from https://works.bepress.com/steveborgatti/3/
Borgatti, S. P., & Everett, M. G. (1999). Models of core/periphery structures. *Social Networks*, *21*(4), 375–395. https://doi.org/10.1016/S0378-8733(99)00019-2
Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *UCINET 6 for Windows: Software for Social Network Analysis*. Harvard: Analytic Technologies.
Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2013). *Analyzing Social Networks*. SAGE publications.
Bright, D., Hughes, C., & Chalmers, J. (2012). Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, Law & Social Change*, *57*(2), 151–176. https://doi.org/10.1007/s10611-011-9336-z
Bright, D. A., Greenhill, C., Ritter, A., & Morselli, C. (2015). Networks within networks: using multiple link types to examine network structure and identify key actors in a drug trafficking operation. *Global Crime*, *16*(3), 219–237. https://doi.org/10.1080/17440572.2015.1039164
Bright, David A. (2015). Disrupting and Dismantling Dark Networks. In L. M. Gerdes (Ed.), *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations* (pp. 39–52). Cambridge University Press.
Bright, David A., Malm, A., Koskinen, J., & O'Connor, A. (2014). Criminal network dynamics: The formation and evolution of a drug trafficking network. Presented at the Illicit Networks Workshop, Adelaide.
Calderoni, F. (2012). The structure of drug trafficking mafias: the 'Ndrangheta and cocaine. *Crime, Law & Social Change*, *58*(3), 321–349. https://doi.org/10.1007/s10611-012-9387-9
Calderoni, F., Brunetto, D., & Piccardi, C. (2017). Communities in criminal networks: A case study. *Social Networks*, *48*, 116–125. https://doi.org/10.1016/j.socnet.2016.08.003
Campana, P., & Varese, F. (2013). Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and Society*, *25*(3), 263–289. https://doi.org/10.1177/1043463113481202
Campana, Paolo. (2016). Explaining criminal networks: Strategies and potential pitfalls. *Methodological Innovations*, *9*, 2059799115622748. https://doi.org/10.1177/2059799115622748
Carley, K. M., Lee, J.-S., & Krackhardt, D. (2002). Destabilizing Networks. *Connections*, *24*(3), 79–92.
Carrington, P. J. (2011). Crime and Social Network Analysis. In *The SAGE Handbook of Social Network Analysis* (Vol. 2011, pp. 236–255).
Coleman, J. (1990). *Foundations of Social Theory*. Cambridge, MA: Belnap Press.
Crossley, N., Edwards, G., Harries, E., & Stevenson, R. (2012). Covert social movement networks and the secrecy-efficiency trade off: The case of the UK suffragettes (1906–1914). *Social Networks*, *34*(4), 634–644. https://doi.org/10.1016/j.socnet.2012.07.004
Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160–175. https://doi.org/10.1080/17440572.2012.702523
Diviák, T. (2017). Ekvivalence a blokové modelování v analýze sociálních sítí – praktický úvod. *Naše Společnost*, (forthcoming).
Diviák, T., Dijkstra, J. K., & Snijders, T. A. B. (2017). Structure, Multiplexity, and Centrality in a Corruption Network: The Czech Rath Affair. *Trends in Organized Crime*, (under review).
Domínguez, S., & Hollstein, B. (2014). *Mixed Methods Social Networks Research*. Cambridge: Cambridge University Press.
Doreian, P., Batagelj, V., & Ferligoj, A. (2004). *Generalized Blockmodeling*. Cambridge ; New York: Cambridge University Press.
Duijn, P. A. C., Kashirin, V., & Sloot, P. M. A. (2014). The Relative Ineffectiveness of Criminal Network Disruption. *Scientific Reports*, *4*. https://doi.org/10.1038/srep04238
Everton, S. F. (2012). *Disrupting Dark Networks*. Cambridge: Cambridge University Press.
Fortunato, S. (2010). Community detection in graphs. *Physics Reports*, *486*(3–5), 75–174. https://doi.org/10.1016/j.physrep.2009.11.002
Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks*, *1*(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

Gerdes, L. M. (2015). *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations*. Cambridge: Cambridge University Press.
Grund, T. U., & Densley, J. A. (2012). Ethnic heterogeneity in the activity and structure of a Black street gang. *European Journal of Criminology*, *9*(4), 388–406. https://doi.org/10.1177/1477370812447738
Grund, T. U., & Densley, J. A. (2014). Ethnic Homophily and Triad Closure: Mapping Internal Gang Structure Using Exponential Random Graph Models. *Journal of Contemporary Criminal Justice*, 1043986214553377. https://doi.org/10.1177/1043986214553377
Handcock, M. S., Hunter, D. R., Butts, C. T., Goodreau, S. M., & Morris, M. (2003). *statnet: Software tools for the Statistical Modeling of Network Data*. Retrieved from http://statnetproject.org
Hanneman, R., & Riddle, M. (2005). Introduction to Social Network Methods. Retrieved April 3, 2016, from http://faculty.ucr.edu/~hanneman/nettext/
Hedström, P. (2005). *Dissecting the Social: On the Principles of Analytical Sociology* (1st edition). Cambridge: Cambridge University Press.
Hedström, P., & Bearman, P. (Eds.). (2011). *The Oxford Handbook of Analytical Sociology* (1 edition). Oxford; New York: Oxford University Press.
Helfstein, S., & Wright, D. (2011). Covert or Convenient? Evolution of Terror Attack Networks. *Journal of Conflict Resolution*. https://doi.org/10.1177/0022002710393919
Hofmann, D. C., & Gallupe, O. (2015). Leadership protection in drug-trafficking networks. *Global Crime*, *16*(2), 123–138. https://doi.org/10.1080/17440572.2015.1008627
Hollstein, B. (2014). Mixed Methods for Social Networks Research: An Introduction. In S. Domínguez & B. Hollstein (Eds.), *Mixed Methods Social Networks Research* (pp. 3–35). Cambridge: Cambridge University Press.
Krebs, V. (2002). Uncloaking Terrorist Networks. *First Monday*, *7*(4). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/941
Le, V. (2012). Organised Crime Typologies: Structure, Activities and Conditions. *International Journal of Criminology and Sociology*, *1*(0), 121–131.
Lorrain, F., & White, H. C. (1971). Structural equivalence of individuals in social networks. *The Journal of Mathematical Sociology*, *1*(1), 49–80. https://doi.org/10.1080/0022250X.1971.9989788
Luke, D. A. (2015). *A User's Guide to Network Analysis in R*. New York: Springer International Publishing.
Lusher, D., Koskinen, J., & Robins, G. (Eds.). (2013). *Exponential random graph models for social networks: theory, methods, and applications*. Cambridge: Cambridge University Press.
McGloin, J. M., & Kirk, D. S. (2010). An Overview of Social Network Analysis. *Journal of Criminal Justice Education*. https://doi.org/10.1080/10511251003693694
McIlwain, J. S. (1999). Organized crime: A social network approach. *Crime, Law & Social Change*, *32*, 301–323.
Milward, H. B., & Raab, J. (2006). Dark Networks as Organizational Problems: Elements of a Theory. *International Public Management Journal*, *9*(3), 333–360. https://doi.org/10.1080/10967490600899747
Moreno, J. L. (1934). *Who Shall Survive?* Washington, D.C.: Nervous and Mental Disease Publishing Company.
Morselli, C. (2010). Assessing Vulnerable and Strategic Positions in a Criminal Network. *Journal of Contemporary Criminal Justice*, *26*(4), 382–392. https://doi.org/10.1177/1043986210377105
Morselli, C. (2009). *Inside Criminal Networks* (Vol. 8). New York, NY: Springer New York.
Morselli, C. (2014a). *Crime and Networks*. New York: Routledge.
Morselli, C. (2014b). Introduction. In *Crime and Networks* (pp. 1–9). Routledge.
Morselli, C. Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*, *29*(1), 143–153. https://doi.org/10.1016/j.socnet.2006.05.001
Morselli, C., & Roy, J. (2008). BROKERAGE QUALIFICATIONS IN RINGING OPERATIONS*. *Criminology*, *46*(1), 71–98. https://doi.org/10.1111/j.1745-9125.2008.00103.x
Mrvar, A., de Nooy, W., & Batagelj, V. (2005). *Exploratory Social Network Analysis with Pajek*. Cambridge: Cambridge University Press.
Newman, M. (2010). *Networks: An Introduction* (1 edition). Oxford ; New York: Oxford University Press.
Newman, M. E. J., & Park, J. (2003). Why social networks are different from other types of networks. *Physical Review E*, *68*(3). https://doi.org/10.1103/PhysRevE.68.036122

Oliver, K., Crossley, N., Everett, M. G., Edwards, G., & Koskinen, J. (2014). Covert networks: structures, processes and types. The Mitchell Center for Social Network Analysis working paper. Retrieved from http://www.socialsciences.manchester.ac.uk/medialibrary/research/mitchell/covertnetworks/wp/working_paper1.pdf

Papachristos, A. V. (2014). The Network Structure of Crime.

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. https://doi.org/10.1007/s12117-008-9059-4

Robins, G. (2015). *Doing Social Network Research*. London: SAGE publications.

Robins, G., Pattison, P., Kalish, Y., & Lusher, D. (2007). An introduction to exponential random graph (p*) models for social networks. *Social Networks*, *29*(2), 173–191. https://doi.org/10.1016/j.socnet.2006.08.002

Sageman, M. (2004). *Understanding Terror Networks* (1St Edition edition). Philadelphia: University of Pennsylvania Press.

Smith, C. M., & Papachristos, A. V. (2016). Trust Thy Crooked Neighbor Multiplexity in Chicago Organized Crime Networks. *American Sociological Review*, 0003122416650149. https://doi.org/10.1177/0003122416650149

Snijders, T. A. B. (2011, July 8). Statistical Models for Social Networks [review-article]. Retrieved December 10, 2016, from http://www.annualreviews.org/doi/abs/10.1146/annurev.soc.012809.102709

Snijders, T. A. B., van de Bunt, G. G., & Steglich, C. E. G. (2010). Introduction to stochastic actor-based models for network dynamics. *Social Networks*, *32*(1), 44–60. https://doi.org/10.1016/j.socnet.2009.02.004

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, *13*(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-H

Stevenson, R., & Crossley, N. (2014). Change in Covert Social Movement Networks: The "Inner Circle" of the Provisional Irish Republican Army. *Social Movement Studies*, *13*(1), 70–91. https://doi.org/10.1080/14742837.2013.832622

van der Hulst, R. C. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in Organized Crime*, *12*(2), 101–121. https://doi.org/10.1007/s12117-008-9057-6

van der Hulst, Renée C. (2011). Terrorist Networks: The Threat of Connectivity. In *The SAGE Handbook of Social Network Analysis* (pp. 256–270).

Varese, F. (2012). The Structure and the Content of Criminal Connections: The Russian Mafia in Italy. *European Sociological Review*, jcs067. https://doi.org/10.1093/esr/jcs067

von Lampe, K. (2009). Human capital and social capital in criminal networks: introduction to the special issue on the 7th Blankensee Colloquium. *Trends in Organized Crime*, *12*(2), 93–100. https://doi.org/10.1007/s12117-009-9067-z

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications* (1 edition). Cambridge ; New York: Cambridge University Press.

Wood, G. (2017). The structure and vulnerability of a drug trafficking collaboration network. *Social Networks*, *48*, 1–9. https://doi.org/10.1016/j.socnet.2016.07.001

Xu, J., & Chen, H. (2008). The topology of dark networks. *Communications of the ACM, 51*(10), 58. https://doi.org/10.1145/1400181.1400198