This is an Accepted Manuscript of a book chapter published by Routledge in **The Routledge International Handbook of Forensic Intelligence and Criminology** on 2018, available online: https://www.routledge.com/The-Routledge-International-Handbook-of-Forensic-Intelligence-and-Criminology/Rossy-Decary-Hetu-Delemont-Mulone/p/book/9781138688216

The Contribution of Forensic Science to the Analysis of Crime Networks

Quentin Rossy, École des sciences criminelles, Université de Lausanne, Switzerland

Carlo Morselli, Centre international de criminologie comparée (CICC), Université de Montréal, Canada

Abstract

This chapter presents network analysis methodologies used in crime and criminal justice research and as part of the intelligence analysis process. It starts with the foundations of the network analysis of crime in computer science, policing and sociology that have led to the 'link analysis' and the 'social network analysis' approaches. It then addresses some of the general methodological recommendations, misconceptions and limitations of these approaches to analysing criminal networks of offenders. Finally, the contributions of forensic science to the reconstruction of crime networks are examined in regard to the potential of using traces to infer relationships among actors, the presence of unknown linked entities and the identification of their characteristics.

Introduction

Analysing crime data to detect patterns relies on the ability of practitioners and researchers to deconstruct the problem into simple parts. To do so, networks are commonly used as convenient models. Two methodologies that are based on graph-like models have merged over time: 'link analysis' and 'social network analysis' (SNA). In this chapter, we start with the historical foundations of these approaches, which may be found in computer science, policing, sociology and legal science. As a descriptive model, networks are more often than not used to model criminal networks of offenders, but practices and research have proven that their scope may be broadened. We therefore discuss some ideas and misconceptions about

their uses and present some general methodological recommendations. Finally, the contributions of forensic science to reconstructing crime networks are examined in regard to the potential of using traces to infer relationships among actors, the presence of unknown linked entities, and the identification of their characteristics.

The Network Dimension of Crime

Networks as models to describe and analyse crime or deviant activities are based on the root principle that such activities can be modelled by a graph of entities connected by relationships. This model aims to detect, collate and interpret the ties between relevant entities (e.g., persons, events, locations). It supports the reconstruction of a criminal activity that may involve a complex set of individuals and events and the inference of the roles or influences of a network structure to the realization of a criminal activity. Networks, like other models, are used to facilitate the analysis of complex problems. Formalized by Chen (1976), the entity-relationship model offers a unified and natural view of the real world. He defines an entity 'as a "thing" which can be distinctly identified and relationships are associations among entities' (Chen 1976, 10). An entity is thus a thing having a separate and identifiable existence.

This model was published nearly at the same time as Harper and Harris's (1975) paper, which defines 'link analysis' as the core method for criminal intelligence analysis in policing. They attribute the earliest application of the approach—in engineering—to Gilberth and Gilberth (1917) (cited in Harper and Harris 1975) and they suggest its application to describe organized crime problems. The link analysis approach is a qualitative method to describe organized crime structures with nodes and edges. In fact, graph-based techniques have been exploited since the nineteenth century to model data gathered during an investigation. They can be found in the work of John Henry Wigmore, whose method inspired the argument diagramming in which nodes represent facts and assumptions linked with causal relationships (Wigmore 1913).

Akin to the link analysis framework is the concept of social network, which, in the social sciences, is defined as 'a set of socially relevant nodes connected by one or more relations' (Marin and Wellman 2011, 11). Individuals and organizations are the most common classes of

entities analysed in the social network approach. The concepts of ‘nodes’, ‘actors’ or ‘entities’ are often used as synonyms. Here we use the concept of ‘entity’ as a distinctly identified part of the reality (e.g., a person, an event or a location) and the notion of ‘node’ as its representation in the network model. The social network approach aims at modelling and studying patterns of relationships between entities and not only their characteristics. ‘The unit of analysis in network analysis is not the individual, but an entity consisting of a collection of individuals and the linkages among them’ (Wasserman and Faust 1994, 5). A network, by itself, is thus an entity embedding a set of interconnected entities. But networks are not the same as groups (Marin and Wellman 2011), which are classifications of a particular type of thing in a common set or a particular discrete group membership. The social network approach is thus a particular modelling process where an object of study is defined with an entity-relationship model to describe the social phenomena.

General overviews of social network analysis, such as Marin and Wellman (2011) and Wasserman and Faust (1994) classify the exploitation of the network model in two main categories. For a recent review of the multiple contributions of SNA to criminology, see Bouchard and Malm (2016). On the one hand, a network can be considered as a dependent variable, which may be explained by a theory of causation. On the other hand, it may be considered as the independent variable leading to a particular phenomenon. In this latter scenario, the social network approach is based on the hypothesis that causation is attributable to social structures and not located in the traditional individual attributes that have formed the basis of social science explanatory models. Thus, the roots of criminal activities may be explained by the relationships between social entities (e.g., personal relationships, opportunities or community settings) and not solely by their intrinsic attributes (e.g., gender or age): ‘More than a set of methods—it is an orientation toward the understanding of human behaviour that focuses on the importance of social relations and their consequence’ (McGloin and Kirk 2010, 210). From a formal perspective, modern social networks find their origins in anthropology and sociology, in particular in the sociometric models pioneered by Jacob L. Moreno and Helen Jennings (Jennings 1943; Moreno 1932 and 1934; see Freeman 2004 for a historical overview of their collaborative work). This approach relies on a network model combined with the use of mathematical measures describing the global structure of the network or the structural importance of its nodes.

In criminology, the network model has been used both to describe (as a dependent variable) and to explain (as an independent variable) crime (Papachristos 2011, 2014). McGloin and Kirk (2010) and Carrington (2011) state that the social network approach is at the crossroads between Sutherland's differential association theory and Hirschi's social control theory. Social networks are seen as a key predicator of crime: 'one of the most robust findings in the field of criminology, namely that the bulk of delinquency is carried out in groups' (McGloin and Kirk 2010, 209). Sutherland (1939) formulated that criminal behaviours, rationalizations and attitudes are learned in the context of overly positive associations with offenders. This was extended into Akers learning theory (1998); he proposed a social structure model to categorize the factors influencing deviant actions: the social organization or community, the socio-demographic characteristics of individuals and groups, the social disorganization or group conflict and, finally, the social location in groups. It is this latter social structure that is typically modelled by a network approach. Carrington (2011) argues that both Sutherland's differential association theory and Hirschi's social control theory can be interpreted and tested with network models at a micro-level (i.e., the ego network of an individual). Furthermore, the network approach can also be applied to the macro-level of communities or neighbourhoods in relation to social disorganization theory (see Carrington 2011) or even at the country level (see Boivin 2014). A social network approach can also integrate an analysis of individual's attributes, such as age and genre. One of the main concepts from this perspective is *homophily*, which refers to individuals in the same social network sharing similar demographic characteristics (Van Mastrigt and Carrington 2014; McPherson et al. 2001). In addition, Papachristos (2011) links the social network approach to opportunity theories, in the sense that 'everyday life is structured by peer groups and the availability of behavioural options in the group' (117). The assumption is that the network dimension of criminal activities generates opportunities (Morselli 2009). For instance, the social network approach may be combined with a geographical analysis through the analysis of the 'journey to associates' (Malm et al. 2008). Papachristos (2014) promotes the concept of 'social space' to describe how neighbourhoods and communities are more than just geographic concepts but are also related to the network dimension of crime.

As a descriptive model, social networks are more often than not used to model criminal networks of individuals involved in a shared illicit activity. Much research on criminal networks does not focus on the aetiology of crime but rather on the description of the

organization of a particular subgroup of individuals. The criminal network as an object of study leads to such questions as how to detect, to describe and to measure the regularities and patterns of social structures. Papachristos (2011) even argues that methods within the social network analysis repertoire could move past the descriptive model to the understanding of the generative processes or aetiology of criminal groups.

Analysing Criminal Networks

Analysing crime problems by their network dimension is commonly associated with the analysis of organized criminal networks to support criminal investigations that aim at developing disruption strategies (Strang 2014). Indeed, the use of link charts has emerged in criminal intelligence analysis as an investigative tool to structure information gathered during an investigation and to reconstruct the network of organized criminal groups (Harper and Harris 1975). Social network analysis methods have then been proposed to enrich the approach by the use of centrality metrics (Klerks 2001; Sparrow 1991). This has led to a narrow view of the overall scope of approaches. In this section, we discuss some ideas and misconceptions about their uses for both practical and research purposes.

Summarizing network analytic techniques as the description and analysis of complex organized criminal groups is an oversimplification. Indeed, for the last 20 years, many researchers have shown how these techniques can support the analysis of a broader range of crime problems and many lines of questioning. Extant research has shown that co-offending generally involves small groups that are not stable in time, which is contrary to the assumption that criminal groups are more often than not hierarchically structured (Hashimi et al. 2016; Morselli 2009; Reuter 1983). Indeed, the size of a network may be positively associated with the probability of detection. Small, flexible and ephemeral groups may be hypothetically more resilient (Reuter 1983). Research has shown that co-offending groups are not stable and are generally composed of two or three co-offenders (Hashimi et al. 2016). Duijn et al. (2014) show that criminal groups are often not characterized by a stable hierarchical structure but rather by a flexible organization. The more ways or paths a network has to achieve its goal, the more flexible and resilient it is to law enforcement actions against its actors (Morselli and Roy 2008). The flexibility of a network is related to its self-organizing capacities that result from its creation process. It relies on the development of interactions

between the multiple relationships that each actor of the network has (Morselli, 2009). This is the snowball effect described by Kleemans (2007).

It should be noted that the flexibility of a network as a core characteristic of its resilience does not necessarily imply that central actors are absent. Some actors may lead the activities or play a strategic intermediary role between unlinked actors. As key middlemen, known as brokers, they are said to control the flow of information and make others dependent on their activities (Freeman 1977). The key role of brokers has been studied in many areas, such as drug trafficking (Desroches 2005; Natarajan 2006; Pearson and Hobbs 2001; Zaitch 2002), illicit markets (Bruinsma and Bernasco 2004; Morselli and Roy 2008) and human trafficking (Kleemans 2007; Zhang 2008; Zhang and Chin 2002). They may spread the flexibility of the networks by their ability to contact several co-offenders to perform a specific task, thus increasing opportunities. It is worth noting that the key role of an actor may be unrelated to its direct centrality and more related to its functional roles within the criminal activity. The roles of actors are thus a key element in analysing criminal networks, leading to new frameworks for combining social network and script analysis (Bright et al. 2014; Morselli and Roy 2008).

The detection of central actors may serve to disrupt the functioning of a network by neutralizing key actors. But the examination of criminal networks may also aim at analysing the formation, composition and functioning of co-offending groups whether or not they are well structured (McGloin and Nguyen 2014). The focus is placed on the way criminal groups emerged and grew to settle prevention strategies: ‘the goal is not to dismantle a network but rather to prevent it from occurring in the first place’ (McGloin and Nguyen 2014, 20). Network analytic techniques may thus support the comparison of structures of multiple criminal groups and the analysis of their differences and similarities. They allow the evaluation of the roles of several sources of information to the reconstruction of criminal networks and how these sources influence their perception (Corazza and Esseiva 2013). In policing, they are key technics used to structure the information gathered during an investigation and facilitate the analysis of a case. As an external aid, they support collaborative thinking and support joint decision-making processes (Rossy and Ribaux 2014). Finally, they may also support the evaluation of disruption strategies in regard to their impact on the structure of criminal groups.

Methodological Elements

To analyse crime from its network dimension, graph-based techniques are more often than not used to model the problem. They can be classified into two main methodological categories. First, link analysis relies on the drawing of a qualitative graph depicting relationships between several types of entities by using adequate visual properties of nodes and edges (or links). Second, social network analysis uses a simpler visual model of nodes and edges but extends the model with quantitative measures depicting the structure of the global network or the structural features of its nodes. In this section, we present the aims, key concepts and methodological aspects of each.

Link Analysis

Link analysis is based on the conception of graph-like charts that aim to describe crime problems with a network model of nodes representing entities of interest such as persons, objects, traces, events or location, and their relationships. Link charts are used in criminal investigations to facilitate the processing of large-scale investigation data. They are commonly used to memorize the collected data and keep an overview of the relevant information. As working memory, they support investigators to remember the elements of the case and facilitate communication within teams or with partners. Even if they are not completely independent of language, link charts are generally well understood in international inquiries. When well designed, they are intuitive and do not require the mastery of complex formalism. In addition, the overview offered by link charts is generally highly appreciated by managers within police and criminal intelligence organizations.

The conception of link charts implies the adherence to some general recommendations. Some are found repeatedly in criminal analysis textbooks (Fedpol 2010; Interpol 1997; UNODC 2002) and the scientific literature (Harper and Harris 1975; Morris 1986; Senator 2005). For instance, ‘minimizing edge crossings’ and ‘favouring orthogonally’ to improve the readability of the chart are repeatedly promoted. Global methodology and a review of these recommendations can be found in Rossy and Ribaux (2014) and Rossy (2016).

Traditionally, these graph-like techniques are used for the representation of criminal networks, smuggling of goods, chronologies of events, as well as the visualization of telephone records and financial data. In this context, visualizations are used for many objectives, such as analysing the traces and information gathered, evaluating a cold-case, helping along the categorization of a particular offence, facilitating the transmission and receipt of a case or supporting an argument at trial (Rossy and Ribaux 2014). The identification of recurrent forms of usage in regard to repetitive crime and investigative problems has led to the formalization of patterns of visualizations. They are formalized to describe a design framework defined by the problem. Traditional link chart patterns are (1) the criminal network chart; (2) the chart of a trafficking action-set; (3) the event chart; and (4) the chart of a series. The first two support investigations involving the reconstruction of criminal groups. The latter two are intended to support the reconstruction process of complex criminal events whether a single case or a sequence of cases. A complete description of these patterns can be found in Rossy (2016).

The identification of patterns in link charts aims at formalizing adequate visual representations to support decision-making. Without cumulative experience, effort and time may be required to design an effective chart (Innes et al. 2005). Indeed, the design of a link chart is based on the understanding of the problem addressed by the analyst and his/her ability to model it in the form of a network representation (Peterson et al. 2000). The quality of the representation is then dependent on the analyst's ability to identify and classify entities and relationships relevant to the investigation and to distinguish them from those that may be omitted. The design involves both an ability to produce an expressive visual structure and an ability to properly model the situations encountered. Some authors note that a link chart does not solve the problem of information overload (Klerks 2001; Schroeder et al. 2007). Indeed, link charts seem to work well when the number of entities and relationships represented is limited. Moreover, if visualizations provide many benefits, they are not neutral and may induce biases. Designer choices, whether intentional or not, and user induced effects (e.g., confusion, distraction or misinterpretation) are two frequent causes of bias (Bresciani and Eppler 2009). For instance, the designer may oversimplify the problem and leave aside crucial elements that may lead to ambiguities and interpretation mistakes (Rossy and Ribaux 2012). This kind of bias may feed rhetoric in court.

However, these methods continue to be exploited and seem to respond to concrete needs. They allow for a common support to managing a large amount of heterogeneous data and they facilitate both the analysis and communication of information. The visual language is sufficiently rich and expressive to integrate the diversity of concepts encountered during the analysis of a criminal activity.

Social Network Analysis

Social network analysis is based on a simpler network model usually consisting of one set of social entities. Usually nodes depict individuals, but they may also represent groups of individuals or moral persons such as companies. Relationships among such actors are then depicted by edges between the nodes. This form of social network is known as a one-mode network. Analyses may also be derived from two-mode network data (i.e., two types of nodes) by extracting relations that consist of co-membership or affiliation to a group or co-attendance to an event. The number of types represented by nodes on a social network is the main feature that distinguishes it from a link chart. More often than not, a one-mode approach is used (Borgatti 2012; Strang 2014). On a link chart, the number of types of entities represented is not limited in the model, but defined by the criminal activity and chosen in consistency with the investigative questions.

The key methodological aspect of social networks is the integration of quantitative measures to depict the structure of the global network or the structural importance of specific nodes. The first category of methods, known as first order metrics, aims to describe the network as a whole. Among others, classical measures are the size of the network, its density, averaged degree, average shortest path (geodesic), and degree or betweenness centralization. The size of a network is calculated in terms of the number of nodes or links. The density is a measure of network cohesion, which accounts for the proportion of ties to all possible ties. A network containing all possible links is called a clique. The average degree is the mean of the number of links per node, and the average geodesic describes how far apart any two given nodes are (i.e., the average number of intermediates between two nodes). Degree and betweenness centralization describe the amount of variation in degree and betweenness scores for each node of the network (see below). These four calculations are often used to compare the value of a specific node to the average value of all nodes in the whole network. They are based on

metrics that aim to describe the centrality of the nodes within a network. Such calculations are known as second order metrics or 'centrality measures'. Classical measures are degree, closeness, betweenness and eigenvector centralities. Additional indicators have been developed and classified into three types of measures: local, distance and feedback (Brandes and Erlebach 2005).[1]

Since centrality may come in many forms, the centrality metrics aim at distinguishing them. Degree (i.e., the number of direct links with other nodes) and closeness (i.e., the shortest distance between a particular node and all other nodes) centrality measures aim to detect whether one individual could be central because he or she has many contacts. Others may have few contacts, but remain central because they link unconnected entities. The betweenness measure (i.e., the number of times a node lies on the shortest path between two other nodes) and eigenvector measure (i.e., the degree to which an individual is connected to other highly connected individuals) aim to detect these intermediaries or related roles. The interpretation of the metrics is an unresolved problem. Sparrow (1991) argued that it is a sign of strength, whereas Peterson (1994) sees a high degree of centrality as a vulnerability (see Morselli 2010 for an assessment within crime contexts). But no matter how they are interpreted, centrality measures allow discrimination of nodes and the detection of particular nodes that may have specific or abnormal activity within the network. They allow a quantitative description that may support the examination of the evolution of the network and the comparison of multiple networks. More specifically, social networks support (1) the detection of central individuals or subgroups in a criminal network; (2) the identification of their interactions; (3) the description of the structure of the network; (4) the evaluation of the impact of removing an individual from the network; and, finally, (5) the analysis of a network's information flows (Morselli et al. 2013). Researchers, however, have to be cautious of the limitations of the approach. Indeed, the reconstruction of co-offending networks often fails to integrate the social environment of offenders and relies on abilities to detect crimes. The perception of the networks is highly influenced by the efforts taken to reconstruct them (Bouchard and Malm 2016). As described below, these challenges are common to both methods.

Common Challenges of Conception

The conception process of both link charts and social network graphs relies on key considerations. The first is known as the boundary specification problem (Laumann et al. 1992). Whatever the problem being addressed, it is necessary to realize that the information gathered and its network model may be incomplete and reflect only one part of the whole picture. Analysing a whole network requires one to consider all connected nodes. Such an analysis is based on the assumption that the knowledge gathered is sufficient to describe the network as a whole. This is often not the case, and the classical way to address this problem is to clearly specify its delimitation. One way is to analyse an egocentric network dataset that focuses on the nodes surrounding one node known as the ego. Alternatively, a set of preset nodes may be selected. For instance, this is the case when an investigator analyses the telephone record data of the suspects in an investigation. However, even if several nodes are used as ego, this conception process leads to a bias. Indeed, the ego will naturally be central. This process is typical during investigations (Sparrow 1991). Laumann et al. (1992) identify three approaches to addressing this boundary specification problem: (1) considering those entities that are members of a known group, such as the members of an organization; (2) defining the population by limiting the entities to those involved in an event or a series of events; (3) selecting the entities based on a particular type of relationship. The conception process must thus be documented and the incompleteness in data should be well documented. Relevant entities and relationships must be selectively chosen leaving out the rest. The definition and the selection of the relevant entities rely on a clear definition of the aims of the analysis and the decisions it has to support.

The second consideration to address is how to handle uncertainties. They must be clearly identified and expressed in the model. Uncertainty can take several forms in a network. In particular, it may be unclear whether two entities are distinct. One physical person may, for instance, have multiple aliases not identified as related to the same entity. A link between two entities may also be uncertain. On a link chart it is common to distinguish unconfirmed links by dashed-lines. Uncertainties may also be handled with probabilities attached to the links and integrated in centrality measures as well as with simulation-based methods (Adar and Re 2007; Svenson 2008). Moreover, a distinction must be made between facts and hypotheses.

This distinction is at the core of the investigation and the research processes, which aim at identifying the causes (i.e., the hypotheses) of the observed effects (i.e., the facts).

Finally, a key element of the conception is to clearly define the nature of the entities and the relationships involved (Rossy and Ribaux 2014). Indeed, a network model aims at analysing the relationships among entities, while also understanding their nature and roles, in order to reconstruct the network. Consequently, the nature and characteristics of the relationships must be described as well as their frequency and uncertainty. Relations may be observed or measured, binary or valued. They may also be directed or undirected. The type of relation may be directly defined by its nature, such as co-membership to a group that is undirected or a sale of goods that is directed. However, the definition of the relationships may also imply making a decision in regard to the available data (Marin and Wellman 2011). For instance, Borgatti et al. (2009) identify four main categories of relations: similarities (e.g., a shared attribute), social relations (e.g., affective ties, friendships), interactions (e.g., participation in an event) and flows (e.g., an exchange or transfer between nodes). Since network analytical techniques aim at analysing the relationships between the entities, the data source underlying their detection and the formalism used to describe them should be well documented.

The Role of Forensic Science: Traces in the Reconstruction of Networks

In this section we discuss the roles of traces in reconstructing criminal activities within a network model of crime where they can take the form of relationships or entities. On the one hand, and as Locard's principle of exchange states, traces can be used to infer links between entities of interest such as individuals, locations and events. On the other hand, they may be used to infer the presence of a particular entity, such as a person or an object, based on Kirk's principle of individualization; the presence of a set of entities; or to provide information about the nature of the entity of interest through its identification (i.e., the definition of its class).

Locard's principle of exchange defines the trace as the result of a transfer during a particular abnormal activity (i.e., a crime, a deviant or illicit activity). In regard to the entity-relationship model, a trace can be considered as an entity. It has its own distinctive existence, for example, a bloodstain or a shoemark. The trace as an entity is an observable and collectable pattern,

signal or material that has its own existence and results from an activity of interest in a particular environment.

Of particular interest to the reconstruction of a criminal network is the fact that a trace is also the sign of the presence of one or more related entities in the network. Even if the identity of the source of the trace is unknown, the trace's presence is the sign of the activity of one or more individuals. For instance, DNA profiles extracted from biological traces may be used to infer the presence of an offender. A network of offenders can thus combine both known and unknown persons based on the traces they left during crimes. As Kirk's principle states, forensic science relies on the process of individualization that aims to infer the unique source (i.e., a person, an object or a material) of a detected trace (Kirk 1963; Margot 2011). The process relies on the detection of characteristics within the trace, which lead to the discrimination of a particular entity among all the other possible sources. For instance, event A is committed by offender A and crime B by offender B. Both are linked by the same DNA profile, which does not belong to A or B. In such a case, a network of three offenders can be inferred: A is linked to an unknown offender, which is linked to B. Whether or not the source of the trace is known, its existence may be the sign of the presence of a related, distinctly identified source entity. This unknown entity may be defined as a 'virtual entity' or more specifically as a 'virtual person' in the case of a DNA profile. A virtual entity is an abstract entity (i.e., a node in a network model) with a unique identity that may be related to one or more physical or digital entities (Jaquet-Chiffelle et al. 2009, 2008). For instance, the DNA profile of a trace is the identity of a virtual person that may be a unique individual or twins. A broad variety of traces can be used to infer the presence of virtual entities or, more specifically, virtual persons, in networks even if their roles are not identified. For instance, if two drug seizures are linked by forensic profiling, one may infer a common activity of an individual (or a group of individuals) that can be modelled and integrated in the network as an unidentified virtual entity (Corazza and Esseiva 2013). Such hypotheses can then be evaluated in regard to other sources of information collected during the investigation. In a network model of a criminal activity, one trace can thus be used to infer the presence of one or more virtual entities, which may be related to a specific physical entity or to several.

Traces can also be used to infer some specific characteristics of an unknown entity or offender. A trace can indeed be used to define the class of an entity. For instance, the gender of an offender can be detected from a biological trace, or an unknown powder may become an identified illicit drug. This is the process known as the identification of an entity. A trace can thus be used in a network as a partial identifier (i.e., an identity-related information) (Jaquet-Chiffelle et al. 2008). In this case, the trace is not the sign of the presence of a specific, fully identified entity but of a 'frame' of entities. The concept of frame defined by Kind (1987, 1994) referred to the set of persons of interest or entities of interest during an investigation. More broadly defined, it is the set of entities that matches the identity-related information.

A trace can also be interpreted as a tie between involved entities, commonly the source entity that produces it and the substrate entity where it was left during the event. Traces can link involved entities in both directions, as the principle of exchange states. For instance, a stain mark resulting from an assault can link a particular individual to the victim. But a trace as a tie may also link multiple entities, such as an email involving more than two email addresses that may be linked to several individuals. A stain mark containing a mixture of several DNA profiles can be associated with two or more individuals. In a network model of criminal activity, one trace can thus be used to infer one or more relationships among entities. The trace as a relationship is an observable and collectable tie, resulting from an activity of interest in a particular environment, between two or more entities.

A trace can thus link many types of entities, but the reconstruction of criminal networks aims at the identification of links between individuals. In these regards, traces may be used as direct links when the source of the trace is a person, or as indirect links when the source is an object. The relationship may also involve several types of entities such as a link between an individual and an event or a link to a location. Such links are of particular interest in reconstructing a two-mode network or a link chart of the criminal activity. Traces as a relationship can thus be classified according to the types of entities involved:

1) A relationship between individuals: a stain mark of an offender found on a victim or a mixture of DNA profiles found at the crime scene linking multiple offenders.
2) A relationship through objects: the trace is a sign of a transaction such as a telephone call, an email or bank transfer that is commonly used by criminal intelligence analysts

to reconstruct networks of offenders. The trace is the result of an activity involving several types of entities such as mobile phones, bank accounts or computers. To infer a link between offenders, their relationships to the objects used should be evaluated.

3) A relationship to an event: the trace is a sign of an activity such as gunshot residues resulting from the use of a firearm or glass fragments resulting from a glass breakage. Situating traces in time is a key aspect to inferring a link between a relevant entity and a particular event. Such links may be reconstructed by the use of direct markers of time (such as a digital record), ageing techniques or reconstructing chronologies (Weyermann and Ribaux 2012).
4) A relationship to a location: the trace is a sign of the presence of the offender such as stain marks, fingerprints or shoemarks detected at a specific location. Traces linked to the location such as soil, fibre or glass microtraces may also be recovered on a suspect. Records of digital traces are also used to link an individual to a location with geocoded databases (e.g., the geocoded cell of a mobile phone call, the record of a GPS signal or a geocoded IP address).

A single trace can thus be considered as a sign of a relationship between two or more entities of interest in a network model. But the comparison of two or more traces detected on several events can also serve the detection of multiple forms of relationships among events. This forensic link is defined as ‘a relationship established between forensic science entities sharing similar features that stems from the hypothesis of a common cause’ (Baechler et al. 2015, 186). The common cause is the most plausible explanation of the observed similarity (Cleland 2013). It is often a unique source entity such as an individual or an object or a similarity of actions such as a modus operandi reconstructed by the observation of traces (Baechler et al. 2015). Forensic links can be classified according to the nature of the inference involved. Several hypotheses about the common cause may indeed be inferred (for more details, see Ribaux et al. 2006). If two biological traces share the same DNA profile, one may infer a unique person as the source of both traces. In this case, traces may link a distinctly identified entity such as a person or an object. The link may also be less specific. For instance, if two shoemarks shared the same pattern, one may infer the presence of a frame of entities (i.e., the same type of objects). The detection of forensic links is at the core of the forensic intelligence process, which covers a broad range of exploitation of forensic science in policing (see Ribaux and Caneppele ‘Forensic Intelligence’, in this volume). The use of forensic case data

to reconstruct criminal networks is one form of exploitation of the informative value of traces in the field of knowledge known as forensic intelligence (Ribaux 2014; Ribaux and Talbot Wright 2014). In a network model, forensic links may link two or more events.

Traces can thus be integrated in a network model of criminal activities as relationships between entities of interest or to infer the presence of one or more entities from the profile of the trace itself. They may also serve the identification of the type of an entity. When multiple traces are considered, a forensic link between two or more events may be inferred. It takes the form of a virtual entity describing a common source. The profile of the trace defines the identity of the virtual entity, which may be linked to one physical or digital entity of the real world or a frame of entities (see Table 17.1 for a summary).

Table 16.1 The roles of forensic case data in a network model of criminal activities

Network model		Physical/digital world	Examples
A trace to infer the presence of one or more virtual entities	A virtual entity*	- An object or a person - A set of objects/persons sharing the same virtual identity	*A fingerprint of a person* *A DNA profile of twins, an email or an IP address*
	Multiple virtual entities	- A set of distinctly identified objects or persons	*A DNA mixture*
	An identity-related information of a virtual entity	- A frame of objects or persons	*A partial DNA profile, a shoe-mark's pattern*
		- A modus operandi of an event	*A drug synthesis method, a website conception*
A trace to infer relationships among virtual entities	A relationship** between individuals	- A direct link between two or more persons	*A stain mark of an offender found on a victim, a DNA mixture*
	An indirect relationship through objects	- An indirect link between two or more persons through the use of objects	*A telephone call, an email, a bank transfer*
	A relationship to an event	- A link between an object/person and an event	*A gunshot residue, some glass fragments, a time stamp of a file*
	A relationship to a location	- A link between an object/person and a location	*A soil trace, a GSP record*
Two or more traces to infer the presence of one or more virtual entities	A same virtual entity	- An object or a person as a source entity	*A same DNA profile, a same shoe or tire mark*
	A same identity-related information of a virtual entity	- A frame of objects or persons	*The model of an object*
		- A modus operandi of an event	*A drug synthesis method, a website conception*

** In a network model, a virtual entity refers to a node*

*** In a network model, a relationship refers to an edge between two nodes or multiple edges between more than two nodes.*

Conclusion

To conclude, decades of research have demonstrated the potential of the network perspective to analyse crime phenomena, and thousands of intelligence analysts are using link analysis and SNA methods, all around the globe, to manage the flow of information they must handle in real cases and to infer the activities of offenders. The entity-relationship model seems to complete and complement the geospatial and temporal dimensions of analysis of crime and supports both qualitative and quantitative research. Nevertheless, analysts and researchers should be cautious about the pitfalls and limitations of these approaches. These limitations are promoted by 'what you see is what you get' technologies, which hide challenges and methodological rules.

The growth of (digital) data collated during an analysis raises the temptation to jump to the use of the technical/technological, whereas the first step of any analysis is the careful evaluation of the objectives and the evaluation of the quality of the information at hand. This is one of the root principles of any scientific inquiry and this is where the trace may play a critical role. We have shown in this chapter how traces—whether they are physical or digital—as the most direct remnant of any criminal activity can be used to reconstruct criminal networks. Both link analysis and social network analysis approaches constitute a promising venture for forensic scientists and criminologists to collaborate around a shared model that supports the analysis and the integration of multiple sources of information to detect patterns in crime data.

References

Adar, E., and C. Re. 2007. 'Managing Uncertainty in Social Networks'. *IEEE Data Engineering Bulletin* 30(2): 15–22.

Akers, R.L. 1998. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press.

Baechler, S., M. Morelato, O. Ribaux, A. Beavis, M. Tahtouh, K.P. Kirkbride, P. Esseiva, P. Margot and C. Roux. 2015. 'Forensic Intelligence Framework. Part II: Study of the Main Generic Building Blocks and Challenges through the Examples of Illicit Drugs and False Identity Documents Monitoring'. *Forensic Science International* 250(May): 44–52.

Boivin, R. 2014. 'Macrosocial Network Analysis: The Case of Transnational Drug Trafficking'. In J.A. Masys, ed., *Networks and Network Analysis for Defence and Security*, 49–61. New York: Springer.

Bonacich, P. 1987. 'Power and Centrality: A Family of Measures'. *American Journal of Sociology* 92(5): 1170–1182.

Borgatti, S.P. 2005. 'Centrality and Network Flow'. *Social Networks* 27(1): 55–71.

Borgatti, S.P. 2012. 'Two-Mode Concepts in Social Network Analysis'. In A.R. Meyers, ed., *Computational Complexity: Theory, Techniques, and Applications*, 2912–2924. New York: Springer.

Borgatti, S.P., A. Mehra, D.J. Brass and G. Labianca. 2009. 'Network Analysis in the Social Sciences'. *Science* 323(5916): 892–895.

Bouchard, M., and A. Malm. 2016. *Social Network Analysis and Its Contribution to Research on Crime and Criminal Justice*. Oxford Handbooks Online. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199935383.001.0001/oxfordhb-9780199935383-e-21.

Brandes, U., and T. Erlebach, T. 2005. *Network Analysis*. Berlin: Springer Heidelberg.

Bresciani, S., and E. Eppler. 2009. 'The Risks of Visualization: A Classification of Disadvantages Associated with Graphic Representations of Information'. In P.J. Schulz, U. Hartung and S. Keller, eds, *Identität Und Vielfalt Der Kommunikations-Wissenschaft*. Konstanz, Germany: UVK Verlagsgesellschaft mbH.

Bright, D.A., C. Greenhill, M. Reynolds, A. Ritter and C. Morselli. 2014. 'The Use of Actor-Level Attributes and Centrality Measures to Identify Key Actors: A Case Study of an Australian Drug Trafficking Network'. *Journal of Contemporary Criminal Justice* 31(3): 262–278.

Bruinsma, G., and W. Bernasco. 2004. 'Criminal Groups and Transnational Illegal Markets'. *Crime, Law and Social Change* 41(1): 79–94.

Carrington, P.J. 2011. 'Crime and Social Network Analysis'. In J. Scott and P.J. Carrington, eds, *The SAGE Handbook of Social Network Analysis*, 236–255. Thousand Oaks, CA: SAGE Publications Ltd.

Chen, P.P.-S. 1976. 'The Entity–Relationship Model: Toward a Unified View of Data'. *ACM Transactions on Database Systems* 1(1): 9–36.

Cleland, C.E. 2013. 'Common Cause Explanation and the Search for a Smoking Gun'. *Geological Society of America Special Papers* 502: 1–9.

Corazza, D., and P. Esseiva. 2013. 'L'apport de la trace matérielle dans l'enquête criminelle: évaluation de la contribution des liens chimiques issus du profilage de produits stupéfiants par l'analyse des réseaux sociaux'. *Revue internationale de criminologie et de police technique et scientifique* 66(3): 341–363.

Desroches, F.J. 2005. *The Crime That Pays: Drug Trafficking and Organized Crime in Canada*. Toronto: Canadian Scholars' Press.

Duijn, P.A., V. Kashirin and P.M. Sloot. 2014. 'The Relative Ineffectiveness of Criminal Network Disruption'. *Scientific Reports* 4: 1–15.

Fedpol. 2010. *Manuel d'analyse criminelle opérationnelle*. Suisse: office fédéral de la police.

Freeman, L.C. 1977. 'A Set of Measures of Centrality Based on Betweenness'. *Sociometry* 40(1): 35–41.

Freeman, L.C. 1979. 'Centrality in Social Networks: Conceptual Clarification'. *Social Networks* 1(3): 215–239.

Freeman, L.C. 2004. *The Development of Social Network Analysis: A Study in the Sociology of Science*. North Charleston, SC: Booksurge Publishing.

Harper, W.R., and D.H. Harris. 1975. ‘The Application of Link Analysis to Police Intelligence’. *Human Factors* 17(2): 157–164.

Hashimi, S., M, Bouchard, C. Morselli and M. Ouellet. 2016. ‘A Method to Detect Criminal Organizations from Police Data’. *Methodological Innovations* 9: 1–14.

Innes, M., N. Fielding and N. Cope. 2005. ‘The Appliance of Science? The Theory and Practice of Crime Intelligence Analysis’. *British Journal of Criminology* 45(1): 39–57.

Interpol. 1997. *Guide sur l’analyse criminelle*. 2nd ed. Lyon : Interpol.

Jaquet-Chiffelle, D.-O., B. Anrig, E. Benoist, R. Haenni, M. Hildebrandt, E. Kosta and K. Lefever. 2008. *FIDIS Deliverable D2.13: Virtual Persons and Identities*. http://www.fidis.net/deliverables.

Jaquet-Chiffelle, D.-O., E. Benoist, R. Haenni, F. Wenger and H. Zwingelberg. 2009. ‘Virtual Persons and Identities’. In K. Rannenberg, D. Royer and A. Deuker, eds, *The Future of Identity in the Information Society: Challenges and Opportunities*, 75–122. Springer-Verlag Berlin Heidelberg.

Jennings, H.H. 1943. *Leadership and Isolation: A Study of Personality in Inter-Personal Relations*. New York: Longmans, Green, and Company.

Kind, S.S. 1987. *The Scientific Investigation of Crime*. Harrogate: Forensic Science Services Ltd.

Kind, S.S. 1994. ‘Crime Investigation and the Criminal Trial: A Three Chapter Paradigm of Evidence’. *Journal of the Forensic Science Society* 34(3): 155–164.

Kirk, P.L. 1963. ‘Criminalistics—a New and Independent Discipline Evolves from Modern Techniques and New Concepts of Individualization’. *Science* 140: 367–370.

Kleemans, E.R. 2007. ‘Organized Crime, Transit Crime, and Racketeering’. *Crime and Justice* 35(1): 163–215.

Klerks, P. 2001. ‘The Network Paradigm Applied to Criminal Organizations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands’. *Connections* 24(3): 53–65.

Laumann, E.O., P.V. Marsden and D. Prensky. 1992. 'The Boundary Specification Problem in Network Analysis'. In L.C. Freeman, D.R. White and A.K. Romney, eds, *Research Methods in Social Network Analysis*, 61–87. Piscataway, NJ: Transaction Publishers.

Malm, A.E., J.B. Kinney and N.R. Pollard. 2008. 'Social Network and Distance Correlates of Criminal Associates Involved in Illicit Drug Production'. *Security Journal* 21(1–2): 77–94.

Margot, P. 2011. 'Forensic Science on Trial—What Is the Law of the Land?' *Australian Journal of Forensic Sciences* 43(2–3): 89–103.

Marin, A., and B. Wellman. 2011. 'Social Network Analysis: An Introduction'. In J. Scott and P.J. Carrington, eds, *The SAGE Handbook of Social Network Analysis*, 11–25. Thousand Oks, CA: SAGE Publications Ltd.

McGloin, J.M., and D.S. Kirk. 2010. 'Social Network Analysis'. In A.R. Piquero and R. Weisburd, eds, *Handbook of Quantitative Criminology*, 209–224. New York: Springer.

McGloin, J.M., and H. Nguyen. 2014. 'The Importance of Studying Co-offending Networks for Criminological Theory and Policy'. In C. Morselli, ed., *Crime and Networks*, 13–27. New York: Routledge.

McPherson, M., L. Smith-Lovin and J.M. Cook. 2001. 'Birds of a Feather: Homophily in Social Networks'. *Annual Review of Sociology* 27: 415–444.

Moreno, J.L. 1932. *Application of the Group Method to Classification*. New York: National Committee on Prisons and Prison Labor.

Moreno, J.L. 1934. *Who Shall Survive? A New Approach to the Problems of Human Interrelations*. Washington, DC: Nervous and Mental Disease Publishing Company.

Morris, J. 1986. *Crime Analysis Charting*. Loomis: Palmer Press.

Morselli, C. 2009. *Inside Criminal Networks*. New York: Springer.

Morselli, C. 2010. 'Assessing Vulnerable and Strategic Positions in a Criminal Network'. *Journal of Contemporary Criminal Justice* 26(4): 382–392.

Morselli, C., V.H. Masias, F. Crespo and S. Laengle. 2013. 'Predicting Sentencing Outcomes with Centrality Measures'. *Security Informatics* 2(1): 1–9.

Morselli, C., and J. Roy. 2008. 'Brokerage Qualifications in Ringing Operations'. *Criminology* 46(1): 71–98.

Natarajan, M. 2006. ‘Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data’. *Journal of Quantitative Criminology* 22(2): 171–192.

Papachristos, A.V. 2011. ‘The Coming of a Networked Criminology?’ *Advances in Criminological Theory* 17: 101–140.

Papachristos, A.V. 2014. ‘The Network Structure of Crime’. *Sociology Compass* 8(4): 347–357.

Pearson, G., and D. Hobbs. 2001. *Middle Market Drug Distribution*. London: Home Office.

Peterson, M.B. 1994. *Applications in Criminal Analysis: A Sourcebook*. Westport: Praeger.

Peterson, M.B., B. Morehouse and E. Wright. 2000. *Intelligence 2000: Revising the Basic Elements*. Lawrenceville: Law Enforcement Intelligence Unit and International Association of Law Enforcement Intelligence Analysts.

Reuter, P. 1983. *Disorganized Crime: The Economics of the Visible Hand*. Cambridge, MA: MIT Press.

Ribaux, O. 2014. *Police scientifique. Le renseignement par la trace*. Lausanne: Presses polytechniques et universitaires romandes.

Ribaux, O., and B. Talbot Wright. 2014. ‘Expanding Forensic Science through Forensic Intelligence’. *Science & Justice* 54(6): 494–501.

Ribaux, O., S.J.J. Walsh and P. Margot. 2006. ‘The Contribution of Forensic Science to Crime Analysis and Investigation: Forensic Intelligence’. *Forensic Science International* 156(2–3): 171–181.

Rossy, Q. 2016. ‘La visualisation relationnelle au service de l’enquête’. In R. Boivin and C. Morselli, eds, *Les réseaux criminels*, 17–39. Montréal: Les Presses de l’Université de Montréal.

Rossy, Q., and O. Ribaux. 2012. ‘La conception de schémas relationnels en analyse criminelle: au-delà de la maîtrise des outils’. *Revue internationale de criminologie et de police technique et scientifique* 65(3): 345–362.

Rossy, Q., and O. Ribaux. 2014. ‘A Collaborative Approach for Incorporating Forensic Case Data into Crime Investigation Using Criminal Intelligence Analysis and Visualisation’. *Science & Justice* 54(2): 146–53.

Schroeder, J., J. Xu, H. Chen and M. Chau. 2007. ‘Automated Criminal Link Analysis Based on Domain Knowledge’. *Journal of the American Society for Information Science and Technology* 58(6): 842–855.

Senator, T.E. 2005. ‘Link Mining Applications: Progress and Challenges'. *SIGKDD Explorations* 7(2): 76–83.

Sparrow, M.K. 1991. ‘The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects’. *Social Networks* 13(3): 251–274.

Strang, S.J. 2014. ‘Network Analysis in Criminal Intelligence’. In J.A. Masys, ed., *Networks and Network Analysis for Defence and Security*, 1–26. New York: Springer.

Sutherland, E.H. 1939. *Principles of Criminology*. 3d ed. Philadelphia: Lippincott.

Svenson, P. 2008. ‘Social Network Analysis of Uncertain Networks’. *Proceedings of the 2nd Skövde Workshop on Information Fusion Topics*, 1–3. University of Skövde, Sweden.

UNODC. 2002. *Criminal Intelligence Training: Manual for Analysts*. Vienna: United Nations Office on Drugs and Crime.

van Mastrigt, S.B., and P. Carrington. 2014. ‘Sex and Age Homophily in Co-offending Networks’. In C. Morselli, ed., *Crime and Networks*, 28–51. New York: Routledge.

Wasserman, S., and K. Faust. 1994. *Social Network Analysis*. Cambridge: Cambridge University Press.

Weyermann, C., and O. Ribaux. 2012. ‘Situating Forensic Traces in Time’. *Science and Justice* 52(2): 68–75.

Wigmore, J.H. 1913. *The Principles of Judicial Proof as given by Logic, Psychology, and General Experience, and Illustrated in Judicial Trials*. Boston: Little, Brown, and Company.

Zaitch, D. 2002. *Trafficking Cocaine: Colombian Drug Entrepreneurs in the Netherlands*. The Hague: Springer.

Zhang, S. 2008. *Chinese Human Smuggling Organizations: Families, Social Networks, and Cultural Imperatives*. Stanford: Stanford University Press.

Zhang, S., and K.L. Chin. 2002. 'Enter the Dragon: Inside Chinese Human Smuggling Operations'. *Criminology* 40(4): 737–768.

[1] For more details about the centrality measures, see Bonacich 1987; Borgatti 2005; Brandes and Erlebach 2005; Freeman 1979; Wasserman and Faust 1994.