Trends Organ Crim (2009) 12:101–121
DOI 10.1007/s12117-008-9057-6

ORIGINAL ARTICLE

Introduction to Social Network Analysis (SNA) as an investigative tool

Renée C. van der Hulst

Published online: 13 December 2008

Abstract Social behavior is brought about mainly through social ties and connections. Our contacts with other people shape our view of the world, reinforce our identity, and the interactions provide us with all kinds of opportunities and resources to get things done. The social capital associated with networks is also one of the primary ways facilitating crime. Therefore, the systematic analysis of criminal networks is considered a viable means to gain a more thorough understanding of criminal behavior. This paper is a general introduction to social network analysis (SNA) as an analytical tool for the study of adversary networks. The paper reviews some theoretical and key concepts, highlights functional applications, and presents a tentative protocol for data handling and coding. The discussion deals with some methodological issues, challenges and future developments in the field.

Keywords Social Network Analysis (SNA) · Organized crime · Terrorism · Social capital · Methods · Criminal investigation

Organized crime is a relational phenomenon that involves multiple actors. For quite some time, organized crime groups were considered to be durable groups of at least three offenders, involved in several types of offences with the primary motive to gain financial profits. Contrary to earlier assumptions, organized crime in the Netherlands turns out to be less hierarchically and much more loosely structured and it is characterized by a logistic web in which many smaller networks are active (Kleemans et al. 2002; Klerks 2001). The same typology of cellular structures applies to 'home-grown' terrorist networks (Sageman 2004). Steered by political, philosophical, ideological, racial, ethnic or religious motivations, the primary motivation of terrorism is not economic profits but the destabilization of political,

Part of this paper was presented at the 2008 Blankensee Colloquium on Human Capital and Social Capital in Criminal Networks, Berlin, Germany.

R. C. van der Hulst (✉)
Research and Documentation Centre (WODC), Ministry of Justice,
P.O. Box 20301, 2500 EH The Hague, the Netherlands
e-mail: Vanderhulst@online.nl

constitutional, economic or social structures. Despite the motivational and group dynamic differences between organized crime and terrorist groups, they share the same loosely connected and fluid ad hoc organizational principles. Hence, social ties and connections are to a large extent crucial determinants for the performance, sustainability and success of both criminal and terrorist organizations. Systematically accumulating knowledge about the structural 'blue print' of criminal activity increases our understanding of their functioning and flaws, and may lead to effective ways to counteract and disrupt those networks. In the following sections we discuss social network analysis (SNA) as a promising tool for scrutinizing the fundamental principles and structures of concerted criminal action with specific emphasis on directions to classify and handle research data.

The study of adversary networks

In a way, criminal organizations are not much different from legal ventures that constantly look for new opportunities, structures and strategies to maximize profits. They recruit the right employees, cooperate or build coalitions with business partners, walk all kinds of legal (or illegal) paths, and frequently bridge social structures if this serves their best interest. Fijnaut et al. (1998: 123) emphasized that the Netherlands is the crossing-point of various number of criminal groups that operate worldwide. Major activities involve the trade in drugs, frontier-running and human trafficking that require careful planning and organized action. As Fig. 1 illustrates, the identification of such criminal connections (e.g., between actors, resources, activities, events and locations) is a well-established method in the field of law enforcement and intelligence. The basic questions emphasize: who are the *actors* involved, what criminal *activity* are they involved in, and are the activities *structured* in such a way that they can be referred to as a criminal or terrorist organization?

The link analysis method

A variety of tools is regularly used in both the tactical and strategic analysis process of intelligence (for a complete overview, see McDowell 1998: 177–178). Examples are case comparison analysis, profiling (of the offence, the victim or the offender),

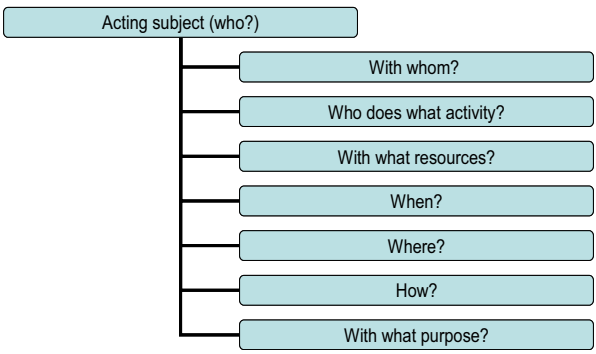

Fig. 1 The path of reasoning in criminal analysis

spatial analysis (GIS), crime pattern analysis, analytical charting techniques (e.g., of activities, events, commodities, frequencies), event flow charting (i.e., relevant events of a crime presented on a time line), template matching, and telephone toll analysis (Sparrow 1991a; Sparrow 1991b). The standard procedure for investigating collaborations of criminal activity that focus on the profiling of relations between criminal actors is better known as link analysis (Harper and Harris 1975). The link analysis method reviews criminal actors, events and activities and visualizes the links between entities in a graph. By organizing a bulk of information in a manageable way this enables the discovery and identification of patterns of activity, criminal roles, and key players. However, at least two important findings need to be acknowledged. First of all, criminal investigators mainly use the visual mapping tools without bothering much about the mathematical considerations and social mechanisms underlying such networks (Klerks 2001). Second, the link analysis method neglects the fact that perceptions of relational patterns are heavily affected by the layout of graphs. Research has demonstrated, for example, that people tend to believe that actors in the center or at the top of a graph are crucially and most important, and that actors who are in close proximity to each other belong to the same group (McGrath et al. 1997; McGrath et al. 2003). This does not necessarily have to be the case. Since the human eye is easily mislead by the arbitrary layout of visual graphs, drawing conclusions based on such graphs may be very fragile and an impertinent thing to do.

Social network analysis

According to Clark (2007: p. 3), the failure to analyze networks in a more objective manner is one of the major reasons why law enforcement and intelligence can fail. There is a continuous need for innovative and advanced research tools that improve the quality of research. One of those tools that help to systematically uncover clandestine and adversary networks is Social Network Analysis (SNA). SNA is considered as the scientific equivalent of link analysis. It is not so much a theory but rather a theoretical and methodological paradigm for sophisticated examining of complex social structures (Emirbayer and Goodwin 1994). The technique allows for much wider applications than simply graphs. That is, in addition to visualizations of network graphs, SNA is an arithmetical technique that analyzes relational patterns of nodes (actors) and connections (ties) based on mathematical computations[1]. These computations result in structural network measurements (or parameters) that quantify characteristics of network activity, social roles, positions and associated social mechanisms like power and dependency (Wasserman and Faust 1994). One of the main purposes of SNA is to detect and interpret patterns of social ties among actors and to identify the impact (benefits or constraints) of the social structure on the functioning of actors and networks. Because of the ability to compute quantified network parameters in addition to graphs, interpretations of network characteristics are less sensitive to subjectivity and limit the risk to miss out important signals.

[1] In mathematics and computer and information sciences the analysis of nodes and connections is known as graph theory (Harary 1969).

Over the last decades SNA has been used a lot as a policy tool in organization and business management (e.g., to promote the communication, cooperation, team performance or innovation) and in health sciences (e.g., to map the spread of particular diseases like aids). Since 9–11 (the terrorist attacks in the United States in 2001) there has been a considerable increase in interest from law enforcement, criminal investigators, military and intelligence communities to use SNA as a research tool to systematically describe, model and analyze adversary networks (Carley et al. 2001; Clark 2007; Coles 2001; Krebs 2002; McNally and Alston 2006; Morselli and Giguère 2006; Morselli and Petit 2007; Natarajan 2006; Rothenberg 2002). The technique is of particular interest because of the ability to identify structural patterns and associated roles and functions that are not easily discovered at first glance (Morselli and Roy 2008; Schwartz and Rouselle 2008). SNA allows identifying, for example, who is central in organizations, what key players or ties are vital to monitor, and what interventions would be most effective to cause a major disruption of the network (Koschade 2006). We summarize briefly some analytical purposes of SNA as a law enforcement and intelligence tool (cf. Koschade 2006; Sparrow 1991a, 1991b; Clark 2007).

✓ *Scenario building*

Scenario building is a reconstruction based on speculation about what might have happened in order to explain a current reality with a fixed outcome (e.g., a murder case). The aim of this creative thinking process is to look for directions and fruitful ways to continue an ongoing investigation that may lead to the offender(s).

✓ Risk analysis and threat assessments

Prospective scenario building refers to the monitoring, evaluation and prediction of potential threats associated with individuals or groups. By closely monitoring the behavioral strategies of the targets (e.g., their networks and activities), investigators gain a better understanding of the way crimes are structured, how the involved actors and networks are positioned to operate and to what extent they pose a threat to society. The use of sophisticated SNA parameters can help identify potential risks that otherwise may be overlooked.

✓ Hypothesis testing

A hypothesis is a plausible explanation often thought of as a ‘theory waiting to be tested’ or ‘an answer waiting to be confirmed’ based on information, understanding, and speculation (McDowell 1998: 123–124). The development and testing of hypotheses is absolutely critical in the intelligence process. SNA can help to identify the key players and central actors in criminal networks and evaluate or predict the possible consequences of removing specific actors from a network (e.g., to destabilize a network).

✓ Destabilize networks

Based on the information of (suspected) criminal networks and activities, particular targets can be identified that would cause maximal disruption of the ongoing or planned criminal activities. Hence, knowing what determines the strengths and vulnerabilities of a network and the particular roles and positions associated with actors provides criminal investigators with tactical options to demobilize (or reinforce) it.

✓ Identify aliases, identical role and substitutes

SNA can also prove useful to identify names of actors in a database that appear to be aliases based on the similarity in their patterning of social ties (e.g., role

equivalence) or to identify subsets of actors that employ identical roles (i.e., serve as substitutes). This would make sense, for example, to locate potential successors of key players who are dismissed or eliminated from a network (e.g., by imprisonment or death), or to compare roles and functions across networks in order to target important players when only sparse information is available (e.g., if actor X is the brain behind criminal ventures in network A then actor Y may be occupying an identical role in network B if the social ties and structures of both actors and both networks resemble each other).

✓ Support decisions on the deployment of intelligence assets

Because of the ability to identify important key players and ties in a network, SNA can support tactical decisions on the deployment of intelligence assets in the most optimal locations worth monitoring.

✓ Evidence for prosecution

The particular challenge of SNA, in particular with regard to network parameters, is whether it will be able to serve as evidence for prosecution. That is, when roles and responsibilities can be proven based on the ability to identify and give meaning to social structures, SNA can become a powerful tool in support of law enforcement by making criminal actors accountable for their role and involvement. Mainly due to the imperfection of available data in law enforcement and intelligence, the current state of the art of SNA has not reached this quality yet but scientists worldwide put in a great effort to handle missing data and other methodological issues such as dynamic network analysis.

Networks as opportunity structures

Criminal and terrorist organizations may be clandestine but other than that their management principles are quite common to any other goal-oriented network: it's all about integrating people, information and technology. If we consider organized crime, for example, as a complex and dynamic set of goal-oriented processes, we must assume that the criminal networks are designed to optimize their efficiency and effectiveness. The core or the 'blue print' of criminal operations includes a strategic design (i.e., the overall organizational structure including subunits and relationships) and an operational design (i.e., defining roles and processes that are operated by individuals and groups). Beyond that, one of the general challenges in human capital or human resources management (HRM) is to fit the right people with the necessary competencies, skills and expertise into the right jobs in order to optimize overall performance. Another cornerstone for organizational success is to create competitive advantages through social connections that facilitate the achievement of goals that would not be attainable in its absence (Coleman 1990). It should come as no surprise that criminal and terrorist networks depend to a large extent on social contacts, ties and the ability to generate the necessary resources for their operations. Metaphorically speaking, the advantages that result from social networks are known as social capital.

According to the *Theory of Social Capital* (Bourdieu 1986; Coleman 1990; Flap and Völker 2003; Lin 1992; Lin 2001; Portes 1998), people who have better access to valuable social resources are more successful in their performance. This does not only apply to individuals, but also to groups, organizations and communities. In

essence, social networks are opportunity structures to get things done and they can be considered as one of the main building blocks of (criminal) success. The way that relations are structured, including the embedded positions of actors create, facilitate and set boundaries to behavioral opportunities. Social capital results in strategic advantages basically from two factors:

(1) Connections to other people provide access to their assets (e.g., instrumental resources, emotional support, expertise, knowledge);
(2) The overall network structure (including the way that actor's positions are embedded within) provides strategic benefits in and of itself.

As Fig. 2 illustrates, a social network can be defined as a compilation of entities (e.g., people, groups, organizations) that are connected through social ties in which a variety of resources are exchanged. Entities are actors that are represented by nodes, and ties between actors are represented by lines. In order to study criminal networks using SNA-tools and routines, one needs to understand the key theoretical concepts and implications from social networks. We briefly discuss the major characteristics of social networks that serve as input for analysis.

Actors

As discussed earlier, people are critical assets for organizations as they can provide resources, for example, by way of their socio-economic position, their experience, specific knowledge or skills, connections to important others, because they are wealthy, or because they can exert (political) influence. In SNA, characteristics of actors are analyzed as actor's attributes. This include, for example, demographic characteristics (age, sex, place of birth, residence, ethnicity), attitudinal characteristics (motive, personality, identity, social norms), socio-economic status (income, job), and skills (competencies, training, experience, hobby, job). On an aggregated level these characteristics can also apply to groups or organizations.

Resources

According to *Social Exchange Theory* (Blau 1964; Cook and Whitmeyer 1992), people continuously exchange a variety of material and immaterial goods and

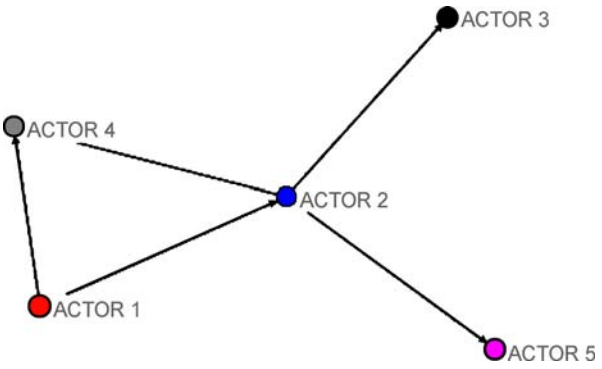

Fig. 2 A social network of actors and ties

services with each other that are instrumental to achieve goals. The resources can vary from money or information (instrumental resources) to social support (an expressive resource) (Van der Hulst 2004).

The interplay between ties and resources

Social ties are connections between actors that indicate some form of activity or bonding between actors. One of the structural parameters of dyadic ties that refers to the intensity or quality of relations between actors is tie strength (often measured by the frequency of contact times the intensity of a tie). Strong ties are close, solid and trusted reciprocated relationships (e.g., family and friends), whereas weak ties are characterized by less intimacy (e.g., co-worker). Both kinds of ties bring their own benefits and constraints in terms of access and instrumental value of resources. The major benefit of strong ties is that people are generally more willing to help and share the same norms and values which increases the ability to access instrumental resources. On the other hand, similar people tend to have identical qualities[2] and circulate in the same social circles which means that they share identical resources as well. Hence, the available pool of resources may be abundant but tend to be redundant in their instrumental value. The reverse holds for weak ties: the available pool of resources may be more limited because of the limited willingness of other people to help, but weak ties are more likely to connect people from different social circles, which creates access to a pool of more diverse resources that are instrumental to achieve goals. The latter is known as the *strength of weak ties* argument (Granovetter 1973). The fundamental dilemma for criminal offenders is to balance their need for strategic initiatives based on a broad access to instrumental resources (i.e., through weak ties), and their need for trusted and solid collaborations that facilitate secrecy, protection and the enforcement of norms and sanctions (see also Burt 2000, 2001; Kadushin 2002; Morselli et al. 2007; Sageman 2004: 165). The benefits and constraints of strong and weak ties are summarized in Fig. 3.

Network positions

Network positions are the structural positions of actors relative to other actors in a network. Not only the dyadic tie between two actors (e.g., between actor 1 and 2 in Fig. 2) but also the indirect ties between actors are taken into account (e.g., actors 3 and 5 that have an indirect tie to actor 1 in Figure 2). The positions indicate, for example, to what extent an actor is able to (de)mobilize sources, or to transfer or selectively share information and exert influence. Network positions often coincide with specific social roles, functions or tasks in a social network that may be very informative from an intelligence point of view. Centrality is an important network parameter of positions that is used in a lot of network research. Actors with many direct contacts (high scores on *degree centrality*) play an active role in the network

[2] People have the natural tendency to develop strong ties to others who have identical characteristics as ourselves (e.g., sex, age, training, ethnicity). In network terms, this tendency is referred to as *homophily* (Homans 1958; McPherson et al. 2001).

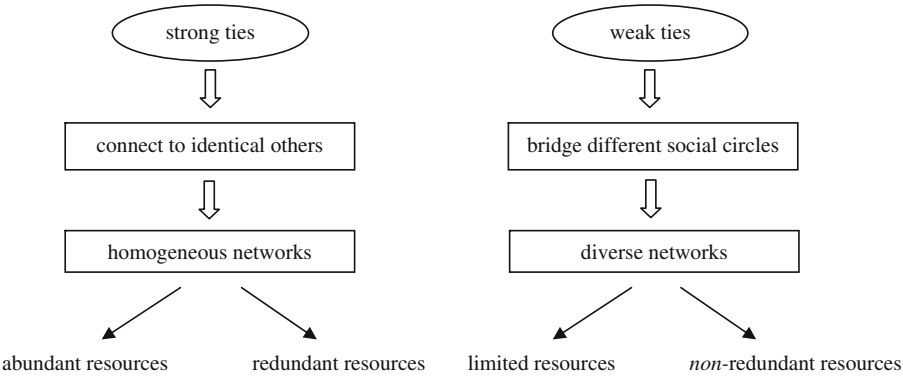

Fig. 3 Benefits and constraints associated with tie strength

and are assumed to have access to multiple behavioral alternatives which makes them less dependent on others and more powerful. Actors who are closer to more actors in the network than any other actor (high scores on *closeness centrality*) are important to quickly spread or transfer resources and coordinate tasks in the network. Actors who frequently operate as the 'quickest' bridge connection by means of shortest paths between other actors (high scores on *betweenness centrality*) are powerful key players for core business of the network and have the ability to isolate, influence, manipulate or prevent contact between other parties.

The strategic benefits associated with being in a unique bridging position between other actors is central to *Structural Holes Theory* (Burt 1992; 2000; 2001). If two non-redundant (groups of) actors are focused on their own (in-group) activities without paying much attention to the activities of the other, according to Burt there is a hole in the social structure (i.e., a structural hole). Actors who span structural holes, or social gaps, and who position themselves in between the groups create competitive benefits. Criminal brokers, for example, are able to identify more rewarding opportunities and power through: (a) information benefits (i.e., early access to non-redundant information and the ability to anticipate and adapt to opportunities or difficulties), and (b) control benefits between parties. As a result, between central actors are more creative, identify opportunities fast, know exactly where to find the right people, and create higher returns on their investments. Fig. 4 illustrates a structural hole between two countries (e.g., drug producers and sellers in country X on the left and drug buyers and distributors in country Y on the right) that is bridged by the circle node D[3]. Research indicated that brokers in transnational crime who bridge the connections between sources, transit and destination countries (e.g., actor D), are often ethnically homogeneous to the counterparts they work with (e.g., actors K and E). Their relations are mostly based on trusted friendship or family ties (Bruinsma and Bernasco 2004; Kleemans et al. 2002).

[3] Note that actors K (country X) and E (country Y) also score high on betweenness centrality but, contrary to actor D, they are high degree central as well.

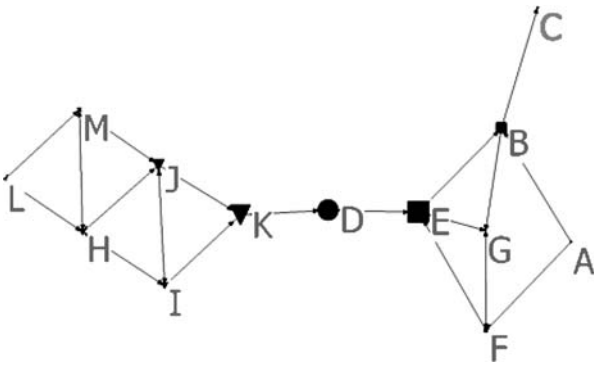

Fig. 4 A structural hole between groups bridged by a broker

Network structure

When referring to groups or social activity between two or more people, implicitly we refer to social structure. Ties between two actors are referred to as *dyads*. According to Simmel (1950), however, it is not particularly the dyad that influences our behavior, but the embeddedness of dyads in cliques (i.e., groups of close ties between three persons or more). So-called *Simmelian ties* are reciprocal ties between two actors while at the same time both actors have a reciprocal tie to the same third (or more) parties. The embeddedness encourages people to strive for social balance in their relationships which makes them more sensitive and willing to act more consistently with the group's norms (Heider 1958; Krackhardt 1998). Such ties are at the basis for developing trust, social norms, cohesion and cooperation and reduce individualism and power concentrations (Coleman 1990). Hence, the overall network structure can be of specific importance to a variety of group processes and social mechanisms like trust, reciprocity, influence, and leadership. This is one of the reasons why SNA is considered as a suitable tool to study criminal phenomena.

It is important however to keep a couple of things in mind. First of all, social structures can have positive outcomes in the sense that they facilitate the achievement of goals. We refer to this as social capital. But second, social structures can also have negative outcomes in the sense that they constrain the achievement of goals. We refer to this as social liability (Gabbay and Leenders 1999). The outcomes or effectiveness of social structures and the interpretation of associated network parameters are likely to be contingent to goals (e.g., secrecy, efficiency), to personal characteristics (e.g., gender), and activities (e.g., a central actor in a network of friends is likely to be a popular and key person, whereas a central actor in a network of enemies is not popular at all, and a central actor in a logistic chain of co-workers may not indicate importance but be a mere reflection of the division of labor).

Therefore, we argue that the analysis of social structures is particularly meaningful when additional information on the characteristics of actors, relationships (e.g., friendship, co-worker, enemies) and the type of resources or activities (e.g., information, money, materials) are taken into consideration. All together with a

firm knowledge of human behavior and group dynamics, this will offer investigators with improved directions in the law enforcement and intelligence process.

A neglected specialism and its issues

It has been argued that the neglect of SNA in criminology, law enforcement, intelligence and policy research has hampered the ability to counteract organized crime and terrorism (Bruinsma and Bernasco 2004; Coles 2001; Chattoe and Hamill 2005; McIllwain 1999). Part of this neglect can be explained by the lack of experienced investigators and the specific methodology that is used to analyze networks. The methods and analytical concepts used in SNA[4] are quite different from the methods generally used in traditional statistics and data analysis (Wasserman and Faust 1994). Moreover, clandestine networks bring along specific methodological and statistical problems to the application of SNA. The analysis routines become especially problematic when they are used for inferential statistics and hypotheses testing (i.e., significance tests).[5] Nevertheless, just like other qualitative research, the descriptive techniques can be applied without much problem and is considered to be of great value since it offers key insights in how actors are associated and organized. Still there are other conditions that may limit widespread applications of SNA in the study of adversary networks. In the absence of automated software that recognizes and codes social networks from a variety of unstructured data files, the preparation of data simply takes a lot of labor and coding is not as straightforward as it seems. We emphasize some important issues below before we present a tentative protocol and classification systems that can be used in the analysis of adversary networks.

✓ *Access to network data*

By definition, the collection of complete network data is difficult to attain. Moreover, the target population that is subject to enquiries for law enforcement and intelligence investigators will do about everything to shield this kind of information. It is probably fair to say that suspect targets cannot be asked to fill out a questionnaire to report on all their criminal or terrorist contacts and activities. They simply will refuse. Investigators have to rely on alternative methods of enquiry that result in incomplete data (e.g., phone taps, observations, e-mail, archives, informants, witnesses) that is not necessarily representative of the whole network or subject to a limited time span of enquiry (Natarajan 2000). Unless the investigator is associated to a law enforcement agency even the access to this data remains unfeasible to acquire. Hence, access to network data is considered a hell of a job and

[4] A well known software tool for SNA is UCINET (Borgatti et al 2002).

[5] Because the assumptions are not met to make statistical inferences. First of all, observations in social networks are *not* independent since actors are embedded in social groups and therefore associated. Second, observations are usually not based on sampling, but even if they are the observations are not random since most data is auto correlated. And third, the way that variables of interest are distributed in the population (to which the results need to be generalized) is not known beforehand and probably not random. A possible solution to overcome some of the problems is the use of permutation tests.

not being able to acquire complete network data must simply be taken for granted (see also Rothenberg 2002).

✓ Definition of network boundaries

In law enforcement and intelligence investigations one targets a certain audience. Particularly with regard to SNA applications one of the main questions is what actors to include or exclude from the analysis (Sparrow 1991a, b; Krebs 2002). The boundary specification problem strongly affects the scope and the structure of a social network (as well as the results) and must be based on prior decisions. Selection criteria can be natural boundaries (e.g., a family, an overt organization, or all residents of a particular area) but most of the time decisions will be based on theoretical or practical considerations (Scott 2000: 54).

✓ Assumptions prior to coding

The meaning to attach to particular events, symbols and behavior is not always evident and is heavily influenced, for example, by cultural values. Shaking hands may imply a close relationship in one context whereas it may indicate distance in others. This complicates the coding of data and attention has to be paid to increase inter-rater reliability. Prior to any investigation it needs to be consistent and clear how the information on social connections is to be coded (e.g., when are actors considered to be friends or foes, what are considered important events or key issues?). In particular in the area of law enforcement and intelligence, specific problems ask for prior consideration and solutions, e.g.:

- How to handle nick names / fake names?
- How to handle identical names that refer to different people?
- How to handle incomplete, outdated, or contradictory documents?
- How to handle different types of relations?
- How to handle the various levels of reliability in the information?

✓ Data reliability

In most law enforcement and intelligence research, data is evaluated in terms of reliability of the source and validity of information (McDowell 1998: 172–173). First of all, sources can vary in reliability from 1: reliable (a reliable, authentic, competent and trustworthy source), to 2: usually reliable, 3: unreliable, or 4: unknown (no history of information from the source). Second, information can vary in validity from being 1: truthful (confirmed by other sources and consistent with other information), 2: probable, 3: doubtful, or 4: unknown (no prior data available to compare consistency). This implies sixteen categories to express the quality of data and there is not yet a convenient method or routine available in SNA that takes into account the varying degrees of reliable and valid data.[6] In the intelligence and law enforcement arena, however, investigators simply cannot escape the fact that they are dealing with varying quality in their data (e.g., hear-say). Prior to coding, investigators have to make sure how to handle this problem, perhaps by giving weights to the ties being reported.

✓ Change over time

A social network analysis is based on a particular composition of actors and ties at a given point in time. However, the composition of networks as well as the activities that

[6] In Analyst's Notebook (the link analysis method), for example, ties are usually characterized as confirmed, unconfirmed, or tentative relations.

take place are ever changing. Actors come and go, social relations are build and destroyed, and social contexts as well as criminal opportunities change all the time. Changes in network activity (e.g., increases in particular flows of exchange, rapid emergence of new actors and ties, change of directions in money flows) may even be a key element indicating different phases of a planned event or operation (Krebs 2002; Sparrow 1991a, b). One of the main questions is how to model and deal with the dynamics of networks (e.g., what to do with the distinction between past and current relations?).

✓ Time intensive

Data gathering, coding, and analyzing is a very time intensive job. At the same time, the time-span to deliver results is usually very short which conflicts with the necessity to work accurately. The investigator needs to balance both requirements while not giving in too much on any of the accounts. The time management requirement is probably the most difficult and demanding element when the strategic intelligence process is considered (McDowell 1998: 49, 52).

✓ Handling large datasets

Computing resources for handling large datasets are generally limited whereas criminal or other intelligence databases are generally quite huge (Sparrow 1991a, b). The larger the network of investigation becomes, the more likely it is that computers miss the capacity to handle these data. To exemplify this: for a group of 10 actors the maximum number of ties between actors adds up to 45, but for a group of 200 actors the potential number of relations reaches 19.900!

✓ Data tidying

Along the process of data coding, the data set needs constant adjustment and data tidying. For example, individuals may be registered multiple times under different spellings of their names or nicknames, and the direction of ties in encoding phone tabs, for example, is sometimes mistakenly reversed (Klerks 2001). Although accuracy is a necessary requirement in all research, for the analysis of networks the creation of accurate and exact datasets is of utmost importance.

✓ Missing data

Missing ties have an immense impact on the social structure and analyses of social networks (e.g., incomplete information impairs the options to identify cliques, clusters and so on) (Coles 2001). Besides the fact that data on clandestine networks are most likely to be incomplete to begin with, investigators also have the tendency to underreport ties based on information that is available (Harper and Harris 1975). Incomplete data, particularly when missing data is not random, generate problems of statistical inference to begin with (Sparrow 1991a, b). But also for descriptive purposes, missing out on important links between actors complicates the ability to make inferences based on such data and will mislead the investigator into the wrong directions. Hence, the coding of data comes very precise and at the same time data must always be interpreted with care.

Since the SNA technique is relatively new to the field of law enforcement and intelligence there is a need for a clear and standard protocol with stepwise proceedings in how to handle network data. In the following sections we present a rough draft of an SNA protocol and discuss some methodological issues and future challenges with respect to the application of SNA that are specific to the field of law enforcement and intelligence.

A protocol draft

First of all, as the previous section illustrated, the collation of data on social networks needs careful planning, attention and accuracy. Making mistakes in this phase can blur all relevant outcomes of the analysis (and may be vital to solve a case). Second, in order to process and manipulate data, it must be sorted and coded into specific categories that are thought about well and identified beforehand (e.g., what kind of information on social ties is of specific interest to the analyst with respect to a specific crime?). This means that the relevant data matrices need to be considerably clear before any data is entered in a data base. Finally, it is of essential importance that the relational data is stored properly in a data base so that the analysis and manipulations are efficiently managed. Fig. 5 addresses some stepwise proceedings that need to be taken into account in order to work with network data. For some steps the √ symbol refers to issues that were discussed in the previous section.

Preparation:

1) Define a meaningful social category of the target group (what actors, ties, or events are included or excluded from the analysis?) and report the arguments used to specify the network boundaries.
   - ✓ Access to network data
   - ✓ Definition of network boundaries
2) Formulate research questions.
3) Identify what analysis routines are needed to answer the research questions.
4) Formulate assumptions (e.g., what ties are considered as friends?).
   - ✓ Assumptions prior to coding
5) Develop a coding system for actor's attributes, activities, and affiliations.
   - ✓ Data reliability
   - ✓ Change over time

Data processing:

6) Gather information on the social ties of actors in the target group.
   - ✓ Time intensive
   - ✓ Handling large datasets
7) Identify the attributes, activities, and affiliations associated with the actors.
8) Create a database of individual attributes (e.g., sex, age, skills, criminal records).
9) Create adjacency matrices of ties between actors (e.g., tasks, logistics, resources).
10) Create an incidence matrix of affiliations that associate actors to events (e.g., locations).
11) Sort the names of actors (e.g., in alphabetical order).
12) Tidy up your data.
    - ✓ Data tidying

Data analysis and reporting:

13) Consider what routines are robust measures to analyze your data.
    - ✓ Missing data
14) Perform the analysis routines and properly store the results in a database.
15) Interpret the results.
16) Report the results.

Fig. 5 Stepwise proceedings in handling network data

The target profile sheet

Klerks (2001) emphasized that a different way of data coding in law enforcement and intelligence is needed that is more enhanced than investigators are currently used to. For any criminal or terrorist organization to be uncovered, the analysis needs to reflect the way in which actors and ties are associated with a variety of variables. One way to accumulate data on adversary networks that may prove useful in the field of law enforcement and intelligence is the *Target Profile Sheet.* The Royal Canadian Mounted Police (RCMP) uses it to profile actors that are involved in serious and organized crime (Strang 2005). The profiles are stored in a database and continuously revised and updated on an ongoing basis. The required input for the target profiles incorporates data that can be relevant input for the analysis of social networks (see Fig. 6). The target profile sheet includes the attachment of criminal roles to actors. Note that this is a qualitative judgment or opinion of the investigator (based on observation) and not based on the structural properties of the network (which is a possibility as well).

A tentative classification of roles

It is recommended that investigators work with conventional language, definitions, tools and coding systems. However, a conventional classification system is currently still lacking and the diversity of functional subsets of roles, for example, is enormous. As a result, many studies report on a variety of categories which limits the ability for comparison (cf. Koschade 2006; Natarajan 2000; Sageman 2004; Williams 2001). To improve this, we introduce a tentative format to categorize law enforcement and intelligence data about targets. A first basic distinction that can be made is that between formal and informal relationships (cf. Van der Hulst 2004). Formal relationships are more or less prescribed role sets between actors that are characterized by some form of task dependence (e.g., boss or co-worker). Informal relationships, on the other hand, are mostly voluntary and close relationships (e.g., friends, acquaintances, neighbors, but also kinship). Sometimes the formal and informal relationships overlap in the sense that a business client can at the same time be (or become) a very close friend. The target profile sheet of the RCMP differentiates six role categories that best identify or describe criminal actors based on the qualitative judgment of the investigator (i.e., strategic managers and organizers, crime brokers, financiers, enforcers, operative fieldworkers, and service providers). Based on the work of various scholars (Natarajan 2000; Sageman 2004: 166; Williams 2001), this classification can be extended with at least five categories (i.e., tactical managers and developers, insulators, communicators, extenders, and crossovers). All in all this creates a tentative classification system presented in Fig. 7 to systematically evaluate the key formal (i.e., strategic, tactical, operational, exogenous) and informal roles in adversary networks.[7,8]

[7] Note that actors sometimes occupy multiple roles at the same time.

[8] Note that the classification is tentative and can be extended, refined or revised.

Personal data:

- Personal details of the target (e.g., name, date of birth, alias, citizenship, place of birth, current residence);
- Additional information on the actor's affiliations (e.g., geographic scope of criminal activity, memberships, habits, addictions);

Criminal history:

- The criminal history of the target (e.g., current and past criminal involvement, organizational affiliations);
- The criminal reputation of the target (e.g., their position, influence and importance in the criminal network);

Skills and expertise:

- The skills and expertise of the target that distinguish them from their peers (e.g., professional training, language skills, technical skills);

Finances:

- The financial situation of the target and their deemed nominees (e.g., known fixed assets and income);

Criminal roles:

- The criminal capacity of the target (e.g., the estimated value, magnitude and complexity of the crime projects that the target facilitates);
- The current role or primary function of the target within the network, how easily the target can be replaced (e.g., the redundancy);

Vulnerabilities:

- What aspects makes the target vulnerable or attractive to law enforcement and other criminals (e.g., personal character, behavior, status, relationships);

Social ties:

- The connections of the target (including family ties), specified by:
  - the type of relationship
  - frequency of interaction (daily, often, occasional, rarely, unknown)
  - degree of criminal association (high, some, little, none, unknown)
  - degree of licit professional association (high, some, little, none, unknown)
  - the nature of the social relations (intimate/familial, close, occasional, distant/acquaintance, unknown)

The investigative research:

- The investigation itself (e.g., previous and ongoing efforts)

Fig. 6 Input for the RCMP Target Profile Sheet (Strang 2005)

The meta-matrix

Exactly what kind of data to consider for the analysis of network relations is up to decide to the investigator. Krebs (2002) emphasized, for example, the importance to identify 'trust networks' (e.g., prior contacts in family, neighborhood, school) and so-called 'strategy and goals networks' (e.g., web sites, travel records). To gain an improved knowledge on the structure, network positions, and social roles, Carley et al (2001) suggested to classify social and organizational systems by integrating multiple and related network matrices into a single interrelated meta-

Formal role categories

Strategic level:

1. SMO **-** Strategic managers and organizers (i.e., the core actors responsible for initiating and guiding criminal activities, who direct others to commit criminal offenses but keep away as far as possible from risks);
2. SFI - Financiers (i.e., actors who use personal resources to fund criminal activity);
3. SCB - Crime brokers (i.e., actors who are responsible for repeated brokerage between various individuals and/or groups);

Tactical level:

4. TMA - Tactical managers and developers (i.e., actors who plan criminal activities related to, for example, import, export or distribution);
5. TEX - Extenders (i.e., actors who purposely recruit new members, whether voluntary or not, to extend collaborations with the upper world);
6. TIM - Insulators and monitors (i.e., actors who guard the core players from external dangers, like infiltration, who transmit directives from core to periphery and who provide information to the core players about weaknesses and problems in the network);

Operating level:

7. OCI - Communicators (i.e., actors who are responsible for effective communication within the network and who provide the insulators with feedback);
8. OEG - Enforcers and guardians (i.e., actors who use or threat to use violence to further criminal objectives and use coercion to minimize defection);
9. OFW - Operative fieldworkers (i.e., actors who actually employ core criminal functions like drug offenses or fraud and meet with customers);
10. OSP - Service providers (i.e., actors who provide necessary services, materials or other assistance to a criminal organization other than funding);
11. OCO - Crossovers (i.e., actors who are part of the criminal network and at the same time are employed in legal organizations – like luggage handlers, chemists, investors, corrupt officials - to provide the network with valuable information and protection);

Exogenous level:

12. EWI - Witnesses and informants (i.e., categories of actors that are related to the investigation and somehow tied to the actors of interest but are not subject of investigation themselves);
13. QUU - Unknown or undecided

Informal role categories

1. FA - Family
2. FR - Friends
3. AC - Acquaintances
4. ST - Strangers
5. UN - Unknown or undecided

Fig. 7 A tentative classification of formal and informal roles

matrix model. This includes the analysis of network relations with respect to the distribution of:

- actors;
- knowledge categories (e.g., on criminal methods like fraud);

- resources and equipment (e.g., pill-pressing machines);
- processes, tasks, activities and roles (e.g., buying, storing, selling, transporting, communicating, screening, guarding, and or transferring money- see also Fig. 7).

It is recommended, however, to also include variables that are at the core of effective organizational structures. Based on the coordination principles for the structural design of effective organizations (Mintzberg 1983), the model can be extended to include:

- informal communication (e.g., expressions);
- orders and instructions (e.g., direction);
- market and clients;
- events and locations (e.g., travel, market and meeting places).

Some of the required input for the target profile sheet (see Fig. 6) closely resembles the meta-matrix, although the target profile sheet has its focus on relations of individual actors and the meta-matrix on the overall criminal process. The point is to examine key characteristics that help us understand how clandestine networks operate in order to counter their dynamics. Tentative categories of enquiry are presented in Table 1. From the type of categories it follows that merely an overview of the presence or absence of ties will not provide rich enough information from the analysis. Prior to data coding a comprehensive content analysis of relational data is therefore recommended.

Content analysis

SNA allows to discriminate between resources (e.g., information, finance, influence) that actors can mobilize and exchange through social ties. Qualitative data (e.g., content analysis of phone taps) can provide law enforcement and intelligence investigators with rich information to understand the group dynamic processes for various social phenomena (e.g., recruitment) in particular social settings (Klerks 2001). Expressions or dynamics that indicate trust, advice, liking, respect, anger, fear, pressure, conflict, hate or revenge (e.g., the use of threatening or intimidating language) provide important directions. Particularly the direction of authority and information in conversations is important since it allows to distinguish between leaders and followers, initiators and receivers, sellers and buyers, users and suppliers, targets and victims and so on. Natarajan (2000), for example, described

Table 1 Tentative categories to describe networks (cf. Carley et al. 2001)

	1	2	3	4	5	6	7	8
1. Actors	x							
2. Knowledge, skills, expertise	x							
3. Resources and equipment	x	x						
4. Processes, tasks, activities, roles	x	x	x					
5. Informal communication and expressions	x	x	x	x				
6. Orders, instructions and direction	x	x	x	x	x			
7. Market and clients	x	x	x	x	x	x		
8. Events and locations	x	x	x	x	x	x	x	

High status actors:

1. Give orders;
2. Request for information to check upon the activities of subordinates;
3. Express satisfaction and praise subordinates (e.g., "good job" or "well done").

Low status actors:

1. Clarify orders;
2. Provide information to report on their activities;
3. Use respectful and formal adjectives (e.g., "Sir" or "Madam").

Fig. 8 Content analysis to distinguish status (Natarajan 2000)

a coding guide for conversations to distinguish between high status actors (i.e., superiors) and low status actors (i.e., subordinates) (see Fig. 8).

Future challenges

The systematic analysis of adversary networks is considered a viable means to gain a more thorough understanding of criminal behavior. SNA is a promising tool in law enforcement and intelligence investigations, but specific methodological problems associated with intelligence data and the lack of experience with SNA applications has long hampered our ability to improve our knowledge of organized crime and terrorism. More research, practical applications and development is needed to identify patterns of activities and other regularities in clandestine networks. This paper identified some important issues to precede operational network studies and offered some practical guidelines and proceedings in how to handle network data in criminological research. Nevertheless, much work remains to be done to establish a sophisticated tool for criminal and intelligence investigators. We emphasize in particular the importance to come up with a topology of adversary networks based on previous network studies, and closely monitoring the methodological development in the field of SNA.

A topology of adversary networks

In a study examining the criminal ties of upper world and underworld actors, Morselli and Giguère (2006) found that, compared to other criminal actors, the ties of 'legitimate' actors that are involved in criminal activities (e.g., politicians, lawyers, accountants, bankers, and businessmen) are:

- low profile and limited in activity (low degree centrality)
- connected to the criminal network but often to only one core member
- rarely connected to other upper world actors who are involved in criminal activities
- more often initiating ties towards criminal actors than the other way around (particularly those involved in finances like money managers and investors)

Combining such insights of network activity, patterns and parameters (cf. Borgatti et al. 1998) from multiple studies of adversary networks will enhance our knowledge

of their typical structures and provide us with leads to counteract them. Hence, more research is needed to eventually come up with an inventory of network parameters and analytical results (including those in other areas like organizational and operational research) that identify patterns of activities and other regularities in criminal and terrorist networks.

Methodological issues and development

In the field of law enforcement and intelligence, research materials are of such amount and quality that advanced methods of SNA are needed that enable sophisticated analysis of automated identification of network parameters and sentiment from textual transcripts and documents (Tsvetovat and Carley 2007; Natarajan 2000; Tyler et al. 2003). Other methodological developments in the area of permutation and computational analysis are needed, for example, to overcome the problem of imperfect data (Borgatti et al. 2006) and to model and analyze dynamic behavior (Carley 2003a, b; Contractor and Monge 2003; Xu et al. 2004: 359–377). In order to further the SNA standards in law enforcement and intelligence and expand our ability to fight serious and organized crime and terrorism, we call for a genuine collaboration of criminal investigators and social scientists.

References

Blau PM (1964) Exchange and power in social life. John Wiley & Sons, NY
Borgatti SP, Jones C, Everett MG (1998) Network measures of social capital. Connections 21(2):27–36
Borgatti SP, Everett MG, Freeman LC (2002) Ucinet 6 for Windows: Software for social network analysis. Analytic Technol, Harvard
Borgatti SP, Carley KM, Krackhardt D (2006) On the robustness of centrality measures under conditions of imperfect data. Soc Networks 28:124–136
Bourdieu P (1986) The forms of social capital. In: Richardson JG (ed) The handbook of theory: Research for the sociology of education. Greenwood Press, NY
Bruinsma GJN, Bernasco W (2004) Criminal groups and transnational markets: A more detailed examination on the basis of social network theory. Crime Law & Soc Chang 41:79–94
Burt RS (1992) Structural holes: The social structure of competition. Harvard Univ Press, Cambridge, MA
Burt RS (2000) The network structure of social capital. In: Sutton RI, Staw BM (eds) Res in organ behavior. JAI Press, Greenwich, CT
Burt RS (2001) Structural holes versus network closure capital. In: Lin N, Cook KS, Burt RS (eds) Social capital: theory and research. Aldine de Gruyter, NY
Carley KM (2003a) Dynamic network analysis. In: Breiger R, Carley K, Pattison P (eds) Dynamic social network modeling and analysis: workshop summary and papers. The Natl Acad Press, Washington DC
Carley KM (2003b) Linking capabilities to needs. In: Breiger R, Carley K, Pattison P (eds) Dynamic social network modeling and analysis: Workshop summary and papers. The Natl Acad Press, Washington DC
Carley KM, Lee JS, Krackhardt D (2001) Destabilizing networks. Connections 24(3):79–92
Chattoe E, Hamill H (2005) It's not who you know - it's what you know about people you don't know that counts. Br J of Criminol 45:860–876
Clark RM (2007) Intelligence analysis: A target-centric approach. CQ Press, Washington, DC
Coleman JS (1990) Foundations of social theory. Harvard Univ Press, Cambridge, MA
Coles N (2001) It's not what you know - it's who you know that counts: Analysing serious crime groups as social networks. Br J of Criminol 41:580–594
Contractor NS, Monge PR (2003) Using multi-theoretical multi-level (MTML) models to study adversarial networks. In: Breiger R, Carley K, Pattison P (eds) Dynamic social network modeling and analysis: Workshop summary and papers. The Natl Acad Press, Washington DC

Cook KS, Whitmeyer JM (1992) Two approaches to social structure: Exchange theory and network analysis. Annu Rev of Sociol 18:109–127
Emirbayer M, Goodwin J (1994) Network analysis, culture, and the problem of agency. Am J of Sociol 99 (6):1411–1454
Fijnaut C, Bovenkerk F, Bruinsma G et al (1998) Organized crime in the Netherlands. Kluwer Law International, The Hague, the Netherlands
Flap HD, Völker B (2003) Creation and returns of social capital. Routledge, London
Granovetter M (1973) The strength of weak ties. Am J of Sociol 78:1360–1380
Harary F (1969) Graph theory. Addison-Wesley, Reading, MA
Harper WR, Harris DH (1975) The application of link analysis to police intelligence. Human Factors 17 (2):157–164
Heider F (1958) The psychology of interpersonal relation. John Wiley & Sons, NY
Homans GC (1958) Social behavior as exchange. Am J of Sociol 63:597–606
Kadushin C (2002) The motivational foundation of social networks. Soc Networks 24(1):77–91
Kleemans ER, Brienen MEI, Van de Bunt HG (2002) Georganiseerde criminaliteit in Nederland [Organized crime in the Netherlands]. Boom Distributiecentrum, Meppel, the Netherlands
Klerks P (2001) The network paradigm applied to criminal organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. Connections 24(3):53–65
Koschade S (2006) A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. Stud in Confl & Terror 29:589–605
Krackhardt D (1998) Simmelian tie: Super strong and sticky In: Kramer RM, Neale M (eds), Power and influence in organizations. Sage, Thousand Oaks, CA
Krebs V (2002) Mapping networks of terrorist cells. Connections 24(3):43–52
Leenders RThAJ, Gabbay SM (1999) Corporate social capital and liability. Kluwer Academic Publishers, Boston, MA
Lin N (1992) Social resources theory. In Borgatta EF, Borgatta ML (eds): Encyclopedia of Sociol. NY, vol. 4:1936–1942
Lin N (2001) Social capital: A theory of social structure and action. Cambridge Univ Press, Cambridge, NY
McDowell D (1998) Strategic intelligence: A handbook for practitioners, managers and users. Istana Enterprises Pty. Ltd, Cooma Australia
McGrath C, Krackhardt D, Blythe J (2003) Visualizing complexity in networks: Seeing both the forest and the trees. Connections 25(1):37–47
McGrath C, Blythe J, Krackhardt D (1997) The effect of spatial arrangement on judgments and errors in interpreting graphs. Soc Networks 19(3):223–242
McIllwain JS (1999) Organized crime: A social network approach. Crime Law & Soc Chang 32:301–323
McNally D, Alston J (2006) Use of social network analysis (SNA) in the examination of an outlaw motorcycle gang. J of Gang Res 13(3):1–25
McPherson M, Smith-Lovin L, Cook JM (2001) Birds of a feather: Homophily in social networks. Annu Rev of Sociol 27:415–444
Mintzberg H (1983) Structure in fives: Designing effective organizations, 6th translated edn. Prentice Hall, Englewood Cliffs, NJ, USA
Morselli C, Giguère C (2006) Legitimate strengths in criminal networks. Crime Law & Soc Chang 45 (3):185–200
Morselli C, Petit K (2007) Law enforcement disruption of a drug importation network. Global Crime 8 (2):109–130
Morselli C, Roy J (2008) Brokerage qualifications in ringing operations. Criminol 46(1):71–98
Morselli C, Giguère C, Petit K (2007) The efficiency/security trade-off in criminal networks. Soc Networks 29:143–153
Natarajan M (2000) Understanding the structure of a drug trafficking organization: A conversational analysis. Crime Prevention Stud 11:273–298
Natarajan M (2006) Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. J of Quant Criminol 22:171–192
Portes A (1998) Social capital: Its origins and applications in modern sociology. Annu Rev of Sociol 24 (1):1–24
Rothenberg R (2002) From whole cloth: Making up the terrorist network. Connections 24(3):36–42
Sageman M (2004) Understanding terror networks. Univ of Pennsylvania Press, Philadelphia
Schwartz DM, Rouselle DA (2008) Targeting criminal networks: Using social network analysis to develop enforcement and intelligence priorities. IALEIA J 18(1):18–44

Scott J (2000) Social network analysis: A handbook. Sage, Newbury Park CA
Simmel G (1950) The sociology of Georg Simmel. Free Press, NY
Sparrow MK (1991a) Network vulnerabilities and strategic intelligence in law enforcement. J of Intell and Counterintell 5(3):255–274
Sparrow MK (1991b) The application of network analysis to criminal intelligence: An assessment of the prospects. Soc Networks 13:251–274
Strang S (2005) User guide RCMP target profile sheet. Royal Canadian Mounted Police, Canada
Tsvetovat M, Carley KM (2007) On effectiveness of wiretap programs in mapping social networks. J of Comput and Math Organ Theory 13(1):63–87
Tyler JR, Wilkinson DM, Huberman BA (2003) Email as spectroscopy: Automated discovery of community structure within organizations. Communities and Technol 81–96
Van der Hulst RC (2004) Gender differences in workplace authority: An empirical study on social networks. Univ Groningen (ICS thesis), Groningen, the Netherlands
Wasserman S, Faust K (1994) Social network analysis: Methods and applications. Cambridge Univ Press, Cambridge
Williams (2001) Transnational criminal networks. In: Arquilla J, Ronfeldt D (eds) Networks and netwars: The future of terror, crime and militancy. Rand Corporation, Santa Monica
Xu J, Marshall B, Kaza S et al (2004) Intelligence security and security informatics. Springer, Berlin/Heidelberg