Detecting and disrupting criminal networks
A data driven approach
Duijn, P.A.C.

Publication date
2016
Document Version
Other version
License
Other

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Chapter 1

Introduction
Criminals organized in networks operate most of the time anonymously behind the scenes. The harm caused by their activities becomes however strongly visible on a global scale. It is estimated that transnational criminal networks generate $870 billion a year, which is equal to 1.5 percent of the GDP and 7 per cent of the world's exports of merchandise (UNODC, 2011). At the same time numerous lives are lost as a result of organized crime activities, due to drug related health problems, the use of firearms and violence, human trafficking, or the smuggling of migrants. The strong presence of organize crime networks in particular countries (e.g. Mexico, Italy) is also associated with diminishing levels of social, cultural, economic, political and civil development and threatens world peace and democracy.

Although organized crime is considered a global phenomenon, its origins are often retraceable to local communities. Criminal networks are embedded in local social network structures formed by neighborhoods, high schools, youth gangs, and sport clubs (Kleemans and Van de Bunt, 1999; Klerks, 2001; Kleemans and De Poot, 2008; Morselli, 2009; Von Lampe, 2009). Within these local settings youth gang members converge with experienced criminals to form local organized crime networks (Von Lampe and Johanson, 2004). Enabled by increased mobility and globalization, local networks can evolve into transnational criminal networks over time (Williams, 2001). The money and power achieved through this development provides them with the opportunity to infiltrate local politics or legal businesses leading to corruption and money laundering (Morselli, 2009). Local influence provides security against the consequences of financial loss associated transnational illicit trafficking operations. Disputes within transnational criminal networks can therefore easily result in violent encounters in local settings, putting innocent peoples lives at risk. Criminal networks on a transnational and local level are therefore inextricably linked.

A typical feature of organized crime networks is that its members and their interactions remain rather opaque and hidden. They are therefore also referred to as ‘dark’ networks’ (Milward and Raab, 2003). Criminal networks use counterstrategies to protect their secrecy in defensive (e.g. using encrypted telecommunication) or offensive ways (e.g., by assassinating criminal informants, by threatening public prosecutors). Law enforcement agencies tasked with reducing the damage and harm caused by criminal networks are therefore struggling with important questions: How can we detect these dark criminal networks and their dynamic structures and activities? What are the most efficient strategies to disrupt and control them efficiently and effectively? How can we prevent them from recovering or adapting to these interventions?

The key to answering these questions lies in understanding how criminal networks emerge and evolve over time within their social settings. This phenomenon has already been studied by criminologists for many years and has provided many useful theoretical insights that
shape the policies and law enforcement strategies of today. At the same time researchers and analysts from other scientific disciplines are confronted with similar network problems and have developed theories and policies for network detection and disruption as well (Newman, 2010). Epidemiologists seek ways to identify the spread of viruses through global networks and try to identify high-risk groups to apply specialized treatment or education (Epstein, 2009; Zarrabi et al., 2013). Neuroscientists study the structure of neurological networks in order to identify specific neuron cells responsible for malfunction of information transfer in the brain in support of treatment of Alzheimer or Schizophrenia (Palop and Mucke, 2010, Liu et al, 2008). Complexity science is a scientific field that addresses such complex network problems across many scientific disciplines. It seeks for universal features in the structure and behavior of complex networks trough data-driven methods of computer simulation and combines these insights to create a generic theoretical paradigm in the study of networks (Mitchel, 2009; Newman, 2010). Although this paradigm contains many relevant concepts, methods and ideas for the study of organized crime, it has mainly been neglected in criminal network research.

This chapter starts with a description of the traditional theoretical perspectives on organized crime and introduces complexity theory as an additional theoretical framework in Section 1.1. Section 1.2 introduces what is currently known about criminal network dynamics in terms of emergence and adaptation. Section 1.3 then introduces the empirical research methods for the study of criminal networks and how methods derived from complexity science contribute to a deeper empirical understanding of network dynamics. Finally, the relevance and central aim of this thesis are presented in Section 1.4.

1.1 THEORETICAL PERSPECTIVES ON ORGANIZED CRIME

Scientific progress depends on the continuing interaction between the analysis of the empirical reality and scientific theory (Popper, 1972). Although many scientific theories about crime have been developed and empirically tested in the past century, theoretical insights about the typical phenomenon of organized crime have remained largely undeveloped. The main cause lies in its complexity; ‘organized crime’ is a catchall concept, which is used to label a diversity of criminal groups and different criminal activities at different scales (Kleemans, 2014). Empirical research in the field of criminology has however led to three main theoretical models about the structure of organized crime, which also influenced the public debate and control strategies in the last four decades: The bureaucracy model, the illegal enterprise model, and the criminal network model.
The bureaucracy model

The bureaucracy-model describes organized crime in terms of pyramid-shaped structures, with a strict hierarchy, code of conduct, internal and external sanction system and a clear division of tasks (Cressey, 1969). This theoretical perspective was developed in the 1960s and is mainly based on the study of Italian Mafia syndicates with strict leadership ranks operating in the United States.

Many criminologists have rejected the bureaucracy model and there is a general agreement that this does not represent the social complex reality of organized crime. Some authors, however, emphasis that researchers should not completely exclude the existence of hierarchies in criminal networks, which is undeniably a feature of criminal networks concerning the Sicilian Mafia, the Hong Kong Triads or the Russian Mafia (Campana, 2011; Varese, 2011; Kleemans, 2014). Such hierarchies are preserved by underlying brotherhoods, which are based on status or fraternization contracts with have their own rewarding system (Paoli, 2003). Within such brotherhoods members obey the hierarchical ranks and can demonstrate a strong intrinsic loyalty to their leaders. Nevertheless, more in-depth studies of the underlying social structures within such brotherhoods (such as the Hells Angels) also demonstrate that the formal hierarchies are easily undermined by informal social connections in the day-to-day operation of criminal activities (e.g. Morselli, 2009). Hierarchical criminal groups are therefore considered more the exception rather than the rule.

Illegal enterprise model

In response to the bureaucracy model, criminologists in the 1970s developed the illegal enterprise model. This model compares organized crime with legal business structures. Scholars emphasize that organized crime should be understood as ‘disorganized crime’, since it is not dominated by one or more criminal groups but by multiple criminal entities that are continuously competing for market share (Reuter, 1983). This model has a strong emphasis on rationally driven offenders and their interactions are explained by the laws of demand and supply. Consequently, opportunities for organized crime arise from a high demand for services and commodities, which have been criminalized or restricted by governments (Kleemans, 2014).

The illegal enterprise-model has contributed to the study of illegal activities in terms of business processes. It is based on the idea that initiation and management of illicit business process requires a coordinated effort by multiple individuals over a certain period of time similar to legitimate companies (Van Duyne and Levi, 2005; Spapens, 2006). Structural analysis of the separate elements of the criminal value chain could reveal ‘weak spots’ within the criminal organization, which provide opportunities for effective countermeasures (Cornish and Clark, 1996; Bruinsma and Bernasco, 2004). Although this model is useful
for explaining supply and demand within illicit markets, its power for explaining predatory forms of organized crime (e.g. racketeering or extortion) is limited since these crimes are not based on the laws of demand- and supply (Spapens, 2010; Kleemans, 2014). Another critique of this approach is that it fails in describing the entities that constitute illegal markets and how they are formed.

Criminal network theory

The unexplained questions following the illegal enterprise model prompted the development of criminal network theory in the late 1990s (e.g. Kleemans and Van de Bunt, 1999; Klerks, 2000). Its main concept is that organized crime is a fundamental part of a larger social environment. Organized crime can only be explained by understanding the underlying social ties and interactions (lanni and Reus-lanni, 1972; Kleemans and Van de Bunt, 1999; Coles, 2001; Klerks, 2001; Morselli, 2009; Von Lampe, 2009). Criminal networks are considered non-hierarchical, fluid and flexible and are based on family, neighborhood, or friendship relationships that provide the social opportunity structure to find trustworthy acquaintances. Social relationships are not formed at random but are restricted by social and geographical distances and boundaries (Feld, 1981).

The criminal network model explains how networks are formed on a local level and how they can evolve into fixed elements in the global criminal economy. It also explains how network positioning or specific attributes of individual actors can enable or limit the criminal opportunities of individual actors within the overall system ((Kleemans en Van de Bunt, 1999; Klerks, 2001; Morselli, 2009; Spapens, 2010). It does not solely focus on finding out who is in charge, but merely raises the question: who is dependent on whom? and for what reason? (Kleemans, 2014). Taking into account network topology makes it possible to identify key individuals, who occupy broker positions in-between different parts of the overall network. Identification of such key players creates excellent opportunities for network disruption (Sparrow, 1991; Bright et al., 2015). Supported by the findings of a fast growing number of empirical studies, there is a common consensus that criminal groups should be understood as flexible and tightly knit networks (e.g. Natarajan, 2006, Morselli, 2009; Carrington, 2010; Nash at al., 2013).

A limitation of criminal network theory is tha social embeddedness is a very broad topic that leads to many different views amongst scholars about it should be defined and studied. Especially the functionality of technical social network analysis (SNA) has led to debate within organized crime research. A common critique is that it is too much aimed at static network representations instead of answering relevant theoretical questions about the dynamics of criminal cooperation following from network theory (Spapens, 2010; Kleemans, 2014). Another critique is that empirical observations are too much focused on networks
at a micro-level, while criminal network theory seeks to understand the interaction with embedded social networks at a meso- and macro level (Soudijn, 2014; Von Lampe, 2015).

Regardless of these internal methodological discussions, the general concepts comprising criminal network theory have provided a consistent theoretical framework for understanding the underlying complex mechanisms, which are at the heart of organized crime existence. This line of theoretical thinking has encouraged researchers to improve their methods for empirically capturing criminal network dynamics and its emergent features. Traditional criminological methodologies have their limitations in support of this endeavor and have steered criminal network researchers to seek for theoretical frameworks and methodologies within other scientific disciplines. Recently, a new paradigm known as complexity science has been introduced in the field of criminology, which aims to answer the questions associated with the dynamics and complexity of criminal networks.

**Complexity theory**

Network theory is considered one of the models within a wider theoretical framework, known as complexity theory. This paradigm is increasingly used as a general language for understanding complex systems across various scientific disciplines, such as economy, ecology, biology, sociology and computer science. It studies how relationships between different parts give rise to complex collective behaviors of a system, and how the system interacts with its environment that is also observed in criminal networks (Gell-Mann, 1995). In complexity science there is no universal definition of complexity, which is why it is mainly described by its distinctive properties. A first property of complex systems is non-linearity. Non-linearity means that the whole is different from the sum of its parts (Mitchel, 2009). Complex systems consist of many, diverse and autonomous components that are highly interconnected and interdependent, which can lead to unpredictable outcomes if they form connections (Chan, 2001). A second property of complex systems is self-organization, which is a form of distributed nonlinear pattern formation. This happens when other actors copy the specific state of a particular actor in the network (e.g. opinions, ideas, behavior).

Positive feedback loops (e.g. financial profits) are the key engines behind this process. Via positive feedback loops a random event can be amplified into a macroscopic level of organization. Negative feedback loops can also emerge if a counterbalancing force (e.g. law enforcement interventions) prevents the system to grow nonlinearly (Mitchel, 2009). Negative feedback contributes to the controllability of complex systems. A fourth property is that self-organization can lead to emergence, which means that large entities, patterns and regularities emerge out of interactions amongst smaller or less complex entities that do not exhibit such properties (Sloot et al. 2013). Because the macroscopic system emerges out of the independent behaviors and feedback loops amongst its individual elements, complex systems are unpredictable by nature (Figure 1.1).
The emergence of patterns of transnational organized crime can also be explained by complexity theory, which can be demonstrated by an example derived from law enforcement practice:

The red light district in Amsterdam is a common meeting area for criminals from various cultural backgrounds. Within one of the bars a Spanish-speaking member of a Dutch criminal group by coincidence meets a member of a Dutch Colombian drugs cartel and because they regularly visit the same bar a friendship is formed over time. This friendship leads to mutual trust creating the opportunity to set up a trafficking route from Colombia to the Europe. The result is an exclusive connection between two local criminal clusters along the lines of this individual friendship. The cocaine trafficking operation is successful and expands over time in frequency and quantities. As more people get involved other interdependent social connections emerge between other members of both clusters by the mechanism of self-organization. Subsequently, the positive feedback loops resulting from the financial profits, attracts other local criminal clusters from Belgium, Germany or the UK to engage in the cocaine trafficking activities as well. The result is the emergence of a complex macroscopic system involving many local clusters at the two sides of the Atlantic. This enables the local clusters to control global cocaine trafficking logics at the same time in different points in space. In other words, their sum is more and different than sum of its parts (Anderson, 1972).

However, if one of the individual members within a local cluster autonomously decides to leak information to the police the trafficking ring, the complete network and its local clusters may become compromised. This may cause a negative feedback loop (e.g. fear of detection), which may result in the collapse of the organization at a macro level. Alternatively, the criminal network could adapt or evolve to increased law enforcement attention, by shifting to another form of crime or change their trafficking routes (e.g. local production of synthetic drugs). Subsequently, changes in the behavior of individual members could lead to topological evolution of the network, leading to a more dispersed instead of a dense network topology. This could make the individual members and their criminal behaviors harder to detect and disrupt by law enforcement.
This example demonstrates how microscopic and macroscopic patterns of behavior are in constant interaction with each other and with the elements of their environment. Adaptation and evolution as a result of external pressures are part of a specific area within complexity science: complex adaptive systems theory.

**Complex adaptive systems theory**

Complex adaptive systems (CAS) are defined as complex systems that have the capacity for adaptation. CAS are studied as an environment within which many and diverse actors act and react to each other’s behaviors, as their combined macroscopic structures adapt and evolve over time (Holland, 2000, Gell-Man, 1995). Typical examples of CAS are stock markets and the complex web of cross border holding companies, the internet that is composed and managed by a complex mix of human and computer interactions, ant colonies, and flocks of starlings displaying deceptive macroscopic behaviors to distract their natural enemy: the peregrine falcon (see Figure 1.2).

Criminal networks and law enforcement organizations also form a CAS, in which the process of complex adaptation unfolds from criminal networks learning behavior as a result from targeted law enforcement operations and visa versa. Kenney (2007) applies the theoretical concept of complex adaptation to explain why the leadership interdiction (targeting of kingpins) strategies applied to the global cocaine trafficking network of Pablo Escobar’s Cali Cartel has been ineffective. On the basis of numerous interviews with intelligence experts and some convicted members of these two groups, he found that both networks learned -through a process he defines as *competitive* adaptation- that a strong reliance on crucial hub positions makes the overall system vulnerable to deliberate attacks aimed at leadership positions. Instead they learned through trial and error that a flat organizational structure is harder to detect and disrupt by law enforcement agencies.
Thinking in terms of CAS teaches us how adaptation as a result of external forces could lead to topological shifts enabling criminal network resilience. Kenney (2007) concludes that the topology of Pablo Escobar’s global criminal network evolved from a cartwheel network into a chain network as a result of deliberate hub-attack strategies by the FBI (Figure 1.3). A similar learning process shaped the centralized network of Al-Qaida ten years ago into a dispersed worldwide franchise network of interdependently operating terrorist cells that wave the same flags (Kenny, 2007). In current times, it is not inconceivable that the lessons learned by Al Qaida, also shaped the way Islamic State has emerged as an effective leaderless multinational *franchise* organization composed of militants and terrorist cells operating independently across multiple territories around the world. CAS theory merges well with network theory, to provide a broader theoretical framework for understanding not only criminal network structures but also criminal network dynamics and its impact on network topology and resilience over time.

**Figure 1.3:** The evolution of Pablo Escobar’s global criminal organization as a result of competitive adaptation and self-organization after deliberate hub attacks by the Drug Enforcement Agency (DEA) in Colombia (Kenney, 2006)

### 1.2 CRIMINAL NETWORK DYNAMICS

Empirically capturing the (temporal) network dynamics is one of the major challenges within complex adaptive systems science (Sloot et al., 2013). Especially in the field of criminal networks, many questions about the dynamics as a result of network disruption have remained unanswered. Empirical research in the field of complexity science has however uncovered some universal mechanisms that influence these dynamics, including the emergence, resilience, adaptation and evolution of networks (Albert et al., 2000; Sloot et al., 2013). Such mechanisms apply to complex criminal networks as well, and provide us with a framework to understand these dynamics from a macroscopic perspective. Before
the current state of knowledge concerning these dynamics is discussed, the difference between dynamics ‘on and of’ networks will be explained in the following Section.

**Dynamics on an of networks**

Within the science of complex adaptive systems there is an important distinction between dynamics of and on networks (Sloot et al., 2013). ‘Dynamics on networks’ refers to changes of the states of the nodes in the network without changing the network topology itself, e.g. spreading phenomena, proliferation and diffusion (Figure 1.4). In criminal networks a shift in state can refer to an individual criminal moving from one dominant criminal activity to another, for instance from drugs trafficking to migrant smuggling as his or hers dominant criminal activity. Such shifts can be prompted by external influences, such as intensified custom controls that restrain the current activities or improved opportunities for profit in other illicit markets. Geopolitical or technological developments can enable such opportunities.

![Figure 1.4: Interaction between dynamics on networks and dynamics of networks (Gross & Blasius, 2008)](image)

When the whole system adjusts to this new functionality, topological evolution may also occur. Whereas drugs trafficking activities may flourish within an ecosystem of tightly knit criminal groups cooperating internationally along a chain of legal infrastructures (e.g. ports, airports), migrant smuggling may thrive better within a sparsely organized networks of freelancers operating at different locations at the same time. Changes in the state of the individual nodes and overall functionality of the network could therefore eventually lead to evolution of the way complex systems are spatially and temporally organized. Such phenomena, which bring change in network topology over time, are known as the ‘dynamics of networks’ (Sloot et al, 2013). On the contrary, topological change may also affect its functionality, efficiency and resilience against disruption, causing new shifts in
the state of individual nodes. ‘Dynamics on networks’ and ‘dynamics of networks’ are therefore inextricably linked and particularly relevant to understand the dynamical ecosystem of (transnational) organized crime. The next Section describes how these mechanisms contribute to the emergence and evolution of criminal networks.

Macroscopic dynamics on criminal networks following the European migrant crisis
An example of a dynamical shift was recently observed during the European migrant crisis. The unstable situation and dependence of migrants on local infrastructures provided criminal networks with the opportunity to gain easy profits through the smuggling of migrants to the EU. Criminal networks originally specialized in controlling drugs trafficking routes redirect their logistics and control over border crossings (e.g. across the Western Balkan route), towards the smuggling of migrants. Such shifts start within a local context, initiated by just a few criminal groups. As these local shifts turned out to be very profitable, this news spread across other European countries and networks. It may have triggered other local criminal groups along the transnational trafficking routes to shift from drugs trafficking to migrant smuggling as well, resulting in macroscopic shifts in the functionality of a chain of transnational criminal network as a whole. (Source: Europol- Interpol, 2016).

The emergence of criminal networks
Criminal networks do not emerge randomly. To cope with uncertainties, deception, and the threat of violence, trust is a necessary condition for initiating criminal cooperation. Building trust takes time and is established within a local social context that was established well before the actual criminal career. Criminal networks therefore rely on deeper layers of durable social relationships of which its origin is often retraceable to school classes, youth gangs, sports teams and local diaspora communities (Von Lampe and Johansson, 2004).

Once a newcomer is accepted as a trustworthy member of the criminal network his or hers social- and criminal network (ego-network) may further expand over time (Kleemans and van de Bunt, 1999; Klerks 2001; Morselli, 2009). It is not uncommon that criminals who collaborated in the past will do so again in the future (Von Lampe, 2015). New criminal ties therefore also emerge from past co-offending or out of shared loyalty to the same criminal group. This process is enabled by the presence of offender convergence settings, which can be represented by physical or virtual meeting places, such as local bars, private parties, sports clubs, prisons or Darknet forums, where criminal accomplishes can be found or disclosed information can easily be exchanged (Felson, 2006). According to Felson this is where criminal cooperation persists, even though the actors may vary. The social opportunity structures, which also emerge within these offender convergence settings, shape the evolution of criminal networks and the recruitment of new members. Not occasionally this happens in the later stages of a person’s life course, or even after a legitimate career (Kleemans and Van de Poot, 2008).
On the long term these local dynamics can expand in non-linear ways, best described as a *social snowball-effect* (Kleemans and Van de Bunt, 1999). As one’s network grows over time the dependence on other criminal’s resources (money, contacts and knowledge) gradually declines to a point were membership of the network does not provide new opportunities or resources any more. Well-established network members may therefore start of independently by attracting people from their own social environment to form new criminal clusters.

Spapens (2010) provides a framework to understand these micro-macro interactions by distinguishing between the micro-, meso- and macro networks. Following the global scale of transnational illegal markets, macro networks are defined as a worldwide network composed of interconnected regional clusters (meso-networks). Meso-networks are embedded in local settings and are defined as regional pools of latent criminal connections out of which new co-offending emerges. Micro-level criminal networks are defined as local operational collectives consisting of a little number of actors cooperating for one or several criminal endeavors. Afterwards these collectives may fall apart due to arrests, seizures, or internal disputes. Shortly after such a collapse new accomplishes are found within the embedding meso- networks, which remain robust sources of new emerging co-offending initiatives over time (Kleemans and van de Bunt, 1999; Klerks, 2001; Spapens, 2010; Von Lampe, 2015).

The emergence of the criminal macro-network out of the interactions between its individual parts is mainly driven by connectivity. Globalization, technology and enhanced transportation enable connections between meso-networks and break away the geographical or cultural barriers between separate pools of co-offending. This can eventually result in the emergence of small-world networks (Milgram, 1967; Watts and Strogatz, 1998; Coles, 2001). A small-world network is a type of network in which most actors are not neighbors of one another, but most actors can be reached from every other actor through a small number of steps (Watts and Strogatz, 1998). Its structure is somewhere in-between *regular* networks and *random* networks (see Figure 1.5) and the overall topology is best described as loose connections between densely connected clusters.
Small world networks may contain many structural holes. A structural hole refers to the vacuum that exists between two or more densely connected clusters or meso-networks. Driven by the rules of supply and demand such structural holes provide opportunities for criminal actors to organize new flows of goods, money and information (Burt, 2002). Criminal brokers with unique networking- or language skills play an important role in bridging these gaps. They utilize their social- and language capabilities to bridge (regional) criminal meso-networks across continents to procure new resources and expand their criminal business, e.g. setting up global drug trafficking routes (Bossevain, 1974).

Criminal brokers rely strongly on social capital and human capital to obtain such a network position. Social capital refers to the strategic advantage that a person obtains from his or hers structural positioning within the overall network (Burt, 1992). The criminal broker for instance, derives his or her power and influence from the dependency of other participants on both sides of the structural hole that he or she occupies. Social capital is related to the weak ties (non-redundant) a person is able to maintain in his ego-network (Granovetter, 1983). Empirical case studies show that the ability to inhabit weak ties is an important enabler of a successful criminal career (Morselli, 2001; Kleemans and De Poot, 2008). Maintaining such strategic advantage remains a challenge in itself. It depends on the unpredictable macroscopic behaviors and structure of the overall criminal system. The need for efficiency in communication and cooperation on both sides of the weak tie may eventually results in more strong ties, taking away the strategic advantage. Consequently criminal brokers may seek for new brokerage opportunities, leading to additional connections between criminal meso-networks and strengthening the small world effect.
Another factor leading to strong network positions is human capital. Human capital does not rely on structural network positioning, but on the personal resources an individual is able to provide the network, such as unique skills, knowledge or reputation (Hagen and McCarthy, 1998; Von Lampe, 2009; Robins, 2009; Bouchard and Nguyen, 2010). Specific skills may be needed for organizing or completing a specific criminal logistical process, such as building up illegal cannabis cultivation sites or setting up a money laundering scheme. Typical examples are lawyers, accountants, bankers and other financial professionals, who utilize their knowledge and legal position to facilitate criminals with investing their criminal proceeds (Williams, 2001).

Individuals with high human capital may increase in social capital as well. There may be a high demand for their unique skills, knowledge or resources amongst different criminal groups. The individuals providing such resources may end up providing crime-as-a-service for multiple ‘clients’, and as this unfolds naturally become a criminal broker between isolated criminal groups within the criminal macro-network (Robins, 2009; Kleemans and Van de Poot, 2008; Spapens, 2010). Without proper protection within the opportunistic criminal underworld such positions can become extremely vulnerable, since removal of these key-individuals could also be seen as a strategy of one criminal group to frustrate the criminal logistics of another.

The increased connectivity associated with social- and human capital on a micro-level, fuels the emergence of global patterns within the criminal macro network. Moreover, the diffusion of social- and human capital within criminal networks, leads to bottom-up self-organizing behavior that shapes the overall macroscopic patterns of the overall system. Research has shown that such topologies, which emerge from the bottom-up, can become highly robust and resilient against disruption and noise (Quax and Sloot, 2013; Czaplicka et al., 2014).

**Resilience and adaptation of criminal networks**

The emergence of complex adaptive systems doesn’t happen out of the blue; on every level of organization (micro-macro) there is a continuous interaction with its environment (Chen, 2001). Social networks, competing criminal groups, and law enforcement agencies are also in continuous interaction with each other, which shapes the overall structure, growth or decline of the criminal network over time. Network resilience is key to surviving disruption. It is defined as ‘the capacity to absorb and thus withstand disruption and the capacity to adapt, when necessary, to changes arising from that disruption’ (Bouchard, 2007; Ayling, 2009).
Adaptation is an important element of network resilience, however, if a network’s topology is robust enough to withstand disruption adaptation will not occur. In criminal networks this happens when the impact of an intervention does not affect its primary criminal operation or exposure of its members. This capability depends strongly on the emerged topological advantage of the network as a whole (Barabasi et al., 2000; Sloot et al., 2013). Scale free networks, which are centralized around nodes with many direct connections (hubs), are highly resilient against random attacks. The hubs provide many alternatives for information to flow through the network if any random node is removed. However, if these hubs are deliberately disrupted, such alternatives will soon dry out. By removing just a few hubs, different parts of the network therefore become separated and may lead to complete collapse of the network (Barabasi et al., 2000). Alternatively, the network may survive through adaptation and shift from a scale-free structure into a more robust form. Adaptation varies from minor evolutionary modifications within its topology to complete displacement from its primary criminal activities or geographical area of operation (Ayling, 2009). The ability to adapt to disruption is a typical feature of criminal networks.

Contrarily to licit network, the resilience of illicit networks depends on the dynamical balance between efficiency and security (Baker and Faulker, 1993; Morselli et al., 2006). Efficiency of the criminal network refers to the efficient exchange of information and goods amongst its actors that is necessary in order to coordinate complex criminal operations across different geographical areas at the same time. Secrecy refers to the shielding of the flow of information about criminal activities across the network. The tradeoff between these two elements has a strong effect on network topology (Erickson, 1981; Milward and Raab, 2006).

The high demand for efficiency leads to increased density and redundancy in the networks overall structure. The necessity for tight security on the other hand leads to sparse network topologies, in which information travels via different non-redundant compartments. The balance between efficiency and security depends on the network’s objective and functionality. Criminal networks with the objective of maximizing financial profit, will have to trade efficiency for security to coordinate different criminal activities in short periods of time. Terrorist network, for which accomplishing their objective depends on the long-term planning of one successful terrorist attack, can afford themselves more investments in security (Morselli et al. 2006).

The level of external pressure that threatens the criminal network’s existence may fluctuate over time (e.g. by law enforcement priorities). By trading efficiency for security criminal networks naturally anticipate to such fluctuating pressures in a flexible way. A response to a single arrest may be to seek for a suitable replacement outside of the criminal networks
trusted core, temporary resulting in increased network efficiency at the cost of security. In case of multiple arrests at the same time, however, the pressure may exceed a certain tipping point at which the risks of seeking replacements becomes too high. Then the whole system may fall apart. Under what circumstances such tipping points occur remains uncertain. More extended empirical research of the dynamics of and on criminal networks is needed to understand this mechanism. The next Section describes the different steps and methodologies, which support the development of such a deeper empirical understanding.

1.3 METHODOLOGIES FOR STUDYING CRIMINAL NETWORKS

The previous paragraph shows that criminal networks could be understood as complex adaptive systems. To understand the dynamics inherent to this type of networks, more empirical research is needed. Since criminal networks show different levels of complexity and actively hide their activities at the same time, this is not an easy endeavor. Particularly when the objective is to detect and disrupt them effectively. This Section gives an introduction to the current and potential future approaches for empirical research in this field. In this regard, a distinction can be made between three different steps for studying criminal networks: inference, analysis, and simulation.

Inference of criminal networks

Criminal network data is inevitably incomplete (Sparrow, 1991; Borgatti, 2013; Campana, 2016). Contrary to licit networks, dark networks are generally not easily observed. They are naturally distrustful and generally not committed to self-surveys about their relations with main accomplishments. Criminologists have therefore adopted many strategies to increase the likelihood of observing criminal behavior and interaction. Some went to prisons to interview inmates (Morselli and Trembley, 2004) while others committed to participant observation methods to observe the criminal and social behaviors from within the network themselves (e.g. Zaitch, 2009). Such studies led to unique case descriptions of criminal networks at the individual level, but were not intended to create an overview of the criminal network at a macro level. For creating such a system-level perspective on criminal networks, many researchers found access to law enforcement data. Inference of criminal networks out of such data sources is unavoidably biased towards the initial purpose for which the data was collected (e.g. evidence, intelligence). In criminal network research attention needs to be paid to such limitations and its impact on the inference of criminal networks. Inferring reliable criminal network representations out of incomplete data has therefore become a research topic in itself.
Law enforcement and intelligence agencies are the only legal entities with the authority to utilize advanced investigative methods that infringe on a suspect’s personal privacy, such as wiretapping, surveillance, and recruitment of informants. The intelligence-led policing doctrine that has become introduced within many law enforcement agencies in the past years has resulted in vast amounts of network data that become more and more accessible for network researchers. The majority of criminal network studies are therefore based on law enforcement and intelligence data. The observations retrieved from these sources provides unique structured data about an offender’s personal and criminal activities and his/hers cooperation with other criminals, but are most likely biased towards the aim of the investigation or intelligence collection purposes. The binary network data retrieved from such data-sources should therefore always be analyzed in combination with the contextual content of the links (Varese, 2012).

Raw law enforcement data comes in many formats. Most often the data needs to be cleaned and parsed in order to extract the relevant criminal relations. It is not uncommon that the data is structured in a 2-mode format, meaning that persons in a database are mutually linked to the same piece of information (i.e. document) but not directly to each other. In such cases a 1-mode co-affiliation projection (person-person links) needs to be created out of 2-mode network (person-document links) (Borgatti and Halgin, 2012). For reliable inference of criminal networks it is therefore essential to understand the way each data-source is processed. Persons may for instance be linked to the same document for administrative reasons (e.g. database cleaning), without having a real-life criminal relationship. If not processed properly, such artifacts could lead to a distorted criminal reality. The reliability of such co-affiliation network projections might however be refined by adding weights to the links based on the number of documents that links two persons in the network (Swartz and Rousselle, 2008; Campana, 2016).

In addition to law enforcement data representing the connections amongst criminals in the physical world, there is an increasingly vast amount of (semi-) open source data available which provides insight into criminal networks within the virtual world. Darknet marketplaces and other online forums represent new places for offenders to converge into networks. These for a can however be accessed by criminals, law enforcement experts and researchers alike. Automated methods for inference of networks out of such increasing amounts of data are becoming increasingly important. These procedures are based on specific software that automatically indexes and searches all content available on such forums or servers. Webcrawling (i.e. mirroring) is such a method that concerns the indexing and copying of webpages (Olston and Najork, 2010). First, all hyperlinks on a single webpage are downloaded and indexed. The crawler then visits all linked pages and downloads all links on these pages as well. Webcrawlers are used in conjunction with
**webscrapers**, which seek for specific pieces of information in the content of webpages. Web scrapers need to be taught what to search for (e.g. dates, names, content) and how to store that information in a database or spreadsheet (Decary-Hetu and Aldridge, 2015). Outside of the online environment Diesner and Carley (2004) developed a text-analysis algorithm that automatically creates network representations out of unstructured text, such as law enforcement reporting. Such techniques have already provided criminologists with unique one-on-one network observations of hacker-networks (e.g. Decary-Hetu et al., 2014), online drugs forums (Christin, 2013), and online child-pornography networks (Bouchard et al, 2014).

Another method for inference of criminal networks is the simulation of criminal networks through complex agent network models (Mei et al, 2015). This method is originally developed to capture the multi-scale spatial-temporal characteristics of complex systems, meaning the interaction between individual-level and global-level dynamics of a system. Agent-based models consist of two key components: a population of agents and a simulated environment in which they are situated. Agents are defined as a member of the population represented by an autonomous decision making entity. Similar to a real population, agents exhibit individual preferences, characteristics, and behaviors (e.g. gender, age, preferred social group). Agent behavior is defined by a series of action rules, outlining how agents act under certain conditions. The spectrum of decisions is often inspired by theoretical concepts. The behavior of an individual ‘particle’ (network member) and its interaction with other ‘particles’ is then analyzed and translated into rules for agent behavior simulation (Bonabeau, 2002). By simulating a set of agent behavior rules and making them interact macroscopic system level phenomena start to emerge.

Agent-based modeling has already become an experimental field in computational criminology and may become an important method for analyzing the complex macroscopic systems of crime (Birks et al, 2012; Davia and Weber, 2013). So far this method has mainly been applied to high volume street crime (e.g. burglary) that relies heavily on routine activity theory (Cohen and Felson, 1979) rational choice theory (Cornish and Clarke, 1986) and crime pattern theory (Brattingham and Brantingham, 1993). The rational offender behaviors that follow from these perspectives are suitable for modeling offender decision-making processes in target selection.

This method also holds a strong potential for studying the dynamics in social networks, such as criminal networks. There is also a growing knowledge about how offenders choose their co-offenders. If this leads to the development of parameters for the decision to co-offend, it may hold a strong potential for inference of simulated criminal network formation as well. The macroscopic phenomena can be simulated as a result of changes
on a microscopic level (e.g. removal of agents). Reliability of this approach is however strongly dependent on a set of rules that represent the rational behavior of agents, while emotional irrational decision-making is also part of the offender behavior. The outcome of this procedure should therefore always be interpreted as an approximation of the criminal reality. Real-life data should always provide the necessary validation of the generic criminal network structures developed by ways of computer simulation.

Analyzing criminal networks

Although there is a general consensus that criminal groups should be studies in terms of networks, some scholars disagree about the empirical methodology by which this should be observed (Spapens, 2010). Traditionally, research in the field of organized crime has relied mainly on qualitative methods involving the manual analysis of court- and police files and interviews with law enforcement professionals (e.g Reuter, 1983, Fijnaut et al, 1998; Kleemans and van de Bunt, 1999; Klerks, 2001; Spapens, 2006). Recently, other methods have been added to the toolkit for organized crime research, such as social network analysis (SNA). This is a method by which criminal networks are structurally analyzed in terms of actors (nodes) and relationships (edges). By coding network data in a binary format within a matrix structure, it is possible to visualize networks and calculate some of its features with the help of mathematical metrics. The application of SNA is however also not without limitations, and often leads to discussions about the validity of the findings. This Section introduces and compares these two approaches.

Theory-driven qualitative approach

Theoretical frameworks mainly drive the qualitative approach in the study of organized crime. These frameworks provide the necessary definitions to consistently identify the elements of criminal cooperation within a predominantly top-down approach. Empirical research is often based on an individualistic and manual analysis process, consisting of the collection of case studies inferred from interviews, surveys or police and court files. The analysis of data is guided by a list of research questions also derived from a theoretical framework. The strength of this method is that it provides a collection of detailed empirical case studies and narratives that after clustering and further interpretation lead to more general insights into the embedding social factors behind organized crime (Kleemans, Van Brienen and Van de Bunt, 2002; Klerks, 2000; Spapens, 2006). It is an approved method within the study of organized crime and has led to important contributions to its understanding, especially in relation to the social embeddedness (Kleemans and Van de Bunt, 1999), local breeding grounds for organized crime (Klerks, 2000), different levels of structure in organized crime (Spapens, 2006), and careers in organized crime (Kleemans and De Poot, 2009; Van Koppen, 2010).
Although this approach has formed an important foundation for putting the study of organized crime on the agenda of criminology practice, it is not without limitations. A first practical concern is that the method is very time-consuming and therefore less suitable for studying large datasets in which criminal structure and dynamics remain hidden (Kleemans, Van de Bunt and Kruisbergen, 2012). Because the data is analyzed manually, researchers need to make selections within the available data for practical reasons. Researchers therefore need to choose between a ‘broad and global’ or ‘selective and intensive’ approach for analyzing the data (Van de Bunt et al. 2007). Although the complexity of organized crime thrives on the interaction between the microscopic individual properties of network members and the macroscopic properties of the networks they form, qualitative research is limited in empirically integrating both perspectives at the same time.

Alternatively observations within individual case studies are extrapolated to draw conclusions about organized crime as a whole. These extrapolations rely strongly on set theoretical frameworks, which increase the risk of viewing such case studies trough a certain predetermined lens. Consequently, aberrant macroscopic patterns of co-offending or adapted mechanisms of criminal network emergence may be overlooked.

Many qualitative studies of organized crime are based on police- or court files, which may be strongly affected by legislation. For instance, article 140 in the Dutch penal law is specifically aimed at prosecuting membership of a criminal organization, strongly resembles the elements of the traditional hierarchical criminal organizations. Data that is irrelevant to these elements may therefore be left out of the final case file. This may have an effect on the individual researcher’s observation of the structure and dynamics presented by criminal justice data.

Lastly, not all qualitative empirical studies explain precisely how the process from raw data to conclusions has unfolded, meaning how the complex data has been processed, clustered and interpreted. This limits the extent to compare the findings with other qualitative studies.

**Data-driven approach**

In addition to the theory-driven approach there is the data-driven approach.¹ The data-driven approach seeks rather than assumes structure, by taking nodes and their ties as the starting point for the bottom-up structural analysis of criminal networks (Campana and Varese, 2013; Campana, 2016). Social network analysis (SNA) is one of the primary data-driven methods in criminal network research, which originates from anthropology

---

¹ also known as instrumental approach (Von Lampe, 2009; Campana, 2016)
Sparrow (1991) was the first to introduce this methodology within organized crime research and also stimulated its application within law enforcement practice. SNA allows criminologists to add network visualizations (graphs) and mathematical measures (metrics) of centrality, density and clustering to the researchers toolkit, to help create a deeper and data-driven understanding of large amounts of criminal network data. It combines quantitative mathematical techniques to explore large datasets of criminal associations to identify relevant topological features that require further qualitative in-depth analysis. Since 2000 this field of research is growing fast, with many studies aimed at unraveling network structure, identifying key players, network resilience and network adaptation (e.g. Morselli, 2009, Natarjan, 2006; Papachristos and Smith, 2014; Calderoni, 2014; Bouchard, 2007; Malm and Bichler, 2011, Bright and Delany, 2013).

The main limitation of the data-driven approach is that its results are sensitive to missing data, and exactly this is one of the inevitable aspects of law enforcement data on which most SNA research is based (Campana, 2016). Some criminologists have therefore become skeptical towards the quantitative application of SNA, or hold the opinion that SNA should completely be excluded from the criminal network research field (Kleemans, 2014; Spapens, 2013, Soudijn, 2014).

Network researchers within other scientific disciplines have however made the ‘missing data issue’ a line of research in itself and study its impact on the results or seek ways for improvement. In this regard two types of missing data can be distinguished: missing links and missing nodes. Both can have different impact on the validity of criminal network representations. Borgatti et al. (2006) tested whether statistical network features remain robust when ten percent of the known links and nodes were added or ten percent of unknown links or nodes were removed from different types of criminal networks. Additionally, Xu and Chen (2006) looked at the removal of more than ten nodes and links on network topology for dark networks. Both studies conclude that macroscopic properties of the networks observed did not change when missing links were added or known links were removed. The networks identified through law enforcement sources were robust despite the likelihood of missing data. Campana and Varese (2011) and Berlusconi (2013) specifically studied the effects of missing data in networks inferred from wiretap data. They also found that general network measures within criminal networks, such as betweenness- and degree-centrality, remain robust against missing data.

---

2 A more technical description of social network analysis methodology is provided in chapter 2 and 3.
Other results suggest that the impact of missing data depends on the size of the network. Hence, for small networks consisting of less than ten nodes the results become highly sensitive to missing data as the absence or presence of one node can change the topology of the network as a whole (Burcher and Whelan, 2015). The impact of missing data is therefore dependent on the level of analysis: individual, group or system level.

Although missing data in criminal network research is unavoidable, these studies suggest that its impact can be measured or controlled when the datasets become larger. A data-driven approach is therefore optimally utilized in research that concerns large criminal networks, which are studied at the group or system level. Internal and external validity checks should however always be performed at the start of network analysis at any level (Campana and Varese, 2012). It is important to combine data sources when inferring criminal networks and relational meta-data should always be checked against its qualitative content.

Another relevant method for unraveling criminal networks in a data-driven approach is crime script analysis. Its application is used to obtain insight into the individual positions of actors within a criminal network. Cornish (1994) was one of the pioneers describing criminal markets in terms of crime scripts. A crime script is defined as a systematical blueprint of the different phases of a criminal business process, which each consist of different facets (i.e. steps). The permutation of the possible combinations to pass all phases, results in a combinatorial explosion of possibilities, which is an indicator for the flexibility and resilience of the criminal operation. In other words, the more options (facets) build into the crime script to pass the different phases, the more resilient the crime script is against disruption.

Bruinsma and Bernasco (2004) combined crime script analysis and social network analysis to describe the flexibility within the criminal markets of heroin trade, human trafficking, and car theft. They found some evidence that the structure of criminal networks was shaped according to the features of the criminal activities and illegal markets, for instance the possible legal and economic consequences of the specific criminal activities. Additionally, Morselli and Roy (2008) integrated crime scripting with SNA methodology in labeling different actors within a criminal network according to their involvement in the different phases and facets of the crime script of organized car theft. They identified the importance of brokers between the different roles in the crime script. According to Sparrow (1991) these actors have low ‘substitutability’ and are therefore interesting targets for network disruption, because most of the criminal network depends on just a few actors for a successful outcome. Sparrow (1991) emphasizes that disruption of actors with specific skills might have major consequences for the criminal network, as compared to actors involved
in more general tasks or roles. The notion within law enforcement that scripting helps to
detect weak spots within criminal networks, has led to advances in the way data is pro-
cessed in databases. More role-specific information concerning the involvement of persons
in crime scripts is therefore becoming available to researchers. This makes it possible to
analyze vast amounts of network data in conjunction with crime script data together in
one data-driven approach, which creates the ‘third generation’ network analysis as previ-
ously announced by Klerks (2001).

**Modeling and simulating criminal networks**

Fuelled by increased computational capacity and sophisticated quantitative models the use
of mathematical and computer models have grown considerably in many scientific fields.
In the field of computational social sciences it uncovers dynamical crime patterns that
could not have been detected 20 years ago (Lazer, 2009; Devia and Weber, 2013). Com-
putational models allow researchers to construct simulations of dynamical social systems,
which capture their key elements at a controllable level of complexity (Birks et al., 2012
Lazer, 2009). This provides researchers with the opportunity to experiment with different
manipulations of one or more components of a particular system (e.g. criminal network)
and measure how this impacts others. It provides opportunities to conduct experiments,
which would be technically, financially, or ethically difficult to conduct in real-life.

Computational models can be divided into explanatory models that aim to increase under-
standing of how that system might function and predictive models that aim to predict the
outcome of a system (Birks et al., 2012). Explanatory models are more theoretical in nature
and act as formalized thought experiments aimed at identifying under what circumstances
certain outcomes of a system may arise. One of such methods is agent-based modeling
described above, by which virtual worlds are created through simulated populations of
heterogeneous, autonomous agents (actors) (Epstein, 1999). Moon and Carley (2007) used
agent-based simulation to predict the evolution of a terrorist network across time and
space. They added the dimension of space by also simulating the emergence of relations-
ships between agents and locations, which led to insights into effects of geospatial change
on the structure of terrorist networks.

Predictive models rely on detailed and well-collected parameter data to estimate macro-
scopic systems behavior. Based on these historical data it is possible to generate scenarios
for future dynamics of and on criminal networks. The study of criminal network dynamics
by scenario generation through predictive computational modeling is still in its infancy.
There is however an increasing number of studies concerning its application in the field
of terrorist network research. Prompted by the events of 9-11 and the terrorist attacks
in Madrid, London, Paris, and Brussels many computational and network scientists have
developed models for predicting terrorist activities and the emergence and evolution of terrorist networks.

Allanach et al. (2004) for instance developed a transaction-based model, which relies on the significant links between events and entities in the data that might involve suspicious terrorist network activities. An event in which a person withdraws a vast amount of money from her/his bank account and then shortly buys a plane ticket together with explosive chemicals forms a *tell-tale* (i.e. signal) for the planning of a terrorist attack. The algorithm uses the data from historic terrorist attacks to identify such *tell-tales* in future data concerning flight bookings, financial transactions or border crossings.

Such algorithms can also be programmed to identify patterns between entities in the data themselves, which is known as *machine learning*. As the vast amounts of network data concerning persons, goods, money, vehicles, locations, and events are becoming more and more complex over time, machine learning will inevitably become a standardized method in criminal network research and law enforcement practice. Phua et al. (2004), for instance, already demonstrate how such techniques of machine learning can identify fraud schemes and -networks in multiplex data.

### 1.4 THE RELEVANCE AND AIM OF THIS THESIS

Based on the observations described in this introductory chapter, we can conclude that there is a gap between the theoretical perspectives and the empirical understanding of criminal network dynamics. Unraveling the complexity hidden within criminal networks is the key to effective detection and potential disruption and therefore very relevant to law enforcement control of organized crime. The data-driven methods available to uncover this complexity and dynamics are promising, but still in its infancy. Therefore, its added value to the understanding of criminal networks needs further evaluation and exploration.

This thesis explores the possibilities and limitations of this data-driven approach to the study of organized crime. The **aim of this thesis** is to contribute to a further empirical data-driven understanding of the structure and dynamics of criminal networks, in order to detect and disrupt them more effectively.
REFERENCES


Anderson, P. (1972) The whole is more and also different from the sum of parts, Science 177, 4047, 1972.


Chapter 1: Introduction


UNODC (2011). Research report: estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, Vienna


