Detecting and disrupting criminal networks

A data driven approach

Duijn, P.A.C.

Citation for published version (APA):
Chapter 8
Discussion
This thesis explores the possibilities and limitations of a data-driven approach to study criminal networks. The aim of this thesis is to create an empirical understanding of the complexity of criminal networks in order to detect and disrupt them more effectively. As this is relevant for the scientific world as well as for law enforcement practice, an additional purpose of this thesis is to bridge the gap between these two worlds. To investigate possibilities to bridge this gap chapter 2 and 3 first assess the use of a data-driven approach in understanding criminal networks (i.e. social network analysis) for law enforcement and compares this with existing applications in science. Following up on lessons learned in chapter 2 and 3, chapter 4 introduces the combination of SNA and computer simulations, and aims to identify elements typical for complex resilience found in criminal networks, i.e. processes of self-organization, emergence and non-linearity. Chapters 4-6 aimed to refine this approach and the understanding of complex criminal networks by introducing and exploring other data-driven methods for inference and analysis. Finally, chapter 7 reviews the studies in this thesis by contextualizing the main findings and identification of, limitations, and results in recommendations for future approaches in the study of criminal networks (chapter 7).

8.1 MAIN FINDINGS

The first study (chapter 2) explored the opportunities and limitations of social network analysis (SNA) for unraveling criminal networks. SNA was applied to a local criminal micro-network (N=86) involved in transnational drug trafficking (i.e. cannabis). In line with previous empirical research (e.g. Kleemans and Van de Bunt, 1999; Klerks, 2001; Bouchard and Morselli, 2014), our findings show that the criminal network gravitates and evolves around strong embedded social structures (i.e. affective- and family relationships). Our findings demonstrate how SNA contributes to understanding the emergence of transnational criminal networks emerging from of these local social network structures, emphasizing social ties and affective relationships in regard to resilience against disruption. We also addressed the problem of fuzzy boundaries in relation to the use of wiretap data and its negative effect on the validity of quantitative SNA metrics was assessed, in line with Campana and Varese (2012), Berlusconi (2013) and Campana (2016). It was concluded that quantitative SNA on micro networks (<100 actors) is useful for identifying relevant hidden elements (nodes and ties) in the periphery of the network, in addition to the qualitative in-depth analysis elements to explain the nature and relevance of such elements.

The second study (chapter 3) examines more extensively the methodology of SNA and its application in law enforcement, specifically in investigations. For this purpose, 34 SNA case studies were collected and compared from The Netherlands Police in a structural meta-analysis framework. Our findings resulted in the identification of several specific best
practices for the application of SNA. We show that SNA is of additive value to traditional analysis techniques in investigations concerning organized crime, youth gangs, corruption rings and cold cases. These empirical findings resulted in the following conclusions on the usefulness of SNA to detect and disrupt criminal networks:

1. Manual qualitative analysis of the increasing quantity of network data has its limitations in uncovering the characteristics of criminal networks at systems level, as it mainly relies on extrapolations of case studies to theorize about the overall structure of organized crime. SNA provides the opportunity to link patterns of individual properties to elements of criminal network topology, which is key to understanding its complexity.

2. The added value of SNA applied to micro-level criminal networks is limited. In small networks (N<30 actors) core membership and key players could be observed by traditional analysis techniques. In larger networks the outcomes of quantitative SNA should also be evaluated by the qualitative assessment of the content of relationships in order to reduce the effects of selection bias due to unilateral data availability. This is especially the case for wiretap and surveillance data, as was also previously emphasized by Campana and Varese (2013) and Berlusconi (2013).

3. Collecting and merging various relational data from different stages of the criminal justice chain should always form the basis for inference of criminal networks out of law enforcement data. This leads to a broad scope and high reliability of the final criminal network representation.

4. As previously emphasized by Sparrow (1991), Bruinsma and Bernasco (2008), Morselli and Petit (2007), and Malm and Bichler (2011) we also found that scripting is of additional value in the application of SNA. It adds a logistical dimension to network representations, which contributes to identification of role substitutability. This is particularly relevant for deliberate network disruption strategies. Empirically role data supports the interpretation of quantitative centrality measures (Campana, 2016) or understanding the multiplicity (complexity) of criminal connections (Bright et al, 2015). The collection and processing of role-specific data should therefore become an integral part of every intelligence collection procedure.

5. SNA applied in investigations should aim more at understanding the bigger picture at a meso- (inter-group) and macro (illegal market) level. The interaction of a criminal micro-network with the embedding meso-structures uncovers the driving forces behind its resilience. Such understanding is particularly relevant for the development of network disruption strategies.

6. A limitation of SNA is that it provides a static observation of dynamic phenomena on and of networks. Our findings emphasize that advanced methods in addition to SNA should be developed to capture social dynamics in order to understand the emergence and evolution of criminal networks. In line with Carley et al. (2007) and Bright et al. (2013) we recommended to combine SNA with computational simulation to capture such dynamics.
7. Embedded academics (*pracademics*) employed within law enforcement agencies are key brokers between science and investigations. Their access to empirical network data as well as their understanding of the academic language could bridge science and the operational law enforcement field, resulting in a deeper empirical understanding of criminal networks.

These seven conclusions formed the starting point for the design of *the third study* (Chapter 4), aimed to understand the dynamics of a criminal meso-network in response to different disruption strategies. Our findings -based on the combination of SNA and computer simulations- revealed that deliberately targeting vulnerable positions in a large meso-network (N=22,000 nodes) increases its overall efficiency instead of reducing it. It was observed that this is the result of a complex interaction between manifest criminal networks and their embedded social environment. Social ties of trust facilitate effective replacement. However, it was also found that the increased efficiency results in exposure of the network from ‘the dark’, leaving it vulnerable for subsequent law enforcement detection and targeting of its key players. Our findings emphasize that timing and strategic alignment of detection and persistent disruption efforts lead to more effective disruption strategies of criminal networks in the long run. Strategic thinking about how to structurally monitor criminal networks over time (i.e. strategic thinking in intelligence) therefore lies at the heart of effective criminal network disruption. This makes it possible to estimate the threshold where one disruption strategy becomes more effective in fragmentizing the network over the other (see Bright, Greenhill and Levenkova, 2011).

To support of these findings *the fourth study* (Chapter 5) presents a method to infer dark networks (i.e. population of drug-users) on the basis of scraping online social media networks, i.e. ‘Livejournal’ (N = 23 \(10^6\)). Criminals in the 21st century are not bounded to the physical world, but manifest themselves in the virtual world as well. This often requires big data methods to detect crime networks in online forums and social media. Our findings show that careful assessment of ‘slang’ terminology on drug-abuse as input for context sensitive text mining can be very effective for inference and profiling dark communities from online forums. It was also found that the content of communications can be mined to categorize its members into three different risk-groups for additional prioritization in targeted response. Similar techniques have recently been applied to infer networks from hacking forums (Décary-Hétu et al., 2014), online child pornography networks (Westerlake et al. 2012), and jihadist recruitment forums (Bouchard et al., 2014). Although new insights into these virtual dark networks are created, these studies also emphasize the sensitivity of such methods to the selection of key words used for crawling the online content. False negatives or -positives are the result of too specific or too broad combinations of keywords.
An in-depth study of specific ‘slang’ and keyword combinations used in target networks should therefore precede the scraping process to achieve reliable network representations.

At the end of the fourth study we aimed to contribute to thought ahead multiplexity and the identification of key players. The qualitative scripting approach introduced by Bruinsma and Bernasco (2008) and Morselli and Roy (2009) has proven to be very useful in criminal networks consisting of less than 75 actors. The quantitative scripting approach is however particularly relevant for the analysis of large complex criminal networks (N>75) inclosing many different criminal value chains at the same time. We therefore introduced three different notions for centrality by adding the value-chain dimension to binary network representations. This procedure however requires that intelligence is not only restricted to structural collection and procession of data on criminals and their social relations, but also on information on the individual roles they play in the criminal value chain (logistics) such as coordinator, producer of illicit drugs or supplier of precursors for drugs production.

The fifth study (Chapter 6) examines the strength of ties in organized crime. We investigated and compared three dimensions of tie-strength: structural, temporal and demographical. Our results show that weak ties are important for exchange of information to secluded communities, but not exclusively. Due to a small-world phenomenon there are many alternative pathways for information to flow between its remote parts. Moreover, most weak ties are too temporary and opportunistic to fulfill bridge positions. Furthermore, a categorization of criminal ties - based on intensity and duration- was introduced, which contributes to the identification of general structures of consistency and fluidity within the total network. This categorization might also contribute to a more deliberate approach in detecting criminal networks through human intelligence- or infiltration strategies.

Finally, in the sixth study (chapter 7) the implications of our findings for the future of criminal network research and law enforcement disruption strategies are discussed. The main conclusion from this chapter is that there are still some knowledge gaps in the controllability of complex networks. The controller must have at least as much complexity as the controlled in order to succeed. In practice the organizations tasked with detecting and disrupting such networks are just exploring more fluid ways of co-operation outside of the bureaucratic boundaries, which limits their own variety (complexity).

8.2 GENERAL CONCLUSION

Traditionally research on criminal organizations evolves around qualitative (narrative) studies of three separate organizational levels (i.e. micro-meso-macro). The complexity
of dynamically changing criminal organizations however requires new scientific quantitative methods that integrate the complex patterns connecting these three levels within one empirical framework. Social network analysis (SNA) has been proposed as such a method. SNA also received much critique, since its application is in most cases restricted to investigation of isolated and artificially bounded networks based on individual cases without taking into account the embedding networks structures mainly due to limited data availability. However, the exponentially growing amount of criminal- and social data routinely collected by law enforcement agencies is gradually becoming accessible for scientific research, enabling the inclusion of embedded network structures. At the same time, embedded police academics are introducing empirically derived data-analysis techniques within law enforcement practice. In this thesis we have contributed to this development by introducing new methods to integrate these different data levels, to infer networks, and to make valid and relevant selections of data in support of a data-driven approach. Based on our findings we can conclude that criminal network structures (micro-, meso- and macro) cannot be presumed but emerge. Quantitative analyses of these emerging networks can drive qualitative interpretations and assessment in order to seek rather than assume structure. As such we can consider this to be a paradigm shift in law enforcement practice as well as in organized crime research.

8.3 PRACTICAL IMPLICATIONS OF THE FINDINGS

The studies presented in this thesis demonstrate the flexible and adaptive nature of criminal networks under continuously changing environment. This flexibility and adaptability through levels of self-organization makes them highly effective and efficient in achieving their aim: maximizing profit and escaping from government repression. In contrast, laws and regulations constrain law enforcement agencies to operate in an equally flexible manner. Opportunities for improvement therefore lies in building strategies for detecting and disrupting criminal networks at an early stage. This requires not only a shift in approach, but also a shift in culture.

Law enforcement officers are generally selected and trained for resolute action in case of unexpected emergencies (Rathcliff, 2008; Vis, 2013). Although this reflex is essential for day-to-day police work on the streets, it has become a general characteristic of police culture. As a result the same action-reflex becomes dominant in other law enforcement disciplines as well, such as intelligence work and criminal investigations (Vis, 2013). In general, this leads to reactive rather than proactive operations, for instance with regards to detecting and disrupting criminal networks which is best described as \textit{ad hoc}, predictable, and therefore most likely ineffective. The findings in this thesis however emphasize that detecting and disrupting
Strategic thinking in the detection and disruption of criminal networks can be divided into two phases: the detection phase (i.e. intelligence) and the disruption phase (i.e. intervention). Before strategically deciding about the most effective approach about how to target a criminal network (detection phase) it is required to first answer the questions of what, who and where to target (disruption phase). This requires strategic thinking as well: where and how do I get information? How do I combine this information? What information is missing? How do I make sense of this information in supporting the operational objective? And how do I maintain an up-to-date information position? To answer these questions, law enforcement organization should invest more in developing strategies for detecting criminal networks before disrupting them.

**Strategies for detecting criminal networks**

The development of every intelligence strategy starts with the identification of the main elements out of which a problem consists and their mutual connections. In intelligence practice such elements are fitted into a conceptual model or framework (McDowell, 2008). The conceptual model helps to direct the intelligence collection process. The empirical findings presented in this thesis have contributed to the creation of a generic conceptual model for criminal networks, which is currently used in The Dutch Police to manage the collection and analysis of intelligence (Figure 1). This model consists of three main elements:

1. **Networks**: Who is involved with who? What is the strength, the criminal nature, and the social context of these relationships? What are the specific attributes of the actors in the network?

2. **Logistics**: In what criminal activities is the network involved? How does this process unfold in a value chain (i.e. crime script)? What roles do the actors play in this value chain? How does money flow through the network and how is it laundered?

3. **Infrastructures**: Where does the network commit these criminal activities? In what places do the actors meet and find new accomplishes? On what legal entities does the network rely in executing the crime script? What is the nature of these places and in what way are they connected?

Continuous intelligence collection on these three elements answers the questions of ‘who’, ‘what’ and ‘where’ allows for a look under the hood of the criminal network. The ‘who’ question creates insight in the social dimension behind criminal cooperation. The ‘what’ question creates insight in how the different actors work together in the criminal logistical process (e.g. drugs trafficking, money laundering, migrant smuggling). The ‘where’ question provides insight into the geographical or virtual environment, out of which the
criminal network emerges and evolves over time. At the points where these three dimensions converge, vulnerabilities (i.e. ‘hard-replaceable actors’, hotspots, and convergence settings) within the criminal network’s foundation are revealed (see Figure 8.1). 51

Figure 8.1 Conceptual model for the structural detection of criminal networks based on the continuous monitoring and analysis of the 3 main dimensions enabling organized crime. Convergence between these dimensions reveals key actors (facilitators), hotspots, and convergence settings on which the network relies for its logistics and human resources.

Structural intelligence collection and processing guided by these questions lead to the necessary data-driven understanding about the direction in which the network of offenders moves in space and time. Anticipating to this direction is key to assess the potential outcome of disruption strategies and provides input for proper preparation and planning of operational actions. Identifying key actors and key locations allows for expansion of the contemporary preventive and repressive strategies, which makes disruption less predictable. This unpredictability outbalances the efficiency-security tradeoff on which the resilience within criminal networks is built.

Such an approach requires a proactive intelligence collection process from a variety of sources in a structured way and over long periods of time, followed by the unification, data cleaning, merging and finally, imported in a data warehouse. This requires computational power and specific software. ICT support and management are an inherent part in the development of

51 This analytical framework (nowadays known as the ‘Hyperion-method’) was developed in close cooperation with other strategic intelligence analysts (i.e. Dr. Thijs Vis) employed within the Dutch Police. The author is particularly thankful for this collaboration. The research in this manuscript provided essential building blocks for the development of this framework.
this process. Current criminal intelligence practice relies mostly on a top-down approach for classifying criminal groups, which is frequently driven by a set of general criteria and indicators. In this manuscript it was shown however, that microscopic self-organization within complex networks can lead to unpredictable macroscopic outcomes. A top-down approach is therefore at risk of creating an assumed- instead of an empirical criminal reality. A bottom up approach is therefore essential in identifying the unexpected macroscopic patterns from the behaviors of its individual parts. In support of such a bottom-up analysis, a data warehouse can be created that allows for smart selections of data. This enables analysts to study the three dimensions of the criminal network in conjunction or in isolation.

Another contemporary tendency related to the increasing importance of ICT for intelligence professionalization, is the idea that computers will take over all of the criminal analysis work. Data science is seen as the new solution to the growing problem of how to create meaningful understanding of the criminal reality out of the growing amounts of (unstructured) data within the police databases. It creates the expectation that numerous amounts of data will be fitted into models that directly inform the operational police officer on how, where and when to respond to prevent crime from happening. For common types of crime (e.g. vandalism, bicycle theft), such models have already proven to be useful and have resulted into a more effective and efficient law enforcement practice. To understand complex phenomena such as organized crime, in which models are generated from incomplete and unconfirmed data, operationally following up on computer models could be dangerous. As shown in this thesis, computer models assist the researcher in selecting appropriate sources of data, but it is always the contextual human knowledge that provides the correct interpretation of the outcomes. Therefore it is not suggested that data scientists should replace analysts or vice versa, instead the combination of both strengthens the intelligence profession towards a reliable and validated data-driven approach.

According to Sutherland (1947) every crime phenomenon must be approached in terms of its uniqueness and specific characteristics. Change and evolution of criminal behaviors are therefore best detected from raw data that is collected from sources close to the actual criminal environment. This approach has inspired criminologists to infiltrate prison communities or become a participant observer in situations where social relationships with key members of criminals networks are build (e.g. Zaitch, 2002). In a law enforcement context such methods are called human intelligence or HUMINT (i.e. information from human informants). HUMINT can be directed towards the blind spots in the overall intelligence position, which gives it an advantage as compared with other sources of law enforcement data primarily collected for other purposes (e.g. evidence, safety, patrols). HUMINT can be directed by recruitment of specific informants or by asking specific questions to reliable informants (see also Kenney, 2007).
The reliability of HUMINT is not without debate, since informants can be misleading or manipulative. Researchers unfamiliar with HUMINT do not always know that the reliability of HUMINT is a topic of criminal intelligence analysis in itself. For instance, the ‘one source is no source’ principle is applied to prevent the spread of misinformation after every conversation with an informant. Additional crosschecks with external data sources allow for further assessment of an informant’s reliability. Non-reliable informants are directly placed on blacklist to make sure they are not approached again. Non-law enforcement sources -such as financial information or data from open sources- are also used to verify the information provided by informants. This also adds new dimensions (e.g. financial flows between nodes) to the overall intelligence picture.

The chapters of this manuscript also show that criminal networks have no boundaries. Contrarily, there is a common tendency amongst law enforcement agencies to keep things small and break them up in manageable pieces for budget or operational reasons. In many countries the analysis of organized crime is characterized by artificial clustering into separately labeled organized crime groups, which remain static and unevaluated over time. The outcome of this oversimplification is that the complex overarching macroscopic patterns of the criminal network structures remain unexposed. Essential weak ties between the artificial criminal groups and elements of the specific social context are labeled as irrelevant and deleted from further analysis. As a result the potential outcomes of any disruption strategy become difficult to capture from ‘the bigger picture’ and the critical vulnerabilities of the criminal system remain hidden. In line with Spapens (2010) and Von Lampe (2014) we therefore emphasize that intelligence strategies should start off with the aim of achieving this bigger picture, even when disruption strategies continue to focus on the investigation and targeting of its individual parts. Understanding the functioning, structure and dynamics of criminal networks at a meso- and macro system level, is required to maximize the effect of different micro-interventions on the long term.

Nevertheless, detections- and disruption strategies should not be developed in isolation, but in a network of intelligence- and operational specialists working together in parallel as the operations unfold. Thinking in terms of complexity is essential in this sense: what could be the effects of a single arrest (micro-level) on the functioning of the overall criminal network (macro-level)? What does this require in terms of intelligence? And what opportunities does the operational strategy provide for collecting this intelligence? Operational action (e.g. wiretapping, surveillance, arrests, house searches) could also be applied as part of an intelligence strategy instead of disruption strategy in order to learn more about the organizational background and vulnerabilities of the network, before its disruption at a later stage.
Criminal opportunities that emerge from the fast expanding cyber environment (i.e. *darknet marketplaces*) shorten the social distance within global criminal markets and may lead to recruitment of ICT specialists which provide ‘crime-as-a-service’. Law enforcement agencies should therefore proactively respond to such developments by recruiting similar ICT expertise to monitor virtual illicit activities at an early stage. Additionally, international cooperation and data sharing –especially on a tactical level- is key to such a planning process. This is not an easy endeavor since trust is more easily built along strong- instead of weak ties, equivalent to criminal networks. Organizations such as Europol and Interpol facilitate such trustful cooperation by creating platforms for effective intelligence sharing. In order to detect criminal network activities across borders, such services should be utilized more often when the opportunity arises.

**Strategies for disrupting criminal networks**

Strategic thinking in the disruption phase requires thinking in scenarios: assessing each strategy’s potential success influenced by the specific momentum and circumstances. Networks can be disrupted *structurally*, by removing nodes and/or links. Another strategy is to disrupt them *functionally*, by cutting of the networks access to operational requirements, such as cutting of the flow of money to finance terrorist activities or by frustrating the supply chain for precursors for the illegal production of narcotics (Strang, 2014). The different studies presented in this thesis demonstrate how network analysis helps to develop scenarios in which both approaches are combined.

Understanding of the network’s topology (i.e. scale free, small world, random) provides essential input for strategic thinking about *structural* disruption. Hub-attacks are most effective in disrupting criminal networks with topological scale-free features (Albert and Barabasi, 2000). Bridge-attacks (nodes with high betweenness) are most effective for networks with small world features. Role-attacks are the most effective strategy for networks that constitute various connected value chains. Functionally frustrating the value chain of a criminal process by taking into account node-substitutability proved to be most effective in breaking small world networks as well. In this case the disruption strategy is aimed at frustrating value chain network topology instead of the topology of the overall network. Disruption strategies could therefore be aimed at frustrating the overall macroscopic network or specific dimensions or sub-communities. This decision depends on the desired effect and objective of the strategy.

Finding ways to outbalance the networks trade-off between efficiency and security fuel such structural disruption strategies. For this it is important to seek for *‘the point of gravity’* in a criminal network (Von Clausewitz, 1873). In dark networks this involves for example codes of silence, reputation, family relationships, profit sharing, loyalty to neighborhood
communities, radical ideologies, or a charismatic leader (Strang, 2014). By targeting such points of gravity the network’s social foundation of trust becomes disrupted, potentially leading to a tipping point in its structure’s cohesiveness that eventually enables it’s collapse (see case example 1 and 2).

**Case example 1: in the name of ‘love’**
In chapter 2 we identified that the center of gravity of the Blackbird network consisted of the role of females, love- and family relationships. In the end it turned out that the females were the glue that kept the individual parts together. Ironically, it were also the females who -out of jealousy and self protection- provided detailed statements to the investigators, which finally made the network fall apart. It was however not the subsequent sentence and imprisonment of the main male suspects which made the network collapse, but the lack of trust amongst the members of the network as a result of these incriminating statements. The love relationships turned out to be as fluid as the networks out of which they emerged. The investigators may not have even realized that their most effective intervention was in fact taking these statements within their investigative routine. It broke the trust underlying the social ties, causing a ‘tipping point’ within the dynamics on the criminal networks and ushering its collapse.

**Case example 2: breaking Bald Fred’s reputation**
A regional police unit was confronted with an increasing illicit cannabis cultivation industry in dense urban areas, including violent rages of cannabis cultivation sites and serious risks for fire safety. Efforts to stop this development consisted of clearing as many cannabis cultivation sites as possible without investigating the criminal networks that were responsible for building these sites. Twice as much sites were built as could be cleared, making it a lucrative business despite the law enforcement efforts. Partly inspired by the findings presented in this thesis, a regional intelligence unit decided to use scripting in combination with SNA to identify the actors responsible for building the cannabis cultivation site. It turned out that just a few of them held a strong reputation for installing the electricity supply without the risk of detection by energy companies. One of them was nicknamed ‘Bald Fred’. He provided his services to at least six criminal groups. An investigation led to his arrest and recovery of his criminal assets. Intercepted wiretap data revealed that the various criminal groups relying on his expertise started to doubt his reputation after his arrest, but were struggling in finding a trustworthy replacement for building new plantations. Breaking Bald Fred’s reputation appeared to have more effect than clearing many cultivation sites.

In some instances, locations can also be identified as points of gravity. Networks of freelance career criminals who provide ‘crime-as-a-service’ often get engaged in short-term opportunistic criminal alliances. In most of these cases the independent actors gravitate around a certain point in physical or virtual space, which function as hubs out of which new instant alliances emerge (e.g. club-houses, cafés, restaurants, brothels, sport clubs, chat rooms, online marketplaces). Targeting locations (or legal entities representing these locations) could then be a more effective strategy (Felson, 2006). Administrative measures have already been developed to close down cafés, restaurants, brothels and casinos, if there is an legal indication that such properties are owned by members of
organized crime or facilitate their illicit activities (Fijnaut et al., 1996, Kleemans, 2007). Network analysis, which includes links between persons and locations or legal entities could facilitate such an approach, by identifying the main meeting points or vulnerable locations within the criminal logistical process (See case example 3). More empirical research is needed to understand the connection between criminal networks and the physical- and virtual infrastructure in which they operate.

Within law enforcement practice interventions are mostly aimed at the nodes (i.e. persons, locations), while the links are in fact the most essential building blocks for network formation. Link attacks can be aimed at disrupting the networks communications, for instance by taking down encrypted telecom circuits popular in criminal networks. Another approach is changing the nature of relationships. This can be achieved by manipulating the underlying mechanisms of trust and reputation. In this context we emphasized in chapter 6 that criminal networks may also be influenced from the outside by actively targeting the fluid and weak latent ties, which form the bridges from the outside to its inner dense core. This could for instance be an effective strategy through infiltration of networks in cyberspace or networks that operate on online internet, such as cybercriminals or jihadist recruitment networks. Such a strategy could however have severe ethically unjustifiable consequences, such as a wave of violence. Distrust within the Amsterdam organized crime scene following one stolen shipment of cocaine in the port of Antwerp has for instance contributed to a sequence of assassinations within the Amsterdam underworld. This unfolded in a non-linear way, which often puts innocent civilian bystander’s life at risk.

Strategic thinking in operations aimed at criminal networks should therefore always start with creating a ‘script’ containing what-if scenarios for every separate intervention. Such a script reveals how the potential outcomes of separate interventions could reinforce or contradict each other’s outcome. Evaluation of such outcomes could be mapped and then aligned in chronological order to achieve the maximum synergy. Computer simula-

---

**Case example 3: disruption infrastructures**

Dutch project Emergo was aimed at disrupting the increased economic power and influence of organized crime networks within the Amsterdam Red Light district. Instead of targeting the networks directly it was aimed at critical points of the criminal infrastructure following an administrative approach. An experiment with data-mining and network analysis contributed to a targeted application of administrative measures (Spapens, 2013). The project proved to be successful. Neighborhoods, which were controlled by organized crime, have now become popular touristic hotspots. This project also revealed that legislation for combining confidential data from separate sources (e.g. police, tax-services, local government) is still undeveloped and rather opaque to fully exploit these fast-growing technological opportunities for a data-driven approach.
tion through predictive modeling supports in assessing the interdependent outcomes of multiple strategies, especially when the range of what-if scenarios becomes too complex.

In Dutch criminal justice practice financial investigations generally start after the criminal investigation has been completed. In some scenarios it is however more effective to turn this around. Suspicious bank accounts of key criminal network members could for instance be ‘freezed’ on ground of suspected money laundering, prior to an actual investigation or arrest. A criminal network’s financial means for doing business may then dry out. As a result, the network becomes outbalanced and in an attempt to set things straight financial facilitators supporting the network in the background may become exposed (e.g. corrupt notaries). Such corrupt and reliable facilitators are not easy to find in criminal circles and are therefore harder to replace, providing opportunities to disrupt the financial flows further through specifically by targeting these facilitators in succession. Strategic thinking in terms of networks and scenarios therefore requires re-evaluation of the contemporary in which interventions and tactics are applied (see case example 4).

Measuring the efficacy of these various disruption approaches remains a challenge within law enforcement practice. Although indicators (i.e. number of seizures, number of arrests, number of assassinations) for assessing the outcome of certain interventions have been developed, measuring the exact effect on criminal network structure remains difficult to determine. Validation of the effectiveness of certain strategies often follows from feedback from the criminal environment itself, for instance via deliberate HUMINT collection (see case example 4). Generally, criminal networks tend to become more dispersed after deliberate attacks, such as the example of Darknet marketplaces described chapter 7 (p. 188). Such complex systems may shift from order to chaos, showing increased levels of self-organization, and changes in their general network topology as a result of external

---

**Case example 4: drying out the expertise**

Inspired by the outcome of the research in chapter 4, a police unit in one of the larger Dutch cities experimented with functionally targeting a sequence of criminal production specialists providing their synthetic drug production expertise to a large criminal network involved in the trade of synthetic drugs. The aim was to structurally break the value chain based on role substitutability. A deliberate intelligence strategy based on SNA and scripting led to the identification of four ‘chemists’ interchangeable in the value chain. Three of them were effectively targeted. Several informants from within these criminal networks informed the police, independently from each other, that replacements were drying out as a result of the interventions. As a consequence the network needed to recruit specialists with poor reputations to keep the production going and customers satisfied. This resulted in major delays of the synthetic drugs production, and disruption of the network. As a side effect, separated parts of this criminal network replaced their criminal activities to a different drugs market, demonstrating competitive adaptation on a higher level.
pressures or interventions, which increases their overall complexity and makes them more unpredictable and harder to detect afterwards. As a result, criminal informants may lose their perspective on the networks activities or become demotivated as a result of disruption strategies that also affect their personal lives. This makes it difficult to monitor the effects and validate the simulations of specific network disruption strategies over longer periods of time.

The chapters in this manuscript focused on the disruption of criminal networks that already emerged. The best approach however would be a strategy that prevents them emerging or becoming too complex to control in the first place. This means that interventions should particularly aim for local pools of youth gangs, which provide breeding grounds and essential career paths to organized crime (Moffit, 1993, Loeber and Farrington, 1998). The social trust which is created in these networks forms the basis of future criminal cooperation at a transnational level (see case example 5).

**Case example 5: towards a ‘white’ Christmas**

In a middle-sized city in the Netherlands it was a famous tradition at the end of the year to build a big fire from Christmas trees. Because the neighborhoods with the biggest fires would receive the most respect, it led to rivalry between different neighborhoods. Youth would come together and steal the Christmas trees from other neighborhoods, leading to violent encounters. One of these youth groups from a less developed neighborhood, build a particularly infamous reputation due to their excessive use of violence. Since the police reacted with equal levels of violence and arrests, the members clustered more and more together and soon developed into a youth gang responsible for multiple crimes across the city. The mutual trust the members built within their younger years turned out to form the basis for later criminal cooperation at a transnational level. Almost twenty years later some of the members were identified as the primary suspects for running an international cocaine trafficking ring from South-America to Europe. How would this criminal network evolved if repression would have been traded for prevention and aimed at building ties of trust with the government and the local community?

Convergence between youth gangs and organized crime networks is sometimes facilitated through family ties, in which the reputation of the oldest brother in transnational drug trafficking provides the youngest brother with the status and mentorship to take in powerful positions in a local youth gang (Morselli et al, 2006). Prisons may also provide unwillingly opportunities for networking and learning criminal behaviors and modus operandi. Convergence between members of youth gangs and well-established members of organized crime networks may become enabled in this way. The latter is however receiving increased competition from Jihadist prison communities, who master the art of grooming and providing lost youth gang members with offering them an alternative path in life. This is where the necessary application of violence, contra-strategies and building criminal alliances are learned, in order to become respected members of organized crime networks. If the government therefore fails to become part of these networking processes and provide
a reasonable alternative to these young offenders today, a whole generation of young offenders may become the organized crime- or terrorist leaders of tomorrow.

In this regard, a balance between prevention and repression remains important, especially in the case of late-onset offending in organized crime, which is relatively recently discovered as a phenomenon in the career trajectories to organized crime (Kleemans and De Poot, 2008; Van Koppen et al., 2010). These studies show that the decisions made by people to become a member of organized crime networks is strongly influenced by complex social opportunity structures that occur randomly. Future membership to criminal networks is therefore not something that is prevented or controlled easily by law enforcement or policy measures.

Thinking in terms of complexity therefore teaches us that problems of local youth gangs, late-onset offenders, radicalized jihadist networks and transnational organized crime networks should be analyzed, prevented and disrupted in conjunction, which requires a holistic long-term strategy. With some exceptions, the leading management-style within contemporary Dutch law enforcement operations is known as the ‘firefighter-model’. Many ‘fires’ (e.g. terrorist threats, violent gang wars, cyber attacks) have to be extinguished at the same time, resulting in a very reactive instead of proactive approach to crime control. External pressures from the media, politics and the public influence the many shifts in priorities that direct intelligence- and law enforcement practice. It will therefore take courage and strong leadership to swim up against this stream, but it is the only effective route to follow in countering the growing threat that dark networks pose to the integrity, safety and democracy of our society.

8.4 FUTURE DIRECTIONS

Future research in the field of criminal networks should be aimed at three directions: the empirical, methodological, and practical direction. This thesis shows how our general understanding of complex systems provides a framework for creating an improved empirical understanding of criminal network dynamics. It has led to new strategies for detecting and disrupting criminal networks in law enforcement practice. There is however still little evidence on the side effects of node manipulation in complex networks (Quax et al., 2013). Future research should therefore be aimed at creating a universal understanding of the controllability of complex systems. This is not only relevant for findings ways to effectively control criminal networks, it could also prevent the collapse of ecological, biological, economical and social systems. In chapter 7 it was emphasized that controllability will only be achieved if the controller has at least as much variety (complexity) as the controlled
Understanding controllability remains therefore one of the most challenging research topics in complexity science. A recent study by Gao et al. (2016) aimed at finding universal resilience patterns in complex networks is an example of research focused on this direction. It shows that resilience depends on the interconnected dynamics on and off networks. Such a scientific understanding can have a direct impact on the ways we organize the control of criminal networks as well.

The combination of computer stimulation and network analysis could in particular be of additional value in the criminological research field where it can enhance the empirical understanding of the dynamics of on and off criminal networks. Studies based on SNA are mostly based on descriptive analysis (Scott and Carrington, 2011; Papachristos, 2011; Campana, 2016). Some scholars therefore stimulate the development of a ‘networked criminology’, which involves the utilization of SNA in criminological research (Papachristos, 2011; 2014). Network concepts such as social bonding, diffusion, peer influence, control, and cohesion are already part of the dominant theories of crime. Future SNA based research that is more etiological in nature could bring theory-driven and data-driven research closer together. Integration of SNA with statistical significance tests such as Quadratic Assignment Procedure (QAP) regression models have for instance already been applied to overcome the problems of non-independence of observations in criminal network data and have led to new empirical insights of underlying causes of crime (Dekker et al. 2007; Campana, 2016).

Methodologically, future research should focus on the development of (=dubbel op) methodologies and metrics to study complex criminal networks. Methodological research should for example aim to improve methodologies of criminal network inference. Missing data remains a central issue of technical criminal network research. The development of link prediction models based on network topology is already an important step in the right direction (See Berlusconi et al., 2016). Similar link prediction models are developed in the field of terrorist network research (Chen et al., 2011). Also methods of machine learning based on complex agent-based models could benefit from this type of development, specifically to simulate the emergence of macroscopic dark networks and learn about mechanisms of criminal and terrorist network formation (Mei et al, 2015).

Whilst struggling with similar methodological issues of missing data, it appears that terrorist- and criminal networks are mainly studied separately, and as a result the development of different fields of research. Methodological improvement could be reinforced by integrating terrorist- and criminal network research. This could for instance result in increased knowledge of the synergy between organized crime and terrorism. Especially since this
xxx appears to be an essential part of the facilitation of terrorists plotting attacks, and the pursuit for political power by members of criminal networks (Makarenko, 2004).

A second line of methodological research should aim for further improvement of metrics for analyzing complex network data. As criminal network data is expected to grow and improve in quality, the need for additional metrics that identify critical nodes or ties based on multiple network dimensions (e.g. links or node attributes) will increase. Chapter 6 presented an alternative metric for the identification of key players based on value chain positioning as opposed to the standard metrics of centrality. Also within large network representations (e.g. scraped from online data), community detection algorithms are becoming increasingly important and particularly in criminal network research. Future research should aim to further refine such models. Newman and Girvan’s algorithm for identifying community structures in complex networks is for instance already regularly applied within the law enforcement environment to identify sub-communities in macroscopic criminal networks (Newman and Girvan, 2004).

Practically, there is a strong need for research aimed at the empirically evaluating of different detection and disruption strategies in terms of impact and effectiveness. This requires effective monitoring of criminal networks over time, which is a challenge as network composition and topology may change after intervention. A direction of future research could be aimed at building robust intelligence positions -preferably based on human intelligence- which remain intact even after single elements of the overall network become disrupted. Models for identifying optimal observers in dark networks could assist human intelligence units by recruiting informants with overlapping views on network activities. Besides the practical challenges, such insight could support the development of more robust and long-term intelligence positions needed to detect adaptation and evolution over time. The generated data is particularly relevant for the validation and fine-tuning of the disruption models through simulation. Additionally, the practical law enforcement field could benefit from studies that compare the current network structure and dynamics of law enforcement agencies and compare that with the structure and dynamics of the criminal networks they try to control. This might lead to a more empirical basis for strategic development of optimal law enforcement organization and management in the task of disruption and detection criminal networks.

Although these recommendations for future research could bring us closer to understanding the dynamics and evolution of criminal networks on a macroscopic level, the microscopic interactions between individual propositions will remain unpredictable in nature. Law enforcement agencies and criminal networks are therefore caught in an intricate web of complex adaptively. Preventing criminal networks from adapting and growing towards a
state-in-a-state through corruption, violence, and infiltration of the legal economy, is however one of the main parts of the legitimacy of law enforcement organizations. Improving and adjusting the methods to detect and disrupt criminal networks will therefore always remain an essential part of that endeavor.
REFERENCES


