Detecting and disrupting criminal networks

A data driven approach

Duijn, P.A.C.

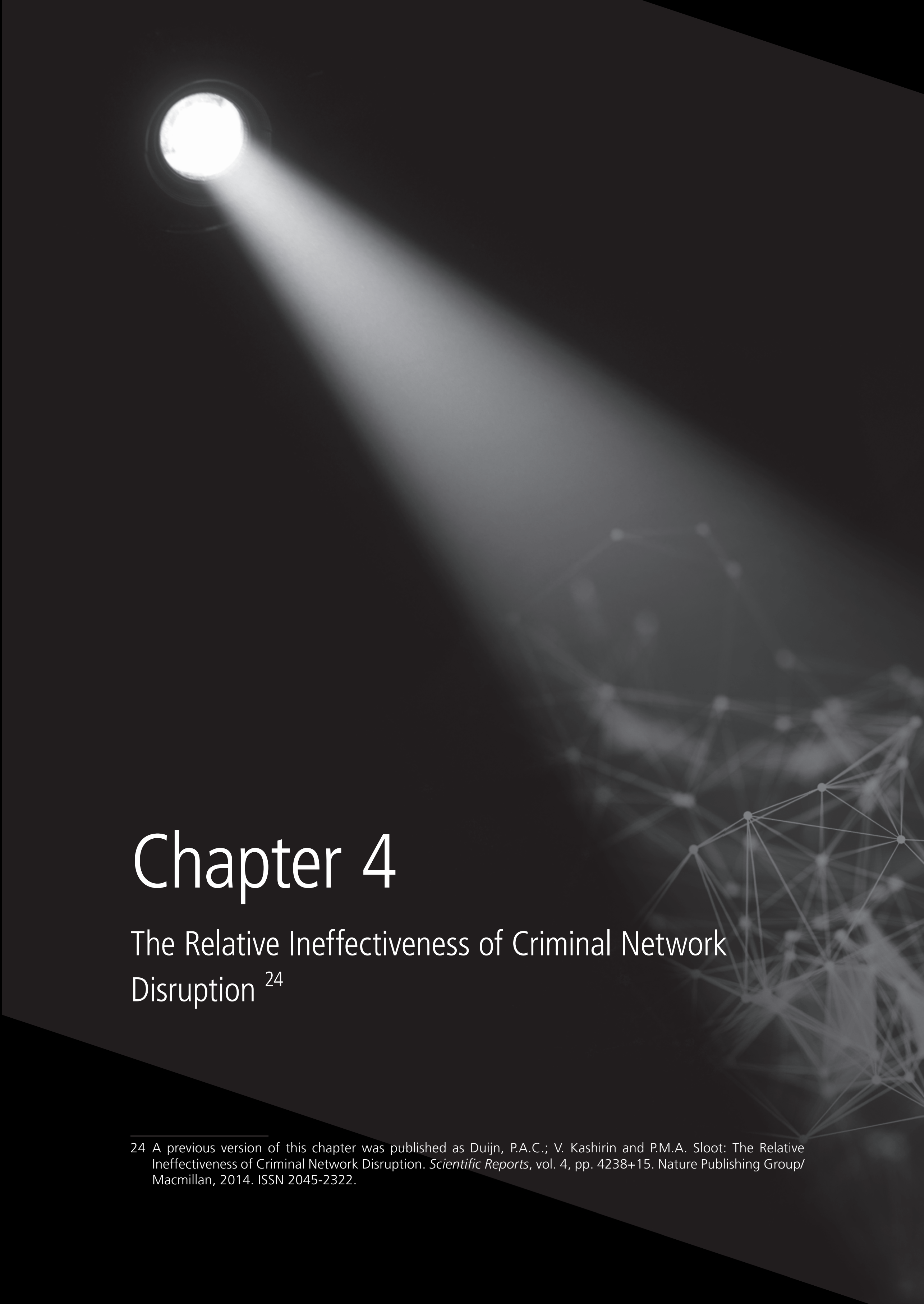
Publication date
2016

Document Version
Other version

License
Other

Link to publication

Citation for published version (APA):
Duijn, P. A. C. (2016). *Detecting and disrupting criminal networks: A data driven approach*. [Thesis, fully internal, Universiteit van Amsterdam].



Chapter 4

The Relative Ineffectiveness of Criminal Network Disruption [24]

[24] A previous version of this chapter was published as Duijn, P.A.C.; V. Kashirin and P.M.A. Sloot: The Relative Ineffectiveness of Criminal Network Disruption. *Scientific Reports*, vol. 4, pp. 4238+15. Nature Publishing Group/ Macmillan, 2014. ISSN 2045-2322.

ABSTRACT

Objective: Researchers, policymakers and law enforcement agencies across the globe struggle to find effective strategies to control criminal networks. The effectiveness of disruption strategies is known to depend on both network topology and network resilience. However, as these criminal networks operate in secrecy, data-driven knowledge concerning the effectiveness of different criminal network disruption strategies is very limited. The first objective is to unravel the dynamics of the interaction between disruption and resilience within criminal networks. The second objective is to find the most effective criminal network disruption strategy according to this model, by simulating the effects of different network disruption strategies on network topology.

Methods: We combine methods of computational modeling and social network analysis to simulate the behavior of a criminal network involved in organized cannabis cultivation based on intelligence data from the Dutch Police.

Network data: N=22.000 Nodes

Results and Conclusions: By combining computational modeling and social network analysis with unique criminal network intelligence data from the Dutch Police, we discovered, in contrast to common belief, that criminal networks might even become 'stronger', after targeted attacks. On the other hand increased efficiency within criminal networks decreases its internal security, thus offering opportunities for law enforcement agencies to target these networks more deliberately. Our results emphasize the importance of criminal network interventions at an early stage, before the network gets a chance to (re-)organize to maximum resilience. In the end disruption strategies force criminal networks to become more exposed, which causes successful network disruption to become a long-term effort.

4.1 INTRODUCTION

Organized crime forms a great threat to societies across the globe. International criminal drugs organizations try to infiltrate legal businesses and governments, infecting economic branches with corruption and violence. Moreover, upcoming threats like cybercrime, child porn, maritime piracy, match fixing and identity theft cause substantial harm and ask for proactive interventions to control the criminal organizations behind them (Europol, 2011; UNODC, 2010). Government and law enforcement agencies worldwide seek ways to disrupt these criminal organizations effectively, preferably at an early stage. Over the past decade a growing number of studies emerged that provide empirical evidence of the use of social network analyses to get a better understanding of organized crime. These studies show that criminal organizations need to be considered as social networks that form collectives rather than organizations with unique features, such as flexible and non-hierarchical internal relations (Klerks, 2001; Krebs, 2001; Natarajan, 2006; Morselli, 2009; Spapens, 2010; Sparrow, 1991; UNODC, 2010; . This approach has serious implications for the way we think about law enforcement control of organized crime. It has long been assumed that targeting the 'kingpin' leader at the top of the pyramid structured mafia organization, would result in the collapse of the entire criminal organization (Klerks, 2001; Raab & Milward, 2003; Spapens, 2010). However, new insights from social network analyses emphasize that the fluidity and flexibility of the social structure of criminal networks makes them highly resilient against these traditional law enforcement strategies (Morselli, 2009) For instance, it was found that even though a drug trafficking network was structurally targeted over a substantial period of time, the trafficking activities continued and its network structure adapted (Morselli & Petit, 2007). Research concerning the resilience of criminal networks involved in the production of ecstasy in the Netherlands lead to the same conclusions (Spapens, 2010). How can this be explained?

The complexity of criminal networks

An answer to this question can be found within the specific features of the associated 'dark' network structures and, more importantly, the conditions under which these exist (Erickson, 1991; Raab & Milward, 2003). Criminal network structures are known to be very complex systems. As Morselli describes it "*Criminal networks are not simply social networks operating in criminal contexts. The covert settings that surround them call for specific interactions and relational features within and beyond the network*" (Morselli, 2009). Criminal networks therefore differ from legal networks in that they face a constant trade-off between security and efficiency which directly affects its network structure (. On the one hand illegal activities need to stay concealed from the government or criminal competition. This means that direct communication between co-conspirators concerning illegal activities needs to be restricted to a minimum. On the other hand, risks have to be taken in times of action, often demanding highly efficient communication and trust among the participants (Erickson, 1981; Morselli et el., 2006)(12,14). Criminal networks therefore continuously balance between efficiency and security according to the given circumstances of the illegal activities.

This trade-off has a direct effect on its network structure as revealed by a study from Baker and Faulkner (1993)). They found that within a covert network, involved in a price-fixing scheme, the most important actors deliberately operated from the peripheries of the network, thus protecting these essential players from immediate detection after government intervention. In addition, Morselli et al. found that the balance between efficiency and security within covert networks was influenced by its network objective. They compared the structure of a criminal network with terrorist networks and showed that criminal networks need more efficiency in their direct lines of communication as compared to terrorist networks. Consequently, this made them less secure and more vulnerable to disruption (Morselli et al., 2006). This can be explained by the fact that economically driven criminal networks need shorter time frames between action (time-to-task) as opposed to ideologically driven terrorist networks. Terrorist networks might achieve their goals by just one successful terrorist attack. Criminal networks are often action oriented, resulting in higher levels of risk of becoming detected. In response, criminal networks try to remain flexible and agile. This flexibility gives them the ability to adapt quickly to external shocks (Raab & Milward, 2003; Kleemans & Van de Bunt, 1999) .

Although these studies help us to understand that remaining flexible is the key to criminal network resilience against disruption, little is known about how these flexible network structures actually recover from an attack and continue their illegal activities. In other words: What actually makes these flexible criminal network structures so difficult to disrupt? In search for an answer, we first need to understand that like every social network, criminal networks are not static, but dynamic in nature (Sparrow, 1991; Morselli, 2009). Criminal networks can change for several reasons: as a result of new business opportunities, as a consequence of competition that requires a defensive orientation or as a direct result of law enforcement controls that may lead to the downfall, stagnation or adaptation of the network (Morselli, 2009). The changing effects of network disruption can therefore only be understood within its dynamics; these networks are truly complex adaptive systems (Sloot et al., 2013). Many researchers of criminal networks agree that *"studying … the dynamics in criminal networks is probably the most challenging obstacle facing anyone approaching this area*." (Sparrow, 1991; Morselli, 2009) Although we recognize the complexity and difficulty that is associated with studying change within social networks, we attempt to capture these dynamics within a computational framework.

Research Aim

The aim of this study is twofold. The first aim is to unravel the dynamics of the interaction between disruption and resilience within criminal networks. Understanding these dynamics might have major implications for the way we think about control strategies aimed at organized crime. The second aim is to find the most effective criminal network disruption strategy according to this model, by simulating the effects of different network disruption strategies on network topology. We combine methods of computational modeling and social network analysis to simulate the behavior of a criminal network involved in organized cannabis cultivation based on intelligence data from the Dutch Police.

Organized cannabis cultivation as a criminal network problem

Organized cannabis cultivation is one of the growing problems concerning international organized crime throughout different continents (Bouchard, 2007b; Decorte, 2010; Malm et al., 2011; Potter, 2010). Recent studies show that cannabis cultivation is associated with the use of more sophisticated methods, from outdoor cannabis sites towards sophisticated indoor settings. A Dutch study based on a study of 19 closed police investigations reveals that cannabis cultivation is a hard crime, involving extreme violence and mutual rip-offs and is rapidly expanding internationally (Spapens et al., 2007). Different studies concerning cannabis cultivation reveal expanding co-operations between criminal networks from Belgium, the Netherlands, Germany and the UK (Spapens et al., 2007; Potter et al., 2011). Outside the EU these trends are also observed within Canada and the US (Malm et al., 2011). These trends of worldwide expansion and increased levels of sophistication and violence, indicates that cannabis cultivation involves professional criminal cooperation with many roles and functions.

Although different countries recognize organized cannabis cultivation as a serious problem, different studies show that law enforcement efforts do not seem to have reduced the problem (Decorte, 2010; Spapens et al., 2007; Wouters, 2008)). Current interventions show no significant effect on large-scale growers, although proximately 6000 cannabis cultivation sites are being dismantled annually. A first reason is that thorough investigations of the criminal networks behind large-scale cannabis cultivation are extremely time-consuming and costly (Wouters, 2008). Secondly law enforcement interventions in for instance The Netherlands aimed at cannabis cultivation can be described as a hit-and-run practice, busting a maximum number of sites with maximum efficiency without paying attention to the potential impact on the associated criminal networks (Decorte, 2010; Wouters, 2008). This seemingly lack of effective strategy within law enforcement interventions was also recognized for the UK situation (Potter, 2010). It was observed that law enforcement strategies focused on cannabis cultivation was largely reactive in nature, instead of proactively disrupting the responsible criminal networks. These studies all recognize the fact that law enforcement control strategies aimed at organized cannabis cultivation lack a focused direction and strategy.

These criminal network problems do not exclusively relate to the control of criminal networks involving organized cannabis cultivation, rather they are observed within the control of criminal networks at large (Klerks, 2001; Morselli, 2009; Spapens, 2011). Understanding how the observed cannabis cultivation network adapts to network disruption, might therefore contribute to a better understanding of the effectiveness of disruption strategies and network resilience. Before we discuss our research design in detail, we introduce the concepts of criminal network disruption and criminal network resilience.

The concept of criminal network disruption

According to previous studies, three indicators of network destabilization can be distinguished: a reduction in the rate of information flow in the network, a reduction in the ability to conduct its tasks or a failure or significant slowing down of the decision making process (Carley et al., 2002). Therefore network disruption can be defined in general as the state of a network that cannot efficiently diffuse information, goods and knowledge (Carley et al., 2003). Based on previous studies, strategies for criminal network disruption can be divided into two main approaches: The social capital approach and the human capital approach.

The social capital approach

The social capital approach aims at strategic positions that individual actors occupy within criminal networks (Sparrow, 1991; Klerks, 2001; Natarajan, 2006; Carley et al., 2002; Schwartz & Rouselle, 2009)). Like legal business, criminal networks depend to a large extent on social contacts and the ability to extract the necessary resources for their operations. The advantages that result from having social networks is called *social capital* (Coleman, 1990; Hulst, 2009). Research in this field is often based on social network analysis (SNA) to identify central actors in the network, that are associated with influential or powerful positions of social capital (Cook & Burt, 2001). There are many ways within SNA to measure network centrality, but the two most common centrality measures that relate to strategic positions are degree centrality and betweenness centrality (Sparrow, 1991; Klerks, 2001).

Degree centrality measures the number of direct contacts surrounding an actor (Wasserman & Faust, 1994). Because high scores on degree centrality as associated with better access to resources, these actors are associated with influential and powerful positions within social networks. Since they are important for the flow of information and resources throughout the network, these actors are called hubs. Hubs have major influence on overall network structure, networks that gravitate around a few hubs, for instance, are defined as 'scale-free' (centralized) networks. In social network terms these networks are characterized by a power-law degree distribution, which means that a small percentage of actors have a large number of links (Albert et al., 2000). In addition, it was found that scale-free networks are resistant against random attacks, because the majority of less connected nodes will more likely be targeted (Watts & Strogatz, 1998.). Moreover, the loss of peripheral nodes for networks with central hubs is less significant for its network survival. On the contrary, decentralized networks are mostly affected by random attacks because the loss of any single actor will be more important for the remainder of the network. Ironically, in the context of targeted attacks, network vulnerability inverses: central actors are more likely targeted, making centralized networks more vulnerable than decentralized networks. Knowledge of a network's structural features is therefore essential before the effects of any network intervention can be understood.

As opposed to degree centrality, betweenness-centrality incorporates the indirect contacts that surround an actor and is calculated by the number of times that an actor serves as a bridge (shortest paths) between other pairs of actors (Albert et al, 2000; Freeman, 1979)). Therefore betweenness centrality represents the ability of some actors to control the flow of connectivity (information, resources etc.) within the network. ((Burt et al., 1998; Burt, 2008))). Because these actors often bridge the '*structural holes*' between disconnected (sub)groups, these actors are called 'brokers'. Burt explained the importance of brokers for an increase of *social capital* within entrepreneurial networks. Entrepreneurs on either side of the brokerage position rely on the broker for indirect access to resources and information beyond their reach (Burt et al., 1998; Burt, 2008). There is empirical evidence that brokers play important roles in connecting criminal networks connecting separate criminal collectives within illegal markets (e.g. Boissevain, 1994; Coles, 2001; Morselli & Roy, 2009; Morselli, 2001; Klerks, 2000). By attacking these brokers, important non-redundant opportunities to expand an illegal business might decrease. This is especially relevant for decentralized networks, such as terrorist networks (Krebs, 2002). Based on these studies betweenness centrality attack is recognized as another important strategy for criminal network disruption. In line with these studies, both centrality strategies will be applied to the organized cannabis cultivation network within our models for network disruption (Section 6.3).

Although centrality strategies can be a very effective approach for disrupting centralized or decentralized networks in general, the application of this approach within criminal networks is not without discussion (Morselli, 2009). Peterson argues that the most central actors in covert networks might also be the most visible. Therefore, they might be the most likely to be detected. According to Peterson (1994) high degree centrality can therefore also be associated with vulnerability instead of strength). In addition, Carley, Lee and Krackhardt (2001) also demonstrate that the most central actor isn't necessarily the network member with the most leadership potential. For instance, they found that in networks where leadership and centrality are fulfilled by different actors, targeting the central node would not necessarily lead to a downfall of the network and that a targeted leader is not necessarily replaced by the most central actor (Carlet et al., 2002). Robins emphasizes that features of network topology also interact with individual-level factors. Therefore, qualities of individual actors (e.g. skills, expertise, information and knowledge) cannot be ignored in understanding the complex dynamics within criminal networks(Robins, 2008). In addition, a recent finding by Quax, Appoloni and Sloot (2013) show the diminishing role of hubs in dynamical processes on complex networks, indicating the need for alternative intervention strategies . These studies illustrate that although the centrality approach is a useful approach to identify potentially 'critical' actors for criminal network disruption, an additional qualitative assessment on the individual level is essential for understanding the effects of network disruption. Moreover, besides centrality propositions, individual qualities (human capital) might be a vital criterion for selecting critical actors for network disruption by itself. This is called the 'human capital' approach.

The human capital approach

The importance of the human capital approach to criminal network disruption has been addressed by several authors (e.g. Sparrow, 1991; Klerks, 2001; Tsvetovat & Carley, 2003)). Human capital is a term originated from economics that is defined as the stock of competencies, knowledge, social and personality attributes, including creativity, embodied in the ability to perform labor so as to produce economic value. Equal to legal business, every criminal market consists of a business process involving different steps of production or activity. (klerks, 2001; Morselli, 2009; Spapens, 2011). In each sequent step of the process different information, goods and human capital is exchanged and added to the next, following a chainlike structure. This process can therefore be defined as a value chain (Gottschalk, 2009). Every step of the value chain requires a different range of skills and knowledge human capital, depending on the specific characteristics of the illegal activity (Morselli & Roy, 2008; Cornish, 1994; Bruinsma en Bernasco, 2004). Illegal entrepreneurs involved in different criminal markets find these 'human resources' in embedding trusted social networks. In this way human capital is assembled and integrated into tight goal-oriented criminal collectives.

Sparrow suggested that identifying the actors fulfilling the most specialized tasks offers great opportunities for destabilizing the criminal network. Hence, as these are often thinly populated within the embedding social networks, they are the most difficult to replace if extracted from the network. Sparrow argues that 'substitutability' might therefore be an important criterion for network disruption (Sparrow, 1991). To understand the structure of a criminal value chain Cornish introduced the crime scripting method (Cornish, 1994)). This method helps systematize knowledge about the procedural aspects and procedural requirements of crime commission, by generating a blueprint of all sequential phases within the value chain. In addition, Bruinsma and Bernasco (2004) combined this crime scripting method with social network analysis, to identify 'human capital' and 'substitutability' within criminal networks. They found that specific specialized roles could be identified in different criminal markets by analyzing crime scripts within the context of the criminal network. Morselli and Roy (2008) applied this method to study 'brokerage roles' within criminal value chains. Their observations reveal that 'value chain brokers' were essential for integrating 'human capital' from the criminal network, within the different phases of the value chain. In addition, Spapens identified this brokerage role within Dutch ecstasy production value chains and observed that these brokers not only increased 'social capital' within these criminal collectives, but added 'human capital' as well (Spapens, 2010). Hence, these brokers possessed sufficient resources and reputation that is essential to initiate and coordinate a ecstasy production value chain. In fact, these findings emphasize that combining social capital approach and the human capital approach the effects of network disruption might be amplified. It can be concluded therefore that crime script analysis is an important method for identifying 'human capital' within criminal value chains.

The concept of criminal network resilience

As a consequence of being disrupted, criminal networks develop the capacity to absorb and withstand disruption and to adapt to change when necessary, that is called network resilience. According to several authors the concept of resilience consists of two aspects: first, the capacity to absorb and thus withstand disruption and secondly the capacity to adapt, when necessary, to changes arising from that disruption (Bouchard, 2007; Ayling, 2009).

The first aspect of the resilience concept depends on the level of redundancy that is inhabited in its criminal network structure. The more its network structure is characterized by high levels of redundancy in sense of diversity of relationships between actors, the more options there are to compensate for loses in 'human capital' or finding new methods to continue the value chain (Williams, 2001). Redundancy enables members of the network to take over tasks of actors that are targeted by successful law enforcement operations. Even if some connections are broken, the diversity of different ties between actors allows the network to function. Redundancy in the network is associated with strong ties between network members. Strong criminal ties offer reciprocated trust, which is essential within the uncertain and hostile criminal environment (Morselli, 2009). Replacements with a reliable reputation are therefore often found within the social connections directly embedding the actors involved within the criminal business process. These cohesive criminal collectives often initiate from already established social networks of for instance kinship, friendship or affective ties (McCarthy et al., 1998; Kleemans & De Poot, 2008). This means that replacements are often found in short social distances, from this cohesive core.

However, actors with essential skills or knowledge might have to be replaced. If these specialists are thinly populated within these redundant collectives, replacements have to come from the 'external' criminal environment. In these settings non-redundant social connections within the embedding network become important for finding 'human capital' at a greater social distance from the trusted criminal core. As described above 'criminal brokers' are essential catalysts for finding these replacements within the embedding network (Morselli & Petit, 2007). This principle is called the '*strength of weak ties*', were non-redundant ties within the embedding network offer access to new opportunities, resources and information, that are not available within redundant networks (Granovetter, 1983; Hagen & McCarthy, 1995) work offers a framework for understanding criminal network phenomena, such as criminal careers in organized crime. For instance, is was found that the social opportunity structure of social ties offers an explanation for late-onset offending and people switching from conventional jobs to organized crime, also later in life (Kleemans & De Poot, 2008).

Although *weak ties* might reveal new business opportunities, finding replacements across these connections inhabits great risks to network security for two reasons. First, trust is more easily built between like-minded individuals, as compared to outsiders from different social and ethnic backgrounds (Spapens, 2010; Kleemans & Van de Bunt, 1999). This means that criminal networks in search for capable and trustworthy replacements might need to cooperate with criminal actors for who reliability is difficult to assess. Secondly, coordinating the search for replacements from the embedding network demands more efficient ways of internal and external communication. This increased transfer of information as a result of disruption or internal 'noise' within social networks in general, was also observed in a study of artificial complex networks (Czlaplicka et al., 2013). This study shows that stochastic resonance in the presence of noise can actually enhance information transfer in hierarchical complex social networks, such as illegal networks . However, this increased transfer of information containing potential incriminating evidence throughout the network, also increases the risk of exposing the whole network by a single arrest (Lindelauf et al., 2009; Lauchs et al., 2012)). The capacity to adapt to these changed circumstances of increased risk refers to the second aspect of the resilience concept.

In adapting to these changed security settings, controlling the flow of information becomes the number one priority within illegal networks (Ayling, 2009). Based on previous studies, this is often achieved through '*compartmentalization*', meaning that important information is isolated within different compartments or 'organizational cells'. This strategy prevents that the whole network becomes exposed, if one compartment becomes detected and disrupted (Williams, 2001). As described above, this compartmentalization is often found in terrorist networks with longer times to task (Krebs, 2002). In addition, Baker and Faulkner (1993) also found a level of compartmentalization between the core and periphery within illegal price-fixing networks as a result of disruption . By deliberately separating the flow of information between members within the periphery and the 'visible' core, the price-fixing network decreased the chance of the 'leaders' becoming exposed after a single arrest. These studies show that in order to adapt to the changing circumstances after disruption, criminal networks tend to organize a form of non-redundancy within their internal flow of information in order to protect their important members from becoming discovered.

In fact, these features make criminal network resilience a paradoxical concept. On the one hand it depends on redundancy, that's essential for finding trustworthy replacements after losses due to disruption. On the other hand it depends on non-redundancy, as the increased risks associated with the search replacement, demand compartmentalization of the flow of information to prevent further detection. The importance of either aspect depends on the given network objectives of recovery or security at a certain moment. This demonstrates again that criminal network resilience is a dynamical process that evolves along the tradeoff between efficiency and security which shapes its network structure accordingly.

4.2 RESEARCH DESIGN AND DATASETS

As described above, the aim of this study is to unravel the dynamics of resilience within criminal networks, as a consequence of network disruption. This is done by simulating and observing the mechanisms of disruption and –resilience in a criminal network involved in cannabis cultivation. First, we introduce five different approaches for network disruption, according to strategies based on the 'social capital'- and 'human capital' approach previously described. Secondly, we introduce three models for network recovery, according to the principles associated with the resilience concept described above. These include *redundancy* and *non-redundancy* in relation to the social structure embedded in the disrupted criminal network. By simulating these disruption strategies and resilience mechanisms at the same time, we observe the way this affects its network structure in terms of efficiency and security. Our simulations are aimed at a real life criminal cannabis cultivation network that we analyzed from a large unique dataset obtained by a regional criminal intelligence unit resorting under the Dutch Police. This dataset contains information on criminals, criminal relationships and criminal activities collected over the period January 2008 – December 2011. The details of the datasets are described in the next Section, followed by a description of the final network representation and its properties in terms of degree distribution.

Datasets

The dataset utilized in this research is built by the aggregation of two distinct datasets: Dataset Soft and Dataset Hard, details of these datasets are provided in Appendix 4A (p. 125)

Dataset Soft (D_{soft})

The data for this dataset was collected by a regional criminal intelligence unit resorting under the Dutch police over the period January 2008 – January 2012. The data is primarily retrieved from criminal informants and consists of anonymous intelligence reports on criminals and their criminal relationships involved in serious- and organized crime (N = 6020). Secondly, it contains information and reports from closed criminal cases aimed at organized crime. Both data sources contain specific variables on the individual roles that network actors occupy within different illegal markets in relation to the specific crime scripts (e.g. cannabis cultivation and trade, cocaine trade, heroin trade, ecstasy production and trade, trafficking of human beings etc.). These role variables are scored by intelligence analysts through structural analysis of intelligence reports on role specific information.

Criminal informants have different motives to talk to the police and their identities stay covered for security reasons. In some cases, this makes it difficult to check the facts. For this reason this data is called soft data. Therefore we call this dataset soft (D_{soft}). However, based on detailed intelligence reports written after every conversation, the reliability of facts were checked by intelligence analysts by comparing this soft information with facts covered in other police data sources, such as criminal investigations data or street police reports. In addition to intelligence retrieved from criminal informants the dataset therefore also contains observations from street police officers during their duty and information from (closed) criminal investigations. This includes detailed data from wiretaps and surveillance reports, as well as eyewitness and suspect statements containing additional information about criminal relationships. Incidentally information retrieved from online communities (e.g. Facebook) was also used in addition to construct relations between all known actors in the criminal network.

The main strength of this dataset is therefore that it contains detailed narrative information on criminal cooperation, individual roles and involvement within illegal markets from multiple data sources, including informants that are sometimes part of the criminal network themselves. This offers the opportunity to combine methods of crime scripting with social network analysis. Moreover it involves information about important criminal individuals that were never arrested nor detected within criminal investigations. In addition to previous studies on criminal networks that are based on closed criminal investigations, this dataset might give a unique perspective on criminal network structure, including the role of actors that are never observed before.

A weakness of this dataset is that it is in part biased; there is a reasonable possibility that there are some blind spots within the criminal network we do not know about, because there aren't informants within these networks. Another point of concern is that data collection is affected by police priorities. Secondly, not all facts that are written within the intelligence reports can be checked. This might be a risk to reliability of the data, if we want to look at a single criminal relationship in detail. However, for this study we are only interested in features of the overall network structure, therefore our results will not be affected by one or two false reports. Moreover, informants that turn out to be unreliable are fired directly; this results in a kind of natural selection of the most reliable informants. In order to alleviate some of these weak aspects we introduce a second dataset: Dataset Hard.

Dataset Hard (D_{hard})

This dataset consists of arrest records over the period 2008 – 2011. The dataset on arrest information consists of persons with a police arrest registration dating from the period 2008 until 2011 (N = 24.284) within the same police region from which the soft data was collected. Every police suspect is registered into a police database with a connection to her or his arrest registrations. This arrest record contains variables of the date, time, place and law article for which they were arrested. This means that in case more actors are arrested for the same felony, they are connected to the same arrest record. Therefore, it can be assumed with a reasonable level of certainty, that these actors have a criminal relationship at the time of the arrest registration.

The strength of this dataset is that it was retrieved from police officers themselves, which makes it reliable. For instance, every personal identity is being checked on the bases of identification. In practice police officers need more hard evidence than solely a criminal intelligence report to arrest a potential suspect. Therefore, all potential criminal relationships following this dataset are based on more concrete evidence as opposed to dataset soft. Therefore, we'll call this dataset hard **(D_{hard})**. Secondly it is bulk data over a relatively long period of time containing many criminal relationships. This offers the opportunity two recover a network structure based on arrests. Unfortunately arrest registrations do not contain much narrative information. Another weakness of this dataset is that important network actors might be under represented in this dataset, because they don't get arrested easily as opposed to the more visible working roles in these networks. In addition, these arrest records are also to a certain extend biased towards police priorities.

The description of both datasets reveals that this study isn't immune to the same dark Figure problem that influenced previous criminal network research (e.g. 7). However, every source of data offers another perspective on the criminal network that is the focus of this study. By combining intelligence reports (soft) with criminal investigations data, surveillance data and arrest data (hard), different perspectives of the same criminal network complement each other in offering us the most optimal observation of the criminal network possible.

The criminal network structure

As described above, the key property of the current dataset is the presence of information about criminal activities of actors, their individual roles and connections to other actors. By combining the two datasets we have recovered the structure of a criminal network involved in multiple criminal markets operating within the Netherlands. In accordance criminal network theory described above, we can distinguish between two network levels: the criminal network involved in a specific illegal market and the (social) embedding macro-network from which criminal cooperation originates (McCarthy et al., 1998; Kleemans & Van de Bunt, 1999; Spapens, 2010). The embedding macro network contains all actors and criminal relationships between all actors disregarding their illegal activities. A criminal relationship is defined as the social links that enable individual members of the network to freely exchange information about potential illegal activities. Therefore this embedding network is called the 'macro network', and we will denote it byG_{Macro}. By itself, G_{Macro} is built up from the dataset D_{soft}, which is collected by criminal intelligence operations as well as the dataset D_{hard} , which is gathered from arrest registrations. In constructingG_{Macro}, the two datasets show little overlap (see Table 1). This can be explained by the fact that central key players are often protected by the network structure, and therefore have a lower chance of becoming arrested, as compared to actors directly involved in the value chain. As a consequence these actors are generally underrepresented within investigative or arrest data, which also characterizes dataset D_{hard}. In contrast dataset D_{soft} is built from criminal intelligence gathering and is collected with the specific aim of identifying the invisible actors, who stay largely unknown within criminal investigations. Both datasets therefore offer a different observation of the same criminal network. The combination of these two observations provides us with a unique empirical perspective of a criminal network structure.

The second level of network structure consists of all actors involved in the specific value chain of organized cannabis cultivation. This second level micro-network is obtained by removals of all actors and connections from G_{Macro}, which are not involved in the value chain of cannabis cultivation as qualitatively scored within D_{soft}. This sub-network will be denoted by G_{VC}. Within G_{VC} there is data on the specific roles of individual actors within the value chain of organized cannabis cultivation. Properties of both networks are described in Table 4.1 and depicted in Figure 4.1.

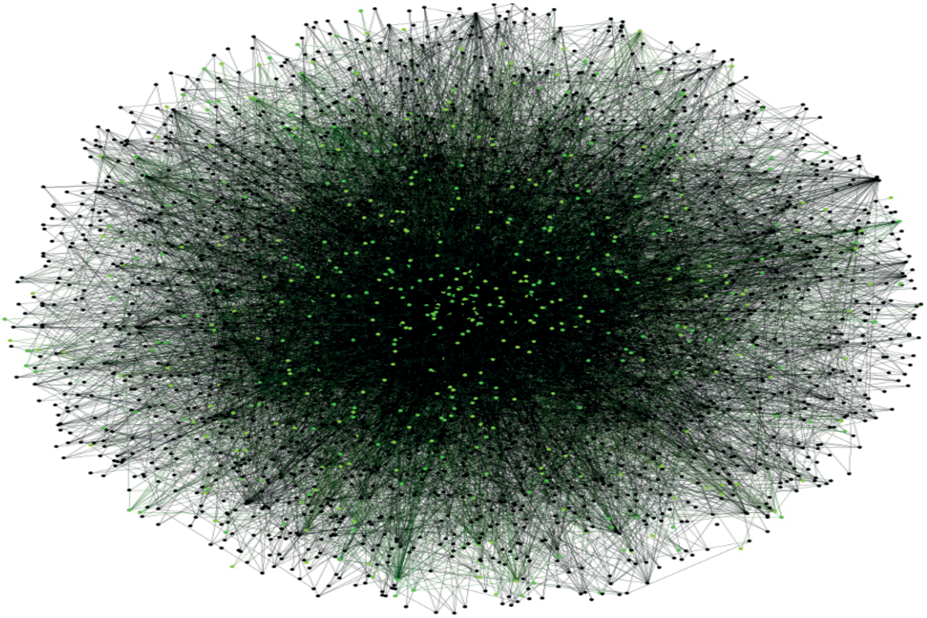


Figure 4.1. Socio-graph of the criminal network under study: G_{VC} light-colored actors) represent network members that are involved in cannabis cultivation. G_{VC} is part of G_{Macro} which includes the actors from the criminal macro network that are connected through other criminal activities (dark-colored) actors.

Table 4.1. This table shows the properties of the Soft (criminal intelligence data) and Hard (arrest registration data) datasets. In the third column the overlap between the two datasets is depicted. The fourth column shows the macro network structure. The fifth column shows the properties of the subnetwork of actors involved in cannabis cultivation. This subnetwork is constructed by removing all actors and links not involved in the cannabis production network.

Network/Stats	D_{soft}	D_{hard}		$G_{macro} = D_{soft} + D_{hard}$	G_{VC}
Number of Actors	6020	24284	958	29346	793
Number of Links	12073	35359	1438	47127	1388
Avg. degree	4.01	2.91	3.6	3.21	3.92
Avg. shortest path	5.48	9.81	5.75	8.62	4.35
Diameter	20	26	14	25	11
Largest component	3998	9413	535	13964	459

In order to test the effectiveness of the three network disruption strategies described above, we need specific data on the value-chain activity of the individual actors within the network. Because data on value chain roles is qualitatively scored for all individual actors involved in cannabis cultivation, we focus mainly on the effectiveness of disrupting the cannabis cultivation network G_{VC} as part of the criminal macro network G_{Macro}.

Identical to any social network, criminal networks have no strict boundaries (Williams, 2001). Therefore, we emphasize that the embedding macro network is in theory a world-wide network (10). However, our observations of the embedding criminal network are limited to where the data collection process within the police region ends. Within social network analysis methodology this is called the 'boundary specification problem' (e.g. Klerks, 2001; Morselli, 2009)), meaning that setting a boundary of the network as a result of the available data, might affect the results of the applied SNA methodology. But, as described above, replacements are preferably found in the 'trusted' and 'like-minded' network directly embedding the disrupted criminal network, instead of replacements from outside through other backgrounds. Moreover, from a practical point of view, finding replacements within substantial physical distances would be counterproductive (Klerks, 2001; Spapens, 2010).

Degree Distribution

For one part the effect of different disruption strategies depends on network topology. As described above, one important measure for network topology is the network degree distribution. If the network degree distribution follows a power law, then the network is scale-free. This means, besides other implications, that network robustness depends on actors with a relatively high degree, so-called hubs. If these hubs are attacked the network will fall apart into subnetworks (Albert, 2000). We estimate the power-law distribution $P(\mathrm{x}) = Cx^{-}\lambda$ to fit the degree distributions in the G_{Macro} and G_{VC} networks using maximum likelihood estimators as well as a goodness-of-fit based approach to estimate the lower cutoff for the scaling region (61). The results of this analysis are shown in Figure 4.2.
Analysis of the graphs show that for G_{Macro} the degree distribution fits a power-law with a lower cutoff of x_{min} = 34 and λ = 1.55 . For G_{VC} the lower cutoff equals 1 and $\lambda = 1.5\lambda^{= 1.5}\,\lambda^{= 1.5}$. In both cases the p value is relatively high, indicating that with high likelihood these distributions follow a power law distribution. This means that both networks are probably scale-free and might therefore be vulnerable to deliberate attacks, targeting actors with high degree centrality (hubs).

In the next paragraph we describe in more detail how the networks are structured with respect to the value chain structure of the cannabis cultivation.

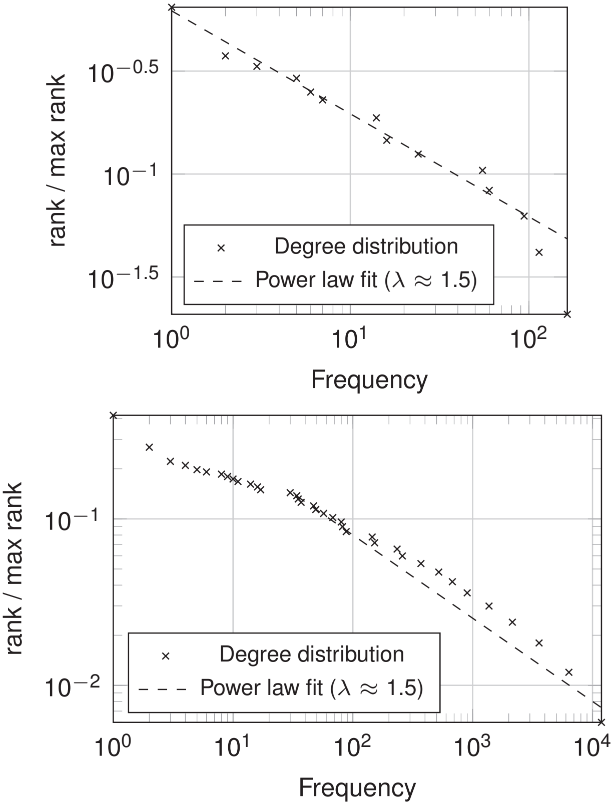


Fig 4.2. Rank-frequency[25] plot for the data and the approximation by power-law distributions:(a) G_{VC}, $x_{\min}$ = 1, λ=*1.5*, p=0.52. (b) G_{Macro}, $x_{\min}$ = 34, λ=*1.5*, p=0.73.

Value Chain configuration of organized cannabis cultivation

As described above, organized cannabis production is a delicate business process, involving many tasks and roles and flow of human capital, information and resources, which can be described in a value chain by using crime script analysis. Figure 2.1 (see p. 34) shows the result of crime script analysis of an illegal market of cannabis cultivation, containing all phases and corresponding tasks/roles in sequential order (Spapens et al., 2007; Morselli, 2001; Emmet & Broers, 2008).

Understanding the value chain of a specific criminal activity is important for developing network disruption strategies from the ‘human capital’ approach. Specific roles can be identified, that are critical for value chain continuation. Within the technical system of

[25] A rank/frequency log-log plot is a plot of the frequency versus the rank on logarithmically scaled axes. For a more elaborate description on how to construct such a plot, see the Mark Newman (Newman, 2005)..

cannabis cultivation the roles of '*coordinator*' and '*growshop owner*' are essential for initiating a criminal collective (Figure 2.1, p. 34). They control almost every stage of the value chain and operate as criminal brokers in bringing essential roles together at the right place and time. *Coordinators* and *Growshop owners* are important for the flow of information and keeping the value chain participants together. Therefore these roles can be marked as vulnerable for network disruption from both a 'human capital'- and 'social capital' approach, as they might also score high on degree and betweenness centrality within the value chain network.

Secondly *specialists* can be identified within the criminal collective, that bring specific knowledge or skills needed to complete the value chain (Morselli, 2009; Spapens, 2010)). These specialists are often sparsely populated within the embedding macro-network and are therefore often part of more than one value chain at a certain point in time. Within the value chain of cannabis cultivation the network members that fulfill the role of *diverting electricity* can be identified as specialists for two reasons: First this role requires specific knowledge and technical skills needed for illegally diverting electricity that fits the needs within cannabis cultivation. Secondly these roles demand high levels of trust and reputation. Hence, these '*electricians*' might retrieve sensitive information about critical locations and participants that is related to their flexible role of specialist (Spapens et al., 2007; Emmet & Broers, 2008) . Therefore, involvement of these actors increases the risk of information being leaked to competitors or the government (Kleemans et al., 2002). A trustworthy reputation is therefore essential for these specialists to operate freely. For cannabis networks, finding or replacing these 'specialists' is not an easy task because reliability and integrity is not particularly part of the ethics within criminal networks. Therefore, network members involved within '*diverting electricity*' can also be identified as vulnerable targets for network disruption from a 'human capital' approach. This will be included as a specific strategy within the disruption model discussed in a later Section.

As was previously described criminal network resilience against disruption depends on network redundancy. Redundant criminal networks offer many alternatives to replace targeted actors within the network. Figure 4.3 shows the direct relationships between value chain roles that are derived from the value chain network of cannabis cultivation (G_{vc}). In this Figure the VC roles are also connected if one actor in the social system fulfills more than one role within the value chain. The size of the actors is proportional to the amount of actors having this role within the data. The thickness of the links corresponds to the number of direct connections between actors with these roles within the G_{vc} network.

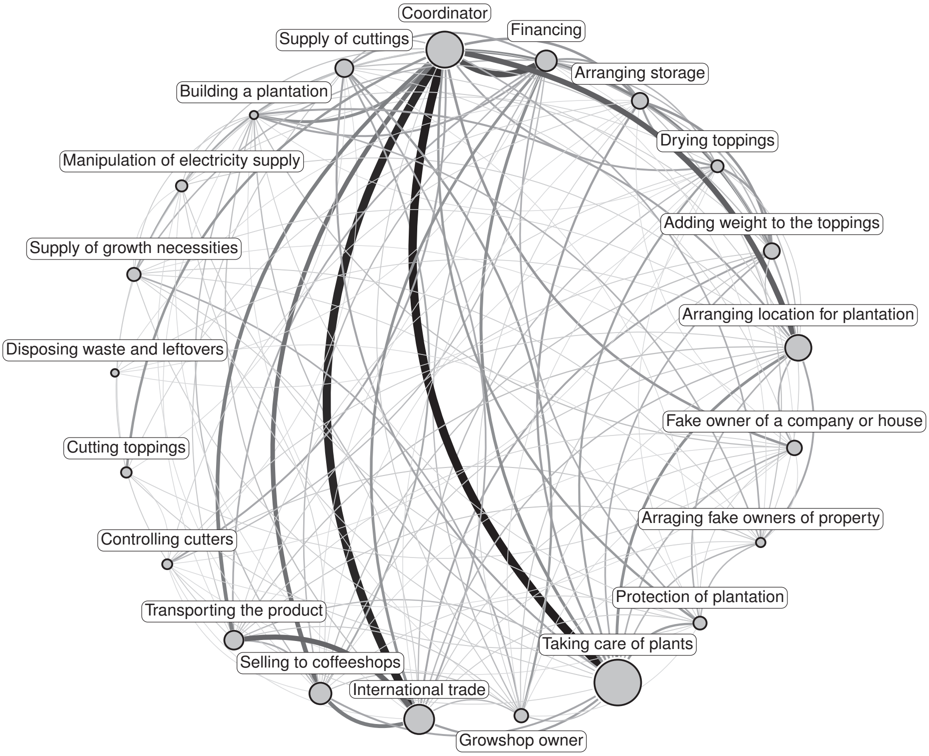


Figure 4.3 Observed configuration of the social system of the cannabis cultivation value chain using soft and hard datasets, see also appendix 4A (p.Error! Bookmark not defined.). Within this system roles are connected if there is at least one link in the value chain network (G_{vc}) between actors of these roles. The sizes of the actors correspond with the number of actors fulfilling this role, and link thickness corresponds with the total number of links between roles within the data.

The infographic shows that some roles within the value chain are highly connected and some roles are not. This indicates that some actors involved in common roles within G_{vc} might easily be replaced by directly reconnecting the 'orphaned actors' with actors with that same role in G_{vc} (e.g. network members that are involved in 'coordination' and 'taking care of plants' in Figure 4.3). For roles that aren't that well connected within G_{vc} (such as manipulating electricity and building a plantation in Figure 4.3) replacement isn't that easy, for reaching the possible replacements might take several indirect connections. As described above trust and reputation are the basis for criminal cooperation. Therefore actors connected within a specific value chain network are often surrounded by a social structure of social ties (e.g. kinship or friendship) or previous criminal cooperation concerning other criminal activities. As descibed above this surrounding social structure is known as the 'embedded macro network' G_{Macro}. Trustworthy replacements within criminal network are generally found at the shortest paths from the targeted actor towards the nearest potential replacement. This means it is also possible that replacements are found trough actors that are part of the embedding macro network but have no involvement in the value chain network of cannabis cultivation at all. These actors from the embedding macro network form a 'bridge' between the 'orphaned actors' and replacements with the same role in G_{vc}. Therefore replacement follows the shortest paths through actors from the embedding macro network, instead of solely the value chain network. This interaction between the embedding macro network (G_{Macro}) and the value chain network is therefore important for understanding criminal network recovery after intervention and will be explained further in the next paragraphs.

4.3 METHODOLOGY

The second aim of our research is to test the effectiveness of different strategies to disrupt an illegal cannabis cultivation network G_{vc}, taking into account that the network will try to recover itself by replacing targeted actors and relations using ties and connections of the embedding criminal network G_{Macro}. Therefore, a modeling framework for both network disruption and network resilience is needed.

Modeling network disruption

From a law enforcement perspective criminal network disruption aims at stopping or frustrating the value chain of a criminal activity by removing active actors from the criminal network. In practice this can be obtained by strategically targeting and arresting individual actors involved in the value chain. The sequential order in which actors are targeted depends on the disruption strategy applied. For this study five different disruption strategies are selected according to the general disruption approaches described above:

Random Disruption

1. The ***Random*** **strategy** follows no preference or ranking during selection of candidates for removal. This strategy can be associated with opportunistic law enforcement control lacking any form of strategy. As describes in the previous Section, this is sometimes the case within the control of organized cannabis cultivation, for instance randomly busting cannabis cultivation sites and making arrests on the spot.

Two types of Social Capital Disruption

The social capital approach aims at strategic positions within criminal networks. As described above, this can be divided in two main strategies: degree centrality attack (hubs) and betweenness centrality attack (brokers).

2. The ***Total degree*** **strategy** aims at the actors with highest degree centrality (hubs) within the G_{vc} network. From this approach the order of actors being targeted follows

individual degree centrality scores from high to low. Both G_{Macro} and G_{vc} networks have heavy-tailed degree distributions, which might make them vulnerable to these hub attacks (Figure 4.2). This strategy is associated with control strategies that focus on 'the kingpin'. However, as described above the most central actor does not necessarily have to be the most powerful. Leaders might be hidden in anonymous periphery, but because we use intelligence data in addition to investigative data, degree centrality might correlate with powerful positioning (e.g. 64).

3. The ***Betweenness*** **strategy** aims at actors with the highest betweenness centrality (bridges) within the G_{vc} network. From this approach the order of actors being targeted follows individual betweenness centrality scores from high to low. This strategy is associated with the 'key player' control strategy in law enforcement. This strategy might be highly correlated with coordinators of growshop owners, but could also involve actors in other roles that might be of importance because of their informal social capital within the value chain. It aims at strategically positioned brokers, connecting several criminal groups.

Two types of Human Capital Disruption

Besides targeting actors based on their general positioning within the criminal network, this approach aims at targeting actors by their individual specific characteristics (Human Capital).

4. The ***Value chain degree*** **strategy** aims at individuals with the highest Value Chain (VC) degree within the G_{vc} network. The VC degree of a particular actor is measured by the amount of links defined within the social system of the value chain configuration (see Figure 4.3). This strategy is associated law enforcement controls aimed at actors that inhabit a great reputation. It can be assumed that actors with a higher reputation will be involved within more and different value chains within the value chain network. From a network perspective this means that these actors will automatically have a higher degree centrality and will be more visible within the network.
5. The ***Specific Value Chain Role*** **strategy** aims at specific 'human capital' within a specific criminal value chain. As compared to other strategies, actors are targeted qualitatively based special skills or knowledge and the presumed 'substitutability' within the value chain. Based on observations within the data under study and the literature on the cannabis cultivation value chain (Spapens et al., 2007; Emmet & Broers, 2008) the role of '*diverting electricity*' was selected to analyze this strategy. From this approach the sequence of actors being targeted follows all actors that are labeled for the *'diverting electricity'* role within the value chain of cannabis cultivation. This strategy is associated with the '*facilitator*' strategy within law enforcement control, for targeting thinly populated specialists in order to frustrate the operational criminal process.

By simulating these strategies we can measure the effect they will have on the network and cannabis production. For each strategy, different runs are being performed and for each run thirty actors are being removed.

Modeling network resilience

The effect of network disruption cannot be measured without understanding network resilience. Therefore the ability of a criminal network to recover its value chain structure after applying a network disruption strategy has to be simulated. In order to recover the value chain, the actors that are not targeted (orphaned actors) will have to find a replacement that can fill the gap that a targeted value chain actor left behind. This replacement needs the same skills and knowledge (VCrole) as its ancestor. By replacing the actor by someone in the network with the same VCrole, the essential VC links are reestablished and the value chain can be operational again. As explained in the introduction, these replacements are often found through redundant or non-redundant contacts from the embedding network G_{Macro} By modeling resilience, we therefore simulate the dynamic interaction between the value chain network G_{vc} and the embedding criminal network G_{Macro} in the search for suitable replacements for network recovery.

At each step of the simulation an actor is targeted by applying one of the disruption strategies. This targeted actor is indicated by n_{rem}. All n_{rem} actors will be accounted for in a set (n_{rem}) of 'orphaned' actors, which were connected to n_{rem} by a value chain connection (VC link). For each broken VC link, it is assumed that recovery will start from these orphaned actors. These actors will be the first to find replacements within the embedding macro-network (G_{vc}) as depicted in Figure 4.4.

At first target actor (*A*) is selected by one of the preferred dismantling strategies (Figure 4.4a). Actor *A* has two adjacent VC Links with actors *B* and *C*. In the next step (Figure 4.4b) target actor *A* is removed from the network, leaving two dangling links. The orphaned actors *B* and *C* tend to recover the lost links by connecting to actor with the same VC role of *coordinator* as the *A* actor had by using one of recovering algorithms. In this way the broken VC links are recovered by connecting to actor *E* (Figure 4.4c). In simulating network resilience three recovery mechanism algorithms are applied: random recovery, recovery preferred by distance and recovery preferred by degree. The general recovery algorithm is depicted below.

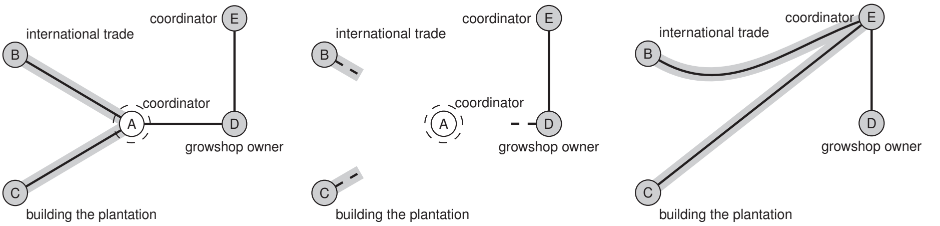


Fig 4.4 Dismantling and recovery of a network: (a) Actor A is selected as a target actor by a chosen strategy. (b) Actor A is detached from actors B, C, D and removed from the network. (c) Orphaned actors B and C recover their connections by linking to actor E of the same role as A actor (here: coordinator).

General recovery algorithm

$G_{VC}(N, E)$ — subnetwork with a set of actors N and set of edges E;

n_{rem} — actor which was removed from G_{VC};

(n_{rem}) — set of orphaned actors n , which were adjacent to n_{rem};

$role(n)$ —VC role of actor n;

$R_N(n_{rem}) = \{n \in N : role(n) = role(n_{rem})\}$ — set of actors from G_{VC} which can replace value chain position of actor n_{rem}.

For each orphaned actor n from (n_{rem}):

1. With likelihood $P_{rewire} = 1 - \frac{1}{|R_N(n_{rem})|+1}$ evaluate whether or not the lost VC link will be recovered by n.
2. If previous step gave positive answer, then select recovery candidate n_c from the $R_N(n_{rem})$ following specific preference, which is chosen based on the recovery mechanism.
3. Connect actors n and n_c.

Next, we introduce three algorithms, which are based on this general recovery algorithm but have a specific preference among candidates for recovery.

Random recovery algorithm

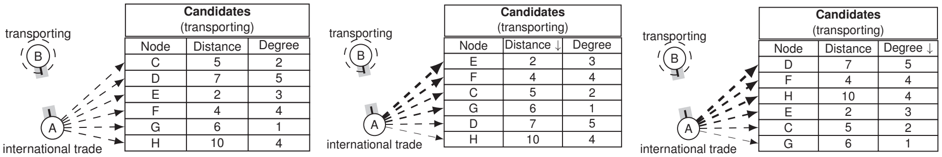
The random recovery algorithm suggests that no candidate from $R_N(n_{rem})$ has preference over others, and all of them are treated equally. This algorithm implies that the macro network is heterogeneous and that replacements can be chosen from all parts of the network, hence, at step 2 of the general recovery algorithm candidate n_c from $R_N(n_{rem})$ is selected randomly.

Preference by distance recovery algorithm

Trust and skills are important criteria for selecting suitable replacements. Therefore,Therefore it's more likely that preferred replacements are preferably found within the redundant network of the actors involved in the value chain. This means that candidates with the shortest path from orphaned actors within the macro network (G_{Macro}) will have more chance of becoming a replacement than actors further away. This can be translated into a preference by distance recovery algorithm, in which the selection of replacement of actors from $R_N(n_{rem})$ in step 2 depends on the distance between a possible candidate actor and an orphaned actor. Within this preferential recovery algorithm,algorithm the likelihood of actor n_c to be selected is proportional to $1/d$, where d is the distance between the orphaned actor and n_c. Within this recovery mechanism, the likelihood that a value chain link will be recovered depends on both the substitutability and the network distance between replacement candidates and orphaned actors.

Preference by degree recovery algorithm

A second criterion for criminal cooperation is reputation. This means that actors with a good reputation have a higher chance of becoming a replacement than actors with a bad reputation. It can be assumed that actors with a higher reputation will be involved within more and different value chains throughout the overall network (G_{Macro}). As identical to the VC degree disruption strategy, this will be associated with actors with high degree centralities. Therefore we introduce a third recovery algorithm with a preference for replacements by degree-centrality, in which the selection of replacement actors from $R_N(n_{rem})$ in step 2 of the general recovery algorithm depends on the degree centrality of the potential replacement. Within this preferential recovery algorithm the likelihood of actor n_c to be selected is proportional to $1/d$, where d is the degree of n_c within GMacro. Within the general recovery algorithm, the likelihood of value chain link recovery P_{rewire} depends on the exchangeability of the targeted actor. If $R_N(n_{rem}) = 0$ then the connection with an actor of a particular role could not be recovered.



Candidates (transporting)		
Node	Distance	Degree
C	5	2
D	7	5
E	2	3
F	4	4
G	6	1
H	10	4

Candidates (transporting)		
Node	Distance ↓	Degree
E	2	3
F	4	4
C	5	2
G	6	1
D	7	5
H	10	4

Candidates (transporting)		
Node	Distance	Degree ↓
D	7	5
F	4	4
H	10	4
E	2	3
C	5	2
G	6	1

Fig 4.5 Random and preferential recoveries of broken VC links are depicted, after strategically removing actor *B*: (a) Candidates for replacement are chosen randomly without preference. (b) An actor with a smaller distance to orphaned actor *A* is more likely to be chosen as replacement. (c) An actor with a higher degree is more likely to be chosen as replacement.

The difference between random recovery (a), distance recovery (b) and degree recovery (c) is depicted in Figure 4.5. Here, actor B is targeted by one of the disruption strategies. As a result, the orphaned actor *A* has lost its value chain connection '*international trade–transporting'*, and will therefore try to re-establish a link with a suitable candidate in order to restore the value chain. The list of candidates, who can fulfill the same role as *A*, is shown in the first column. In case (a) the candidates are chosen randomly and have no preference between each other to be chosen as a candidate for recovery. In case (b) the actors with the shortest distance to *A,* are more likely to be selected for replacement. In case (c) the actors with the highest degree are more likely to be selected for replacement.

Measuring the effects on network structure

After the disruption strategies and the recovery strategies are applied at the same time, after a number of attacks following the same strategy, we want to measure the impact this has on its networks structure, in terms of efficiency and security. Therefore,Therefore we introduce the measure of efficiency within the Value Chain network G_{VC} that is computed by the following metric:

$$Efficiency = \frac{2}{N(N-1)} \sum_{\substack{i,j=1 \\ j \neq i}}^{N} \frac{1}{d_{i,j}} \tag{1}$$

In this metric d_{ij} corresponds to the distance between actors i and j of G_{VC} and N equals the amount of actors in G_{VC}. The denominator creates a measure that varies from 0 to 1, where 1 is complete connectivity and 0 indicates that the network is completely separated into isolated components. Note that in this metric the distance between actors is measured by the shortest paths within the embedding network (G_{Macro}). This implies that some essential values can flow through criminal relationships that are not directly derived from the subnetwork of cannabis cultivation *(*G_{VC}*)*. The metric shows how efficiently actors within the network can communicate and exchange values (information, goods) between each other(Bienenstock & Bonacich, 2003; Memon & Larsen, 2006).

In addition to the efficiency of the network we introduce a second metric that estimates the influence of network disruption on the secrecy within the value chain network. Criminal network structures arrange a level of secrecy by minimizing the direct transfer of information, thereby reducing the risk of exposing direct involvement in illegal activities of individual members to police surveillance- or intelligence services. Secrecy is strongly associated with the metric of 'network density'. This measurement is intended to give a sense of how well communication pathways in the network are capable of getting information out to the network's participants. Density (or the equivalent 'brightness') is calculated by dividing the number of direct connections by the maximum possible connections within the observed network.

ThereforeTherefore, density decreases by a decreasing number of direct connections. This slows down the direct transfer of information throughout the network. A network with a high density is more effective thanks to the large number of direct connection between actors, but it has higher vulnerability as well, because if one actor is caught he can provide critical information about other participants of criminal business (Klerks, 2000). This metric is based on the analysis of network density after interference, in comparison to its initial state. The density, or brightness, of the network is calculated by the following metric:

$$Density(G_{VC}) = \frac{2E(G_{VC})}{N(N-1)} \tag{2}$$

In this metric $E(G_{VC})$ corresponds with amount of links in G_{VC} and N equals to amount of actors in G_{VC}. The values of this metric are also bounded between 0 and 1, where 1 happens to be in complete network where all actors are interconnected and, hence, exposed, and 0 indicates that the network is completely dismantled, dark and secure.

4.4 RESULTS

In order to test the network resilience of G_{VC}, three sets of simulation experiments were conducted – with random recovery, with distance recovery and degree recovery algorithms. Each simulation was performed on G_{Macro}, and because the aim is to disrupt the value chain of organized cannabis cultivation, disruption strategies are targeted at the actors who are specifically part of G_{VC}. In each simulation thirty runs for every disruption strategy were conducted, resulting in an average score for each strategy.[26] As described above, the role-specific strategy was targeted at all actors involved in the role of *'diverting electricity'*.

Figure 4.6 presents the efficiency of the value chain network G_{VC} with random recovery at each step of the law enforcement strategy. In contrast with the aim of the applied strategies, it shows that as the disruption strategies are being applied the efficiency of G_{VC} actually *increases*. This means that when more specific actors are being targeted from the value chain, the more efficient the network becomes after random recovery. Figure 4.6 also indicates that *Random* and *Role-specific* disruption strategies slightly increase the network efficiency. From a topological perspective this implies the network is highly resilient and flexible in restoring these crucial value chain facets from its network structure. On the other hand, when the 'role specific' specialist strategy is taken into account the network

[26] The numerical experiments showed that ten runs were enough to get stable results with standard deviations less than 5 %.

might be much more vulnerable. Hence, the value chain simply ends when a single facet within the technical system of the value chain (Figure 2.1, p. 34) cannot be restored from its social structure. Therefore, this role specific disruption strategy is only effective in the long run (after removing 18 actors), when the VC network is not able to replace the specialists of 'diverting electricity' any more (see Figure 4.6). Furthermore, the VC degree attacks seem to have the most disrupting effect on the network efficiency during the initial steps of the simulation. In summary, Figure 4.6 shows, counter intuitively, that when the criminal network recovers itself randomly from all five disruption strategies, the network becomes more efficient as compared to its previous state.

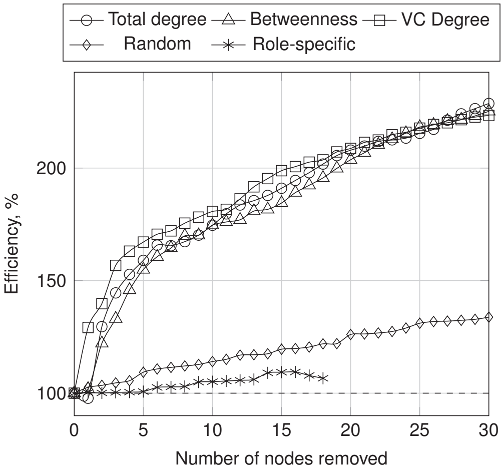


Figure 4.6 Efficiency of the value chain within the network using 'random recovery' during various law-enforcement strategies

In Figure 4.7 the results for the simulation of 'preference by distance' recovery are depicted. For this recovery mechanism the network efficiency does increase with a slightly lower rate in comparison to the previous case with random recovery due to the fact that fewer shortcuts appear in the network during the recovery process. These results show that if the network restores itself by finding replacements that are close, the VC disruption strategy will have the biggest impact on the network efficiency.

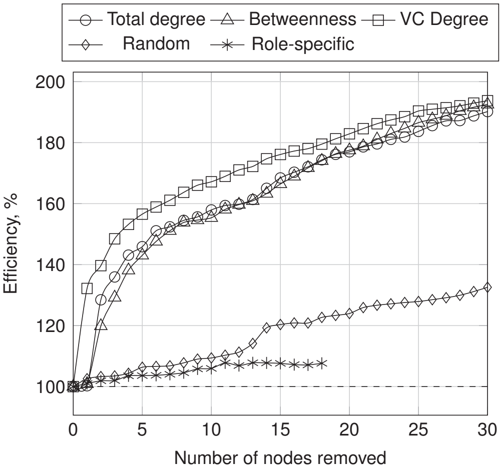


Fig 4.7 Efficiency of the value chain within the network using 'preference by distance' recovery during law-enforcement strategy simulations.

In Figure 4.8 the results for simulation with 'preference by degree' recovery are depicted. This means that the VC network prefers to replace someone by actors that are easiest to find, because they are more visible within the network. This recovery mechanism shows almost the same pattern as the preference by 'distance recovery' mechanism.

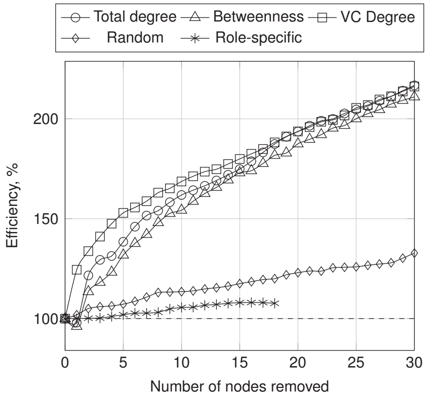


Fig 4.8. Efficiency of the value chain within the network employing 'preference by degree' recovery during law-enforcement strategy simulations.

In addition to these simulations, Figure 4.9 shows the roles that are removed from the network by applying three different disruption strategies ('Random' and 'Role-specific' strategies showed no relevant effects). This Figure indicates the difference in impact that the three interventions have on specific roles within the value chain. In accordance with criminal network theory, it shows that 'visible' roles like *taking care of the plants* and *transporting the product* are vulnerable to these network disruption strategies. In general these roles are directly involved in the value chain and as a result score high on degree centrality. But it is important to note that central key player roles, like *Coordinator, International trade* and *Financing* also seem to be highly affected. This implies that these central key players are not that much concealed in the criminal,network as was assumed in previous studies. Furthermore Figure 4.9 shows that 'specialist' roles, like '*diverting electricity*' and *'building plantation'*, are not affected by these strategies and are therefore the ones that might be protected within the network structure.

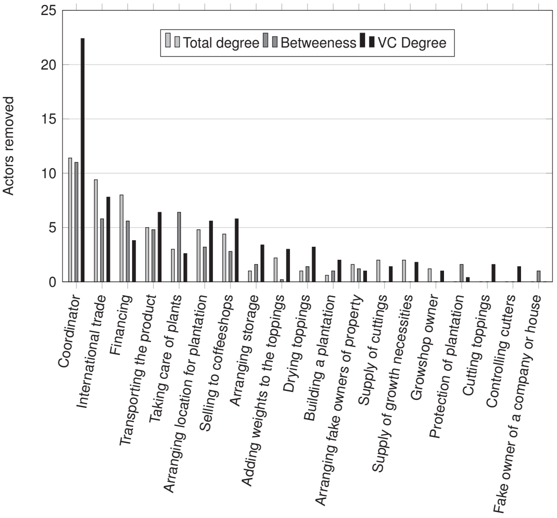


Fig 4.9 Roles affected by disruption strategies applied to a network with preferential recovery.

Figure 4.10 depicts what happens with the density (brightness) of value chain network G_{VC}, before and after applying the disruption strategies. It shows that the brightness of the value chain network actually *increases* as a consequence of intervention. This is a result of the fact that network members that try to continue criminal activities are forced to communicate efficiently as a result of the applied network disruption strategy. Hence in order to recover the value chain, these members have to act as brokers to establish new value chain relationships. Consequently, overall network density increases, and it becomes more redundant after each intervention, forcing the cannabis cultivation value chain network to expose itself increasingly from the dark.

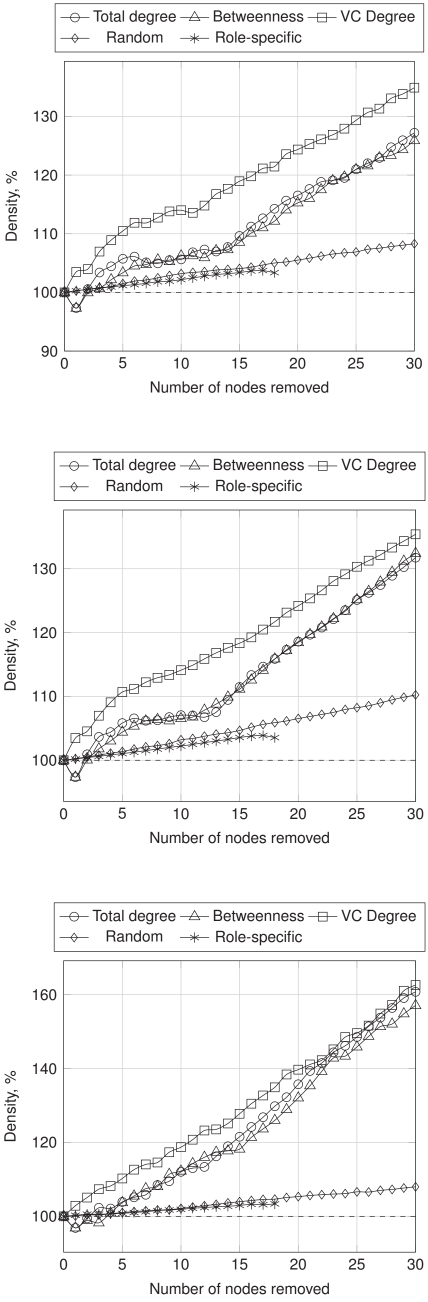


Figure 4.10. Difference in density of the overall network G_{VC} , after applying (a) strategies with random recovery, (b) preference by distance and (c) preference by degree recovery. Density is associated with brightness of the network, and is presented as a percentage relative to its initial value

4.5 DISCUSSION

In this paper we present the impact of dynamic network recovery on the effectiveness of four different criminal network disruption strategies. A unique dataset of a large complex criminal network involved in organized cannabis cultivation was the starting point for the simulation and analyses of these disruption strategies. In addition, three different network recovery mechanisms were investigated, in order to assess the effects on network structure in terms of network efficiency and security (i.e. higher connectivity is more visibility is less security)

Previous studies of criminal network resilience showed that coordinators try to keep a social distance from the actual flow of illicit goods within the value chain. These key players therefore limit their direct connections to actors involved in executive tasks, to minimize the risk of exposure (e.g. Baker & Faulker, 1993; Klerks, 2000; Dorn et al., 1998). Based on these studies, high scores for degree and betweenness centrality were expected for executive actors directly involved within the technical value chain of cannabis cultivation. This hypothesis is partly consistent with our observations for the roles of '*transport*' and '*taking care of plantation*' (see Figure 4.10), which are vulnerable to degree- and betweenness attacks. However, our results also show, that central key-player roles within the value chain of cannabis cultivation, such as '*coordinator*', '*financing*' and *'(inter)national trade'*, are highly visible and therefore vulnerable to degree centrality attacks as well (see Figure 4.4 and Figure 4.10). From an efficiency/security perspective, this implies that the structure of the observed cannabis cultivation network is very efficient and flexible, but rather insecure. Hence, if these key players become exposed, the whole value chain might become visible. How can this be explained? The answer to this question is concealed into two factors: a) specific features of the cannabis cultivation process b) the observed properties of the dataset.

Cannabis cultivation is a delicate process, involving many roles and functions. In order to bring these roles together at a certain time and place, the role of '*coordinator*' is essential for retaining the technical system of the value chain (Figure 4.2). To fulfill this role, information needs to be exchanged efficiently through the value chain network. Coordinators therefore need to occupy strategic hub or bridge positions within the network, naturally resulting in higher than average scores on degree and betweenness centrality observed within our data.

However, in practice this doesn't necessary make these actors easy targets for network disruption strategies that focus on high degree- or betweenness positions, since these vulnerable positions are also recognized by criminal networks themselves. Non-redundant and compartmentalized ways of communication are applied, keeping these central key players highly concealed from direct involvement within the value chain (Erickson, 1981); Baker and Faulker, 1993; Morselli et al., 2006; Ayling, 2009). As a consequence, reliable incriminating evidence of involvement of the direct involvement of these 'critical actors' within illegal markets and activities is harder to retrieve, as compared to actors directly involved within operational activities of the value chain. This explains why these actors can operate from the core of the network but stay concealed in the dark at the same time. However, this is still in contrast with the high levels of 'visibility' these key players seem to have as we observed from the data (see also Appendix 4A, p.122). An explanation can be found within the detailed properties of our dataset:

Empirical criminal network research is often based on a single source of data, such as closed criminal investigations (e.g. Klerks, 2001; Spapens, 2010; Kleemans et al., 2002). These datasets often contain detailed observations of the behaviors and roles of the suspects under investigation. However, due to limited resources and time, criminal investigations generally start off with a specified and restricted objective. Depending on this objective, the scope of data collection within these investigations is naturally confined by the jurisdiction, money or law enforcement capacity (Morselli, 2009). Because of these investigative boundaries, chances that powerful or influential actors become exposed within criminal investigation data are relatively low. To overcome this potential bias in our study, multiple data sources were combined to retrieve the final network representation. Some of the data-sources were criminal informants, who sometimes are part of the criminal activities themselves and operate as direct eyewitnesses for 'unknown' criminal cooperation. One of the initial goals of this specific intelligence process is deliberately discovering 'hidden' critical actors, who try to keep their identities concealed in the dark. These unique data properties offer us a different perspective on the criminal network structure, often hidden within data solely retrieved from criminal investigations. This offers another explanation for the visibility of the 'hubs' observed within our results.

We recognize that our dataset is not immune to missing data and boundary specification problems and we understand the difficulty involved with retrieving reliable criminal network data. But, interestingly our results emphasize the importance of '*no boundary*' intelligence gathering focused on criminal networks at a 'macro' level and the multiplicity of criminal relationships, for retrieving a better strategic understanding of the way these networks operate and react. Combining multiple sources of data on criminal cooperation seems to be essential in confining these data validity problems. The importance of a 'no boundary' intelligence gathering strategy, will be presented in chapter 5. Such a strategy opens the door for actually seeking rather than assuming criminal network structure. In addition, our study shows the importance of applying combinations of methods to unravel the complex dynamic network structures. The knowledge generated by combining social network analysis with computational simulation in this paper, might be of direct relevance for thinking about the effectiveness of control strategies of organized crime on an operational level.

Thinking ahead: introducing the notion of value chain centrality[27]

The analysis and simulations in this chapter inspired us to think ahead about new approaches to detect and disrupt criminal networks. We based the current approach on two notions of the importance of a criminal actor as a suitable target for network disruption:

1. **Structural importance**: the importance of an actor derived from its connectivity and positioning in the overall network. This is based on the structure and composition of an actor's ego network together with the structure and composition of the overall network.
2. **Valued importance**: the importance of an actor derived from the unique set of skills, knowledge or tools and actor possesses to fulfill a certain role or function in the criminal value chain. This is derived from the number of other actors in the overall network who may fulfill the same role or function. A low number of potential replacements means that an actor scores high on 'irreplacebility' and therefore gets more important for the network.

Actors that are important because of their structural importance can be identified trough quantitative measures of social network analysis (i.e. degree centrality for identification of hubs, betweenness centrality for identification of brokers, closeness centrality for identification of well-informed individuals). Actors that are important because of their valued importance are now measured by manual analysis. By analyzing the content of the data, actors could be labeled in a specific role and then be cherry-picked for targeting. For large criminal network datasets, this can become a very time-consuming exercise. With datasets growing in size, there is a need for quantitative methods measuring an actor's irreplaceability. However, topological measures such as degree centrality fail to incorporate qualitative data such as roles and skills. So are there any parameters that could serve as quantitative indicators for irreplacibility?

A paradigm that combines structural and valued features of networks is known as multiplexity, which refers to the fact that a connection between two actors can constitute multiple types of relationships. Some criminal ties represent a long lasting friendship, a family connection, and an essential connection between two phases in de production of

[27] With the consent of the senior author (G. Kampis), this paragraph was added as an edited copy of the published work: N. Toth; L. Gulyás; R.O. Legendi; P. Duijn; P.M.A. Sloot and G. Kampis: *The importance of centralities in dark network value chains*, The European Physical Journal - Special Topics, vol. 222, nr 6 pp. 1413-1439. 2013. ISSN 1951-6355 and 1951-6401, with only minor formatting done to fit the style of this manuscript.

illegal drugs at the same time. Others are of a more one-dimensional and instrumental nature, which may last just for the duration of one single criminal operation. Criminal networks therefore constitute of various levels of multiplexity across their structure. High levels of multiplexity are related to strong ties build on trust, whilst low levels are more related to weak ties.

Value chain data (i.e. actor role data) provides such an extra layer on top of the binary network data of who is involved with whom. The 'irreplaceability' of an actor in the network is mainly derived from the uniqueness of his or he role in the value chain. It also depends on how far away (i.e. social distance) a potential replacement could be found. Many value chains can run through the criminal network at the same time, some dependent but others independent from each other. They are however all connected within the overall network at various social distances from each other. In fact these different value chains form a value chain network related to a specific criminal market (e.g. cannabis production, human trafficking, money laundering). By projecting the value chains in one market together as an extra network-layer on top of the overall binary network structure, a 2-dimensional network structure can be inferred (see Figure 4.11).
The first binary dimension represents the networks topology and provides opportunities for information to flow across the edges to all of its nodes. In the example of Figure 4.11a information between nodes 1, 4 and 3 depends on node 2. This makes node 2 more structurally important then the other nodes. By removal of node 2 the network would collapse. The second dimension added in Figure 4.11b adds a purpose to the flow of information, i.e. completing a certain criminal offence consisting multiple steps or phases. In most cases this follows a sequential order. Hence, for illegal drugs to be packed and shipped it needs to be produced first. This second dimension therefore constrains the flow of information further. It provides direction in the way information, goods and money flows, and also through whom in the network. In the case of 4.11b node 1 and 2 posses unique positions since they are unique within there specific role. If they would be removed from the network, the purpose of the network would be disrupted. In real-life criminal networks consisting of hundreds or thousands of actors, the chances for presence of a potential replacement are of course much higher.

This example shows that such added multiplexity provides opportunities for identifying and quantifying 'irreplaceability'. This can be achieved by answering three important questions: (i) How many different value chains does a given node participate in? (ii) How far away is the next replacement node located following the overarching criminal network? (iii) How many acts of introduction are required to reconstruct a particular value chain? All three questions provide another notion (i.e. indicator) of irreplaceability:

i) Alignment membership

In criminal networks actors can fulfill a role in multiple value chains at the same time. The first notion of irreplaceability is therefore the number of possible value chains that a given node may be part of, i.e. the number of alignments that the node makes possible. On the operational level value chains can quickly shift between active or inactive according to the circumstances, such as law enforcement attention, accidents or availability of precursors. Over time however, criminals keep falling back to their most trustworthy contacts, who originate from the same pools of potential accomplishes. Such pools of potential cooperation remain more robust over time and are therefore more suitable for research or intelligence purposes. Our assumption is therefore that all possible alignments are active or potentially active.

In the definitions below *G* = (*V*,*E*) will denote the network with a set of nodes *V* and edges *E*. Each node *n* has a color *c* taken from a color set *C* and the colors of the nodes are given by c(*V*). A value chain *w* is a vector of *k* colors. Finally, G(*G*,*w*) is the set of all value chains *w* that can be realized on graph *G* given the coloring of the nodes c(*V*).

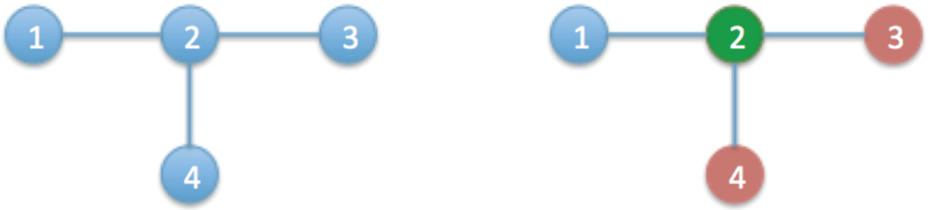


Figure 4.11: a) Representation of a binary 1-dimensional network topology of 4 nodes and 3 edges. b) Inference of a 2-dimensional network by projecting the value chain on top of the network topology. The colors represent the roles actors fulfill in the 3 successive phases (blue, green, red) of the criminal value chain.

Definition 1. *Alignment Membership*

$$\mu_1(\nu,\omega) = |\{\langle v_1 \cdots v_k\rangle \in \Gamma(G,\omega); \exists i \in [1,k]: v_i = v\}| \text{ for } \forall \nu \in V.$$

This concept is illustrated in Figure 4.11b. The depicted graph has four nodes that are colored by three colors. Assuming that the value chain is the following: ω = < *blue,green,red* >, node 1 is part of two alignments, < 1,2,3 > and < 1,2,4 >.

ii) Distance of replacements

Our next centrality notion will consider how much damage a node's removal may cause in the active value chains (i.e., alignments). To assess this, we consider the distance to the closest replacement (i.e., the closest replacement node with the same color).

Definition 2.*Closest Replacement Node*

$\rho(\upsilon) = u \in V$ such that $C(\upsilon) = C(u)$ and $\delta(\upsilon, u) = min\{\delta(\upsilon, t) | t \in V, C(\upsilon = C(t)\}$, where $\delta(\upsilon, u)$ is the shortest distance between nodes *u* and *n* or ∞ if *n* is unreachable from *u*.

Definition 3. *Distance of Replacements*

$$\mu_2(\nu, \omega) = \mu_2(\nu) = \delta(\upsilon, \rho(\upsilon))$$

Remark 1. The closest replacement of a node is not necessarily unique. However, the distance of replacements is.

Remark 2. Notice that this centrality measure is independent of the value chain at hand. It only depends on the coloring of the graph.

Remark 3. If node v has no replacement in the network, by definition, $\mu_2(v) = \infty$. This corresponds to the natural interpretation that node v is indispensable.

As an illustration, let us revisit Fig. 4.11b. Since node 1 is the only blue node in the network, its centrality will be ∞. The same is true for node 2. Node 3 and 4, however, have the same color and are thus (the closest) replacements of one another: ρ*(n3) = n4 and* ρ*(n4) = n3*. Since their mutual distance is 2, *μ2(n3) = μ2(n4) = 2*.

iii) Introduction distance

Our third and last centrality measure elaborates on the ideas of the previous definition. We want nodes to score high if their replacement is difficult. However, in this case, we assume that the search for replacement happens inside the network (using existing connections). That is, after the removal of the node in question, the nodes preceding it and following it in the value chain (alignment) will independently look for another node with the same color, exploring the network's social structure. The motivation here is that we are dealing with a clandestine network where a publicly announced or "global search" for a replacement can be infeasible.

Within dark networks, trust is essential in order to prevent secret information about illegal activity from being leaked outside the circle of people involved. Therefore, involving a replacement with this information is a risky business. Dark network members usually seek replacements within the close by regions of their own social and criminal network (e.g., friends, family). The further away of the personal social network a replacement is found, the more risk is being taken. Therefore, social distance within the network is an important estimate of the riskiness of the replacement for the value chain member (Coles, 2001; Kleemans & Van de Poot, 2008; McCarthy et al., 1998)

For our new centrality measure, we will assume that members of the value chain who lost their connection (preceding or succeeding member) will ask their neighbors (and nobody else) for a suggestion of a replacement. If a replacement is not directly available, the neighbors will ask their own neighbors and so on. The replacement process is completed when the preceding and the succeeding nodes find a replacement that can perform the same task (i.e., node with the same color). We are interested in the minimum number of steps (i.e., "introduction events") that are needed to accomplish this. Naturally, to replace nodes at the start or at the end of the value chain (alignment) only one alignment neighbor will need to find the replacement.

In network terms, we are interested in the sum of distances from the preceding node in the alignment to the replacement and from there to the succeeding node. To be more consistent with the "introduction" concept, we will subtract 1 from each distance: a node introduces two of its neighbors, thus one "introduction event" connects the nodes at two steps' distance. It is important to emphasize however, that the distances are calculated after the removal of the examined node. (The act of removal may disrupt possible paths.)

Since the same nodes can be part of several alignments, there will be an introduction score for each of these value chain instances. Since all of these alignments could be disrupted if an actor with unique skills is removed from the value chain, all alignments need to be restored. Therefore the introduction distance of the node is calculated by the sum of these scores for this paper. Alternatives could be the average, minimum, or maximum introduction distance. Empirical testing of these models could provide the necessary information for how to fine-tune this metric.

Let $\bar{\delta}_v(u,t)$ denote the distance between *u* and *t* after the removal of *v* (and its links) or ∞ if there is no replacement. We continue by defining the first replacement that node *u* finds for node *v* after its deletion.

Definition 4. *First replacement for v from u*

$\varrho(u,\nu) = t \in V$ such that $C(v) = C(t)$ and $\bar{\delta}_\nu(u,t) = min\{\bar{\delta}_\nu(u,s) \middle| s \in V, C(v) = C(s)\}$.

Definition 5.*Introduction Score*

$$\lambda(\nu,\gamma) = \begin{cases} \bar{\delta}_\nu\big(\gamma_2, \varrho(\gamma_2,\nu)\big) - 1, & \text{if } \nu = \gamma_1 \\ \bar{\delta}_\nu\big(\gamma_{k-1}, \varrho(\gamma_{k-1},\nu)\big) - 1, & \text{if } \nu = \gamma_k \\ \bar{\delta}_\nu\big(\gamma_{i-1}, \varrho(\gamma_{i-1},\nu)\big) + \bar{\delta}_\nu\big(\gamma_{i+1}, \varrho(\gamma_{i+1},\nu)\big) - 2, & \text{if } \nu = \gamma_i, i \in [2, k-1] \end{cases}$$
$\nu \in V, \gamma \in \Gamma(\nu,\omega)$.

Remark 4. The first replacement for v from u is not necessarily unique. However, the introduction score is.

Definition 6.*Introduction Distance*

$\mu_3(\upsilon,\omega) = \sum_{\gamma \in \Gamma(G,\omega), \nu \in \gamma} \lambda(\nu,\gamma)$.

Remark 5. Notice that while the *closest replacement* value was independent of the value chain and only depended on the graph's coloring, introduction distance is intimately connected to the value chain.

As said before, in the graph on Fig. 4.11b, nodes 1 and 2 have no replacement. Thus their introduction distance will be *μ3(n1) = μ3(n2)* = ∞. Nodes 3 and 4 are, on the other hand, the replacements of each other. Since both of them are directly connected to node 2, their introduction distance will both be *μ3(n3) = μ(n4) = 0* (i.e., no introduction events are necessary).

Remark 6. There is a distinction between the technical system of the value chain and the social system of the value chain (Gottschalk, 2009). The technical system consists of all the sequential production steps in order to produce an illegal product. The social system consists of all criminal relationships, but also other relationships (e.g. friendship, other criminal activity) that link the value chain members involved within these different production steps together. It might be that a person in step 1 is socially connected to a person involved in step 5 or 8. So the technical system explains the flow of goods and the flow of people, where the social system explains the flow of information. This means that in case of replacements, all nodes within a single value chain might seek a replacement instead of only the 'orphaned' ones. However, due to its complexity this option is not explored in the present paper. In further exploration of these metrics such complexity may be included

Remark 7. The minimum and maximum possible values of the introduced centralities are the following:

$$\min\left(Dom_{\mu_1}\right) = 0$$
$$\min\left(Dom_{\mu_2}\right) = 1$$
$$\min\left(Dom_{\mu_3}\right) = 0$$
$$\max\left(Dom_{\mu_1}\right) = \eta = max_{c \in C_w} \prod_{d \in C_w \setminus c} |\{v \in V | c(v) = d\}|$$
$$\max\left(Dom_{\mu_2}\right) = \begin{cases} \infty, & \text{when there is a color that is only assinged to a single node} \\ l_{max}, & \text{otherwise} \end{cases}$$

where l_{max} is the longest shortest path between connected node pairs in G.

$$\max\left(Dom_{\mu_3}\right) = \begin{cases} \infty, & \text{when there is a color that is only assinged to a single node} \\ & \text{or when the network becomes disconnected} \\ \eta(l_{max} - 1), & \text{otherwise} \end{cases}$$

In the calculation of the maximum value for μ_1, we need to estimate the maximum number of alignments a node can take part of. For this, we take the colors of the value chain, except the color of the node in question. We count how many nodes of the network have each of the colors and multiply these values. This is an upper bound for the possible number of alignments the node can be part of in the given colored network. To get η, we pick the color in the value chain that yields the highest multiplied value.

For a statistic comparison of these value chain centrality scores with traditional centrality scores on theoretical networks we would like to refer further to our research paper on which this paragraph is based (see Toth et al., 2013). By using the Spearman rank correlation we found in this additional analysis that these three new notions of value chain centrality provide new insights in network positioning as compared the traditional notions. The next step is to apply these models to empirical criminal networks and compare it's application with the manual analysis of multiplexity. At the more abstract, theoretical level, we are interested in studying such graphs in the future, where the color distribution is non-uniform, or where the nodes may have more than a single color. Moreover, we also plan to study value chains that have more complex structures, i.e., allowing for branches and repetitions, such as observed in real systems.

4.6 CONCLUSION

The aim of this study is to unravel the dynamics of resilience within criminal networks, as a consequence of network disruption. Based on the numerical studies of four different disruption strategies and three different recovery mechanisms presented here, it can be concluded that disruption of the criminal cannabis network is relatively ineffective.

After applying multiple removals of actors the network efficiency is hardly affected. On the contrary, efficiency actually *increases* over time for the value chain degree disruption strategy, as a direct result of efficient network recovery. It was shown that the integration of a replacement within the network leads to new shortcuts, which in turn reduces overall dimensionality. Our results point out that a delicate criminal process, such as cannabis cultivation, is organized in a flexible and adaptive network structure, which is highly resilient against network disruption.

In part these results can be explained by the natural evolution of these criminal networks over time. As reciprocal connections within the embedding macro-network expand over time, existing connections between value chain members might have become sub-optimal. However, if the value chain itself is still functional, these 'inefficient' connections within the value chain configuration might not cause any problems for a criminal value chain to evolve. In fact, they might even increase security within the value chain, by naturally shaping the network in non-redundant way. Within these settings, chances are that in search for a replacement non-redundant value chain connections become optimized (redundant), leaving the network more efficient then in its previous state.

Previous criminal network studies attribute this phenomenon to a 'snowball effect', by which 'structural holes' between different criminal subnetworks dry out by increasing reciprocal social relationships over time (e.g. friendship, kinship, affective) (Granovetter, 1983). As new illegal opportunities for criminal network expansion emerges, this process starts all over again leading to further network expansion (Kleemans & Van de Bunt, 1999). According to this interpretation, our results emphasize that interference in an established 'old' value chain network will be less effective than intervening in a recently established criminal network or value chain. In fact, the best way to disrupt a criminal network might be not to apply any disruption strategy at all.

These conclusions might sound disturbing for government- and law enforcement that fight to control criminal networks on a daily basis. However, we need to realize that network effectiveness depends on both efficiency as well as secrecy. The capability of criminal networks to organize secrecy after an attack depends on the flexibility of the network to benefit both from the redundancy as well as the non-redundancy that's inhabited within its network structure, according to the circumstances. Redundancy is needed when looking for trustworthy replacements within the embedding network. In addition, non-redundancy is essential for finding replacements that are difficult to find at a greater social distance and for keeping critical roles and information differentiated and secret, in order to prevent revealing the whole network by one arrest. From this perspective, Fig 11 shows that the number of actors close to the average degree centrality increases, meaning that also '*not* *so well-connected*' actors will become more visible than before disruption strategies were applied. This means that after every attack the criminal network becomes more and more redundant. Forcing the network to become efficient, but at the price of a higher visibility (brightness), the network becomes less 'dark'. The criminal network might even become imbalanced, leading to progressively more exposure after replacements are integrated within its structure.

From a network resilience perspective, overall network exposure increases the risk to reveal the critical actors for value chain survival, such as specialists from which multiple criminal value chains have become dependent. Because these specialists are underrepresented within the macro-network, these roles are hard to replace. Moreover replacing specialists demands direct interference of central brokers (coordinators) within the value chain, leading to even more exposure of these strategic network positions. In this sense, our results indicate that network disruption causes these networks to become more efficient at first, but rather ineffective in the end as recovery forces them to light up more and more from the dark.

This increased visibility might induce a serious change within agencies involved in contemporary law enforcement control of organized crime, as new opportunities for surveillance and advanced intelligence gathering arise to identify and target more critical actors, specialists or even potential future replacements. With this strategy, the network resilience progressively declines and additional cracks within network structure will emerge in the long run, offering more specific disruption opportunities in the end. Our results emphasize the importance of considering these criminal network structures within their complex adaptive dynamics, instead of focusing on a snapshot of a group at a certain point in time. In practice this means that disrupting a criminal network demands a long-term consistent intervening effort.

In this chapter we demonstrated how computer simulation in combination with SNA provides understanding of the complex macroscopic dynamics that fuel the resilience of criminal networks against network disruption at a micro-level. The use of such methodology within the criminological research field is however in its infancy. One reason lies within a lack of access to reliable criminal network data by scientific researchers. Until law enforcement agencies have been willing to create a legal- and technical framework by which disclosed databases could be made accessible for scientific purposes, scientists need to rely on their creativity to obtain empirical illicit network data. In the next chapter we demonstrate how the techniques of web crawling and text scraping can contribute to the inference of hidden community networks (i.e. drugs networks) from the openly accessible

online world. This methodology may also provide law enforcement professionals with a methodology to create a deeper data-driven understanding of the social dimensions behind illicit networks outside of the law enforcement context.

REFERENCES

Albert, R., Hawoong J., Barabási A., (2000). Error and Attack Tolerance of Complex Networks. *Nature* 406, 378–382.

Ayling, L., (2009). Criminal Organizations and resilience. *International Journal of Law Crime and Justice* 37, 182–196.

Baker, W.E., Faulkner, R.R., (1993). The social organization of conspiracy: illegal networks in the heavy electrical equipment industry.*American Sociological Review* 58, 837–860.

Bakker, R.M., Raab, J., Brinton Milward, H. (2012). A Preliminary Theory of Dark Network Resilience. *Journal of Policy Analysis and Management*, Vol 31, No. 1 33-62

Bienenstock, E.J.,Bonacich, P., (2003). Balancing efficiency and vulnerability in social networks. Dynamic social network modeling and analysis: *Workshop summary and papers*, 253–264. Washington, DC: The National Academy of Sciences.

Borgatti, S.P., (2003). The Key Player Problem. Dynamic Social Network Modeling and Analysis: *Workshop Summary and Papers*, R. Breiger, K. Carley, & P. Pattison, (Eds.) National Academy of Sciences Press, 241–252.

Borgatti, S.P. (2006). Identiying sets of key players in a social network. *Computational and Mathematical Organization Theory*, 12(1), 21-34.

Bouchard, M., (2007).On the resilience of illegal drug markets. *Global Crime* 8 (4), 325–344.

Bouchard, (2007b). M. A capture-recapture derived method to estimate cannabis production in industrialized countries. *First annual conference of the International Society for the Study of Drug Policy*, Oslo, Norway.

Burt, R.S., Joseph, E.J. & James, T.M. (1998). Personality correlates of structural holes. *Social Networks*, 20. 63-87.

Burt, R.S., (2001). Structural holes versus network closure as social capital. In N. Lin, K.S. Cook & R.S. Burt (Eds.). *Social Capital: Theory and Research* (pp.31-56). New Brunswick: Transaction Punblishers.

Cook K. and Burt R. S. (2001) *Social capital: Theory and Research*. New York: Aldine de Gruyter, 2001, 31–56.

Carley, K.M., Ju-Sung, L., D. Krackhardt, (2002). Destabilizing network. *Connections* 24(3), 79–92.

Carley, K.M., Dombroski, M., Tvetovat, M., Reminga, J., Kamneva, N., (2003). Destabilizing Dynamic Covert Networks. *In Proceedings of the 8th International Command and Control Research and Technology Symposium*.

Clauset A., Shalizi C.R., Newman M.E.J., (2009). Power-law distributions in empirical data.*SIAM Review*51(4), 661–703.

Coles, N., (2001).It's not what you know, but who you know that counts: Analyzing criminal crime groups as social networks. *British Journal or Criminology* 41, 580–594.

Cornish, D.B., (1994). The Procedural Analysis of Offending and Its Relevance for situational prevention.R. Clarcke (Ed.) *Crime Prevention Studies* 3, 151–196.

Czaplicka, A., Holyst, J. A. & Sloot, P. M. A. (2013) Noise enhances information transfer in hierarchical network. *Nature Scientific Reports***3,** 1223. (DOI: 10.1038/srep01223)

Decorte, T., (2010).The case of small-scale domestic cannabis cultivation. *Int J. of Drug Policy***21**, 271-275

Dorn, N., Oette, L. & White, S., (1998). Drugs Importation And The Bifurcation Of Risk: Capitalization, Cut Outs and Organized Crime. *Brit. J. of Criminology***38**, 537-560

Emmet, I. & Broers, J. (2008). *The Green Gold. Report of a Study of the cannabis sector for the National Threat assessment of Organized Crime*. Zoetermeer: KLPD-IPOL.

Erickson, B. , (1981). Secret societies and social structure, *Social Forces***60**, 188-210

Europol (2011).“*OCTA: EU Organized Crime Threat Assessment*”. European Police Office, Hag, Nederland.

Freeman, L. C., (1979). Centrality in social networks conceptual clarification. *Social networks***1**, 215-239

Granovetter, M., 1983.The strength of weak ties: a network theory revisited. *Sociological Theory* 1, 201–233.

Gottschalk P., 2009. Value configurations in organized crime. *Policing & Society* 19 (1), 47–57.

Holme, P., Beom, J. K., Chang, N. Y.,Seung, K. H., (2002). Attack Vulnerability of Complex Networks. *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physics* 65(5).

Hun, D., Kaza, S. Chen, H.,(2009). Identifying Significant Facilitators of Dark Network *Evolution. Journal of The American Society for Information Science and Technology* 20(4),655–665.

Milward, H.B.,Raab,J., (2006). Dark Networks as Organizational Problems: Elements of a *Theory. International Public Management Journal* 9(3), 333–360.

Kleemans, E.R., Brienen, M.E.I. & Bunt, H.G. van de (2002). *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC monitor.* Den Haag: BJU. http://www.wodc.nl

Kleemans, E.R.,De Poot,C. J.,(2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology* 5, 69–98

Klerks, P.P.H.M., (2000). *Big in Hash: theory and practice of organized crime* Antwerpen: Samsom en Kluwer Rechtswetenschappen.

Klerks, P. (2001). The network paradigm applied to criminal organizations. *Connections, 24*, 53-65.

Kossinets, G., Watts, D.J., (2006). Empirical Analysis of an Evolving Social Network. *Science* 311, 88–90.

Krebs, V.E., (2001).Mapping networks of terrorist cells. *Connections* 24(3), 43–52.

Lauchs, M.A., Keast, R.L., Chamberlain, D.,(2012). Resilience of a corrupt police network: the first and second jokes in Queensland. *Crime, Law and Social Change* 57(2), 195–207.

Liben-Nowell, D., Kleinberg, J.,(2007).The link predictionproblem for social networks. *Journal of the American Society for Information Science and Technology* 58(7),1019–1031.

Lindelauff, R.,Borm, P.,Hamers,H.,(2011). Understanding Terrorist Network Topologies and Their Resilience Against Disruption.Counterterrorism and Open Source Intelligence

Lecture Notes in Social Networks 2, 2011, 61–72.

Malm, A., Nash, R. & Vickovic, S., (2011). Co-offending networks in cannabis cultivation. *World Wide Weed: Global Trends in Cannabis Cultivation and Its Control***127**, McCarthy, B., Hagan, J.,Cohen, L.,(1998).Uncertainty, Cooperation, and crime: Understanding the Decision to Co-offend. *Social Forces* 77(1), 155–176.

Memon N., Larsen, H. L.,(2006). Structural Analysis and Destabilizing Terrorist Networks. *Conference on Data Mining DMIN'06*, 296–302.

Moiseyev, A., Solberg, B., Michie, B., Kallio, A.M.I. (2008) Modeling the impacts of policy measure stop revent import of illegal wood and wood products. *Forest Policy and Economics* 12(1), 24–30.

Morselli, C., (2001).Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade. *Crime, Law and Social Change* 35, 203–44.

Morselli, C., Giguère, C., Petit, K.,(2006). The efficiency/security trade-off in criminal networks. *Social Networks* 29(1), 143–153.

Morselli, C. & Petit, K. Law enforcement disruption of a drug importation network. *Global Crime***8 (2)**, 109 – 130 (2007).

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

Morselli, C., (2010). Assessing vulnerable and Strategic positions in a criminal network. *Journal of Contemporary Criminal Justice* 26(4), 382–392.

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

Newman, M.E.J, (2005). Power laws, Pareto distributions and Zipf's law. *Contemporary Physics* 46(5), 323–351.

Peterson, M.,(1994). *Applications in Criminal Analysis: A Sourcebook*. Westport: Greenwood Press.

Potter, G. R., Bouchard, M. & Decorte, T., (2011). The globalization of cannabis cultivation. *World Wide Weed: Global Trends in Cannabis Cultivation and Its Control.* 1-20.

Raab, J. & Milward, H.B., (2003). Dark Networks as Organizational Problems: Elements of a Theory. *J. of Publ. Administr. and Theory***13(4)**, 413 - 439

Roberts, N., Everton, S.F., (2011). Strategies for combating dark networks. *Journal of social structure* 12.

Robins, G., (2008). Understanding individual behaviours within covert networks: the interplay of individual qualities, psychological predispositions, and network effects. *Trends in Organized Crime* 12, 166–187.

Spapens, T., (2010). Macro networks, Collectives, and Business Processes: An integrated approach to Organized Crime. *European Journal of Crime, Criminal Law and Criminal Justice* 18, 185–215.

Spapens, T., (2011).Interaction between criminal groups and law enforcement: the case of ecstasy in the Netherlands. *Global Crime* 12(1), 19–40.

Sparrow, M. (1991), The Application of Network Analysis to Criminal Intelligence: an Assessment of the Prospects', *Social Networks* 13: 251- 274.

Schwartz, D. M. & Rouselle T. D. A., (2009). Using social network analysis to target criminal networks. *Trends in Organized Crime***12**: 188- 207

Tsvetovat, M.,Carley, K.C., (2005).Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence. *Institute for Software Research*. Paper 43. Available at:http://repository.cmu.edu/isr/43.

Tsvetovat, M., Carley, K.C.,(2003). Bouncing back: Recovery mechanisms of covert networks.NAACSOS Conference, Pittsburgh, PA, June 22-25, 2003, Day 3, Electronic Publication. Available at: http://www.casos.cs.cmu.edu/events/conferences/2003/proceedings.html.

United Nations Office on Drugs and Crime, (2010).*The globalization of crime: A transnational organized crime threat assessment*. United Nations publication, Vienna.

Van Calster, P., (2008). Netwerkonderzoek als perspectief op georganiseerde criminaliteit. *Justitiele verkenningen*, 34(5).

Watts, D.J.,Strogatz, S.H., (1998). Collective dynamics of small world networks. *Nature* 393(6684), 440–442.

Wouters, M. ,(2008). Controlling cannabis cultivation in the netherlands. In: Korf, D. J. (ed.) *Cannabis in Europe: dynamics in perception, policy and markets.* Lengerich: Pabst Science Publishers.

Xu, J.,Chen, H., (2008). The Topology of Dark Networks. *Communications of the ACM* 51: 58–65.

VPRO. http://www.youtube.com/watch?v=ZbFGrq9mWmU (date of access: December 17, 2013).

APPENDIX 4A: DESCRIPTION OF HARD- AND SOFT- DATASETS

The dataset used for our simulations consists of two data sources. First dataset consists of the data collected by criminal intelligence operations and criminal investigations. Because it is harder to estimate the reliability of this data, we call it soft data. The second dataset consists of arrest record data and is denoted as hard data.

Soft dataset information

The soft data is collected over the period January 2008 – January 2012 within a criminal intelligence unit. Detectives collected this data by systematically gathering intelligence from criminal informants, who are often part of the criminal network themselves or the social network surrounding it. We call this data 'soft' information. Criminal informants have different motives to talk to the police that are not always clear and their identities stay covered for security reasons. In some cases, this makes it difficult to check the facts. In order to check the facts detectives write a detailed report after every conversation. The facts written in these reports are checked by other informant intelligence and other police data sources, such as criminal investigations data or street police reports. If informants turn out to be unreliable, they are 'fired'. In addition to intelligence retrieved from criminal informants, this dataset also consists of information from closed criminal investigations and observations from street police officers during their duty. The data therefore contains detailed information on criminal cooperation and individual roles and criminal activities of the actors within the criminal network we observed.

After processing the reports police obtain information about records such as:
- Person (anonymous)
- Link Person – Registration (Soft)
- Link Person – Person

This kind of data has various aspects that contribute to its usefulness:

Strengths:
- Data is retrieved from criminals themselves within the social context of the criminal network. This gives us a unique observation of a criminal network.
- The data is checked with other information (police registrations) and has an indication on the value and importance detectives give to the information.
- The data also consists of person – person link records and detailed information about individual cooperation, roles and criminal activities.

Weaknesses:

- The dataset is in part selective; There is a reasonable possibility that there are some blind spots within the criminal network we do not know about, because we don't have any informants within these networks. Another point of concern is that data collection is affected by police priorities. Fortunately cannabis cultivation has been a top priority over the period our data was collected.

Not every informant is reliable. Not all facts that are written within the intelligence reports can be checked. This might be a risk if we want to look at only one criminal relationship on a micro level. For our research we are only interested in the network on a macro level, therefore our results won't be affected by one or two false reports. Moreover, informants that turn out to be unreliable, are fired directly, this results in a kind of natural selection of the best informants.

Hard (arrest) dataset information

The dataset on arrest information consists of persons with a police arrest registration dating from the period 2008 until 2011 (80.000 records) within the police region of The Hague. Every police suspect has a unique number and is put into a police database with a link to his or her arrest registrations. Every registration contains tag indicating the date when and the law article for which the suspect was arrested. If more than one person was arrested they are all linked to the same registration. Because of this, by connecting persons linked to the same arrest registrations, it was possible to recover the hard network structure. This offered us another perspective of the criminal network. Since this data was retrieved from police officers themselves, it is highly reliable. This means that personal identity is being checked on the bases of identification. Unfortunately arrest registrations do not contain lot information. It consists of the date and the law article for which a suspect was arrested. In addition to our cannabis cultivation network under observation, there are arrest registrations for Opium 1 (cocaine, heroin, XTC) and Opium 2 (soft drugs, almost always cannabis and hash).

After processing the reports, the police obtain information about records such as:

- Person
- Criminal card
- Registration (arrest) for Opium (hard and soft)
- Link Person – Registration (Arrest)
- Link Person – Criminal card
- Link Person – Person

Strengths:

- The data is reliable in that its observed and collected by police officers themselves

- It contains many records over time (2008 -2011)

Weaknesses:

- Less content on the nature of relationships between two suspects in relation to the crime.
- As key players and facilitators stay as covered as possible, chances are that less important criminals are overrepresented within this dataset.

Featured properties of database

We studied a cumulative dataset of persons involved in criminal activity built with arrests registrations and informants data that contains 85192 records. Not all criminals were participating in organized crime; therefore most of them are not a part of criminal network. In Figure A1 we depict the overlap between hard- and soft- data connections within the network.

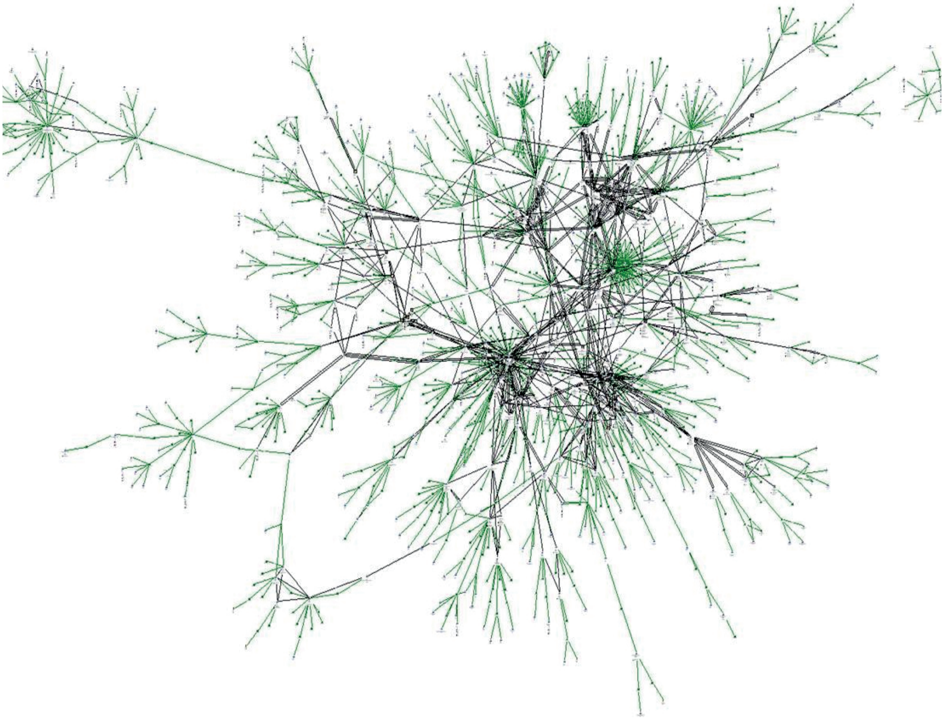


Fig. 4A1. Example of the overlap between hard and soft data connections within the network. The black lines correspond with soft data connections. The green lines correspond with hard data connections.

In Table A1 the distribution of ages between genders and a summary of gender populations is listed. Not all records in the database have information on gender and age of criminals, but most of them have.

Table A1. Gender and age distribution in cumulative hard and soft records database

Age interval// Gender	10-19	20-29	30-39	40-49	50-59	60-69	70-79	80-89	90-99	100-109	Total Amount
Male	5185	19810	14708	13455	8432	4029	1203	301	53	4	**67180**
Female	1485	4660	3139	3046	2069	944	343	96	34	0	**15816**

The data in Table A2 describes the distribution of person records by the countries of origin. The triad that gives the biggest contribution to the cannabis criminal situation is The Netherlands, Suriname and Turkey.

Table A2. Distribution of person registrations by country of origin

Country of origin	Number of actors↓	Country of origin	Number of actors	Country of origin	Number of actors
Nederland	45253	Tunisia	157	Canada	37
Suriname	4405	China	141	Syria	37
Turkey	2878	Romania	127	Germany	36
Morocco	2846	Iraq	113	South Africa	33
Netherlands Antilles	2384	USA	105	Ukraine	33
Poland	2240	Panama	99	Hong Kong	32
Bulgaria	791	Algeria	96	Italy	32
Sudan	446	Yugoslavia	81	Angola	30
Namibia	444	Indonesia	77	Lebanon	30
Iran	425	Liberia	70	USSR	27
Afghanistan	391	Russia	61	Australia	25
Great Britain	290	Kuwait	52	East Germany	23
Colombia	252	Turks and Caicos Islands	51	Congo	22
Dominican Republic	241	Egypt	50	Rwanda	22
Ethiopia	222	Cape Verde	45	Hungary	21
India	207	Nigeria	44		
Ghana	204	Aruba	43		
Pakistan	186	Belgium	40		
Somalia	165	Mongolia	40		
Lithuania	160	Thailand	38		