Erasmus
School of
Law

Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness

E. Rutger Leukfeldt[1], Edward R. Kleemans[2], Edwin W. Kruisbergen[3] and Robert A. Roks[4]

[1]Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and The Hague University of Applied Sciences, De Boelelaan 1077a, 1081 HV Amsterdam, The Netherlands

[2]Vrije Universiteit Amsterdam, De Boelelaan 1077a, 1081 HV Amsterdam, The Netherlands

[3]Scientific Research and Documentation Centre, Dutch Ministry of Justice and Security, PO Box 20301, 2500 EH Den Haag, The Netherlands

[4]Erasmus University Rotterdam, PO Box 17383000 DR, Rotterdam, The Netherlands

Erasmus University Rotterdam

ABSTRACT

This article presents the results of empirical analyses of the use of information technology (IT) by organized crime groups. In particular, it explores how the use of IT affects the processes of origin and growth of criminal networks. The empirical data presented in this article consist of 30 large scale criminal investigations into organized crime, including traditional organized crime, traditional organized crime in which IT is an innovative element, low tech cybercrimes and high tech cybercrimes. Networks involved in cybercrimes or traditional crimes with an innovative IT element can be characterized as a mixture of old school criminals that have a long criminal career, and a limited number of technically skilled members. Furthermore, almost all cases have a local dimension. Also the cybercrime cases. Dutch sellers of drugs on online marketplace, for example, mainly work for customers in the Netherlands and surrounding countries.

Keywords: Organised crime, Cybercrime, Cryptomarket, Criminal network

Erasmus University Rotterdam

INTRODUCTION

325 The increased use of the internet and Information Technology (IT) provides new opportunities for committing crime. The internet is opening up a new world, for the general population as well as for criminals. However, there has so far been only a limited amount of empirical research into how offenders use IT in their daily routines and the consequences of IT for the way in which offenders operate. The use of the internet, and IT in general, raises several questions in relation to organised crime (see, for example, Leukfeldt 2017), particularly when existing knowledge, concepts, and theories in the field of organised crime are linked to new forms of crime, such as cybercrime, or when new technology is used in traditional organised crime (see, for example, Töttel et al. 2016; Leukfeldt et al. 2017a). One interesting question is what the use of IT means for the ways in which criminal collaboration emerges and develops. It is well known, for example, that social capital is of great importance for participation and success in organised crime; in order to be successful in organised crime, you need to know the right people (producers, customers, enablers, etc.). Until now, social capital has primarily been about human relationships in the offline world (see, for example, Bouchard and Morselli 2014, Edwards and Levi 2008, Kleemans and van de Bunt 1999, Morselli 2005). However, the digitisation of society, and particularly the internet, is opening up new horizons, at least in theory (see, for example, studies into online criminal meeting places: Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2012; Holt and Smirnova 2014; Décary-Hétu and Dupont 2012; Décary-Hétu et al. 2012; Dupont et al. 2016; Leukfeldt et al. 2017b, d). Physical and other boundaries now do not longer necessarily form an obstacle to coming into contact with capable co-offenders and enablers. Has, therefore, the importance of social capital, 'knowing the right people', gradually decreased in favour of 'knowing your way on the web (or the dark web)' (see also Lavorgna 2013; Przepiorka et al. 2017)? And do the processes of origin and growth of 'cyber networks and cyber offenders' differ from the mechanisms that are important for the general offender population?

This article focuses on the question of the extent to which, and how, the increased availability and use of IT has led to changes in the ways in which offenders cooperate. This article goes beyond current studies by not solely focussing on offline crime or cybercrimes alone, but by exploring the use of IT and its consequences for a broad range of traditional organised crime and cybercrime cases. The article is based on a Dutch report on the 30 most recent cases from the fifth data collection wave of the Dutch Organised Crime Monitor, an ongoing research project into the nature of organised crime in the Netherlands (Kruisbergen et al. 2018). It starts with an overview of traditional organised crime ("Traditional organised crime: findings from the Dutch organised crime monitor" section), followed by an overview of the literature on cybercriminal networks ("Cybercriminal networks: a review of the

literature" section) to establish what we know from previous empirical research about criminal cooperation in organised crime, and the extent to which the literature on cybercrime provides the same or a different picture. Next, the research methods are described ("Data and methods" section) and the empirical results regarding origin and growth processes are presented ("Results" section). The article ends with conclusions and a discussion ("Conclusion and discussion" section).

TRADITIONAL ORGANISED CRIME: FINDINGS FROM THE DUTCH ORGANISED CRIME MONITOR

Structure and composition

326 The structure and composition of organised crime groups has been heavily debated and intensively researched, particularly since Donald Cressey (1969) described organised crime as a more or less formal bureaucracy in his book 'Theft of the Nation': organised crime as a pyramid-shaped organization, with a strict hierarchy, a clear division of tasks, codes of conduct, and an internal and external sanctioning system. Early critics (e.g. Albini 1971; Ianni and Reuss-Ianni 1972; Smith 1975) fiercely criticised this conceptualization of organised crime and a large body of empirical research found no evidence for this conception, rather the contrary. On the one hand, empirical researchers concluded that, under very specific conditions, some large criminal organizations have emerged and existed for a long period of time, such as the Sicilian Mafia, the Japanese Yakuza, the Hong Kong Triads, and the Russian Mafia (see, e.g. Paoli 2003, Varese 2011). However, these structures do not resemble formal bureaucracies, as suggested by Donald Cressey. On the other hand, these large criminal organizations turn out to be the exception rather than the rule. Offenders operating in contemporary local illegal markets in developed countries with a 'strong state', such as most Western industrialised countries, tend to cooperate in structures that are small and ephemeral (e.g. Reuter 1983). Furthermore, offenders tend to co-operate in varying structures in criminal networks that develop over time. The ways in which offenders cooperate can be explained by various factors, including pre-existing social networks, operational requirements, specific situational factors, or personal characteristics. We do not intend to present an extensive review of the literature on the structure and composition of organised crime groups here as such reviews of specific organised crime groups and criminal networks have been provided elsewhere (see, for example, Bichler et al. 2017, Bouchard and Morselli 2014, Paoli 2014, Morselli 2009). As the purpose of this article is to make a comparison for the Netherlands, we specifically review what is known about the structure and composition of organised crime in the Netherlands, based on four reports of the Dutch Organised Crime Monitor (Kleemans et al. 1998, 2002; van de Bunt and Kleemans 2007; Kruisbergen et al. 2012).

Although pyramid-shaped organisations exist in the Netherlands, they are the exception rather than the rule. This does not imply, however, that criminal organisations do not have a structure or that relationships in criminal networks are interchangeable and horizontal. Some people are more important than others in these networks owing to specific resources or capabilities they offer, such as money, knowledge or contacts. The four Organised Crime Monitor reports highlight the wide variety of forms of criminal cooperation and the fact that the logistics of criminal activities (what has to be arranged?) have a major influence on the ways in which criminal cooperation takes place (Kleemans et al. 1998, pp. 31–59, 2002, pp. 39–63). There are often, for example, key players on whom many offenders depend for their money, knowledge, or contacts. The question when analysing criminal networks should not, therefore, be 'Who is in charge?', but instead 'Who is dependent on whom? And why?'

327 While key players reappear again and again in various investigations and in various criminal collaborations, other offenders may gradually become less and less dependent on these key players because they acquire money, knowledge, and contacts of their own and subsequently generate new criminal collaborations. By not a priori assuming stable, pyramid-shaped organisations, we remain open to the possibility of growth and development within criminal networks, while also being able to see how enablers, who often operate on the periphery of criminal collaborations, regularly provide crucial services to several criminal collaborations.

The first two reports based on the Organised Crime Monitor specifically highlight the importance of enablers and supportive environments for the functioning of criminal collaborations (Kleemans et al. 1998, pp. 61–91, 2002, pp. 56–62). Criminal collaborations often do not carry out all activities themselves, either because they lack specific capacities, or because the risks are too high. In these cases, they can be helped by enablers who provide specific services, such as forging documents, transport, changing or exchanging money, and financial advice.

A characteristic feature of enablers' activities is that they are crucial for performing specific criminal activities. Secondly, they often create a bridge between the 'underworld' and 'upper world'; this is needed because the division between the licit and illicit world frequently creates logistical bottlenecks for criminal collaborations. A third characteristic is that the enabler is often relatively difficult to replace because relatively few people can offer the required expertise. A fourth characteristic is that these services are often delivered to multiple groups because criminal collaborations frequently face the same problems and come into contact with the same enablers through their social contacts. The scarcer the expertise and the more crucial it is for carrying out specific criminal activities, the more important the role of these enablers is within criminal networks.

Processes of origin and growth

An analysis of 92 'starters' in organised crime shows the various ways in which people become involved in this form of crime, including through existing social relationships, work- and job-related relationships, hobbies or ancillary activities, specific 'life' events' (particularly related to financial setbacks), and deliberate re-cruitment (Kleemans and de Poot 2008).

This explains why 'late starters' (i.e. people who become involved in organised crime only later on in life) are not exceptional in organised crime cases, but instead comprise a substantial proportion of the analysed suspects (Kleemans and de Poot 2008). This can be the case because some opportunities for carrying out profitable criminal activities arise only later on in life, while some people only act upon these opportunities later on in life, due to, for example, 'life events' such as bankruptcy and problematic debt situations.

Next to 'late starters', there are also offenders who have been criminally active for some time before switching to forms of organised crime. Criminal careers can gain momentum through factors such as specialisation (particularly in drug trafficking and production), a broker giving an offender access to interesting international markets, accumulation of capital the offender uses to invest in trading opportunities or semi-legal investments, or having specific skills or transnational contacts that attract other 328 offenders. In the latter case, the main catalyst is not the offender himself, but the network around the offender; as many other offenders depend on these skills or resources, offenders tell other offenders about specific expertise, and these other offenders consequently also seek contact.

In the world of organised crime, major financial interests are at stake in a mainly unregulated environment. Therefore, social embeddedness and trust are of great importance for the functioning of criminal collaborations. The four reports of the Dutch Organised Crime Monitor extensively discuss the importance of existing social relationships for criminal collaboration. Family, friends, and acquaintances work together and introduce each other to other people. Existing social relationships, however, do not always offer a solution because these relations are clustered, and physical and social barriers exist between different countries and different ethnic groups, and between the licit and illicit world. Bridging these 'structural holes' (Burt 1992) is very important and often a problem for criminal groups, particularly in cases of 'transit crime'. Transit crime includes profitable, international illegal activities, such as drug trafficking, human trafficking, arms trade, money laundering, and fraud (e.g. evasion of excise duties and taxes), where the Netherlands may function as a production country (for example, the production of synthetic drugs and cannabis cultivation), a transit country, or a country of destination. Such 'transit crime' activities comprise a very important part of organised crime in the Netherlands. However, criminal cooperation does not only revolve around reliability or trust; capacity is also important. That is why offenders

sometimes use 'outsiders' – not being family members, friends, or regular business partners – when they get involved in risky or very large operations (van de Bunt and Kleemans 2007, pp. 49–76). New relationships can offer new trading opportunities. How does trust emerge in such circumstances? First, learning effects are important: trust is based on personal experience regarding a partner's earlier performance. Second, trust can be based on transferred experiences of others. Third, reputation can also be based on generalisations regarding the (alleged or actual) characteristics of particular groups.

CYBERCRIMINAL NETWORKS: A REVIEW OF THE LITERATURE

Cybercrime

This section is about cybercriminal networks. In general, two types of cybercrimes are distinguished (e.g. Holt & Bossler, 2014; McGuire & Dowling, 2013). First, there are new types of crimes which are aimed at IT and committed through the use of IT. Examples include hacking databases with credit card credentials or using malicious software to encrypt files on a computer and demand a fee to decrypt these files. Second, there are traditional crimes which are not focused on IT, but for which IT is essential to commit the offence. Examples include the use of phishing e-mails and phishing websites in order to steal money from the online bank accounts of victims. In this article, in line with the literature, we use 'cyber-dependent' crimes for those within the first category and 'cyber-enabled' crimes for the latter category. 'Cybercrime' is used as an umbrella term for both categories.

Structure and composition

`329` In theory, the internet offers a perfect opportunity structure for decentralised flexible networks of criminals that are loosely organised and divide activities based on knowledge and skills. In practice, however, this does not always seem to apply in the case of cybercriminal networks.

Empirical research into organised cybercrime in the Netherlands, Germany, the United Kingdom, Sweden and the USA, for example, shows that the structure of cybercriminal networks is not very different from that of traditional networks (Bulanova-Hristova and Kasper 2016; Bulanova-Hristova et al. 2016; Werner and Korsell 2016; Leukfeldt et al. 2017a, 2017c, 2017d; Odinot et al. 2017). The majority of the networks studied by Leukfeldt et al. (2017a, 2017c, 2017d), for example, comprised a more or less stable group of core members who committed offences together over a longer period of time. The core members of these networks often knew each other from the physical world and recruited only a few specialists

through online meeting places. Only a few networks could be characterised as ad hoc collaborations in which alliances were forged at online meeting places.

Furthermore, several studies show that – similar to traditional networks – cybercriminal networks still contain important actors with a role as broker or bridge-builder (Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2012; Holt and Smirnova 2014; Décary-Hétu and Dupont 2012; Décary-Hétu et al. 2012; Leukfeldt et al. 2017b, 2017d). Lastly, cybercriminal networks also have some kind of hierarchy. Despite no mafia structure being identified, several layers were observed within all the networks studied by Leukfeldt et al. (2017c, 2017d, 2017f). At the top, there are the core members who plan the criminal activities (in this case: mainly financial cybercrimes, including phishing and hacking), work together for a long time, and find other suitable co-offenders. In the layer below the core members ('enablers') can be found. These enablers provide specific criminal services. A distinction can be made between professional enablers and recruited enablers. Both types of enablers provide services to the core members of criminal networks, so that the criminal activities can be executed or executed more effectively. The difference between the two groups is that professional enablers offer their services to all kinds of networks, whereas recruited enablers are encouraged by core members to provide specific services. The bottom layer is composed of money mules. These types of criminals are used by the core members or enablers to interrupt the money trail to the criminal group. Money mules' bank accounts, for example, may be used to receive money from the bank accounts of phishing victims.

Some networks, however, fully exploit the opportunities the internet offers. Members of these networks can quickly gain an international position through the use of online criminal meeting places (Leukfeldt et al. 2017a, 2017d) or enter into a chain collaboration with other criminals, each carrying out a specific criminal activity (Bulanova-Hristova et al. 2016; Odinot et al. 2017).

Hence, some networks have many similarities with traditional criminal networks – long-term cooperation between the core members and dependency relations –, whereas others comprise more ad hoc and short-term collaborations, in which the individual members specialise in a specific activity. These differences in structure are related to the `330` processes of origin and growth (Bulanova-Hristova et al. 2016; Leukfeldt et al. 2017a, 2017c, 2017d). Traditional criminal networks that start committing cybercrimes retain their original structure, while networks that commit only cybercrimes but originate from offline social contacts also have a structure similar to that of traditional criminal networks. Lastly, networks that commit only cybercrimes and where the core members got to know each other online show some variation in structure: sometimes they have a traditional structure (even criminals who meet each other online have long-term contacts; see, for example, Leukfeldt et al. 2017a, 2017d), but these types of networks can also comprise short-term chain or other forms of cooperation.

Processes of origin and growth

The "Structure and composition" section explains how offline social ties play an important role in the development of criminal networks. In the online world, however, no geographical distances need to be bridged to come into contact with other offenders; distance, location and time are, in principle, no longer a limiting factor for criminal cooperation.

Various studies have provided evidence that digitisation, and particularly online criminal meeting places, can influence the origin and growth processes of criminal networks. Soudijn and Zegers (2012) and Yip et al. (2012) found that newcomers to digital meeting places quickly get in touch with existing forum members and relatively quickly take on a more central position. In an online environment, the important role that core members normally play in networks seems, therefore, to decrease.

However, the studies of Leukfeldt (2014), Leukfeldt et al. (2017a, 2017d, 2017f), Bulanova-Hristova et al. (2016) and Odinot et al. (2017) found that cybercriminal networks use both offline social contacts and online meeting places. In networks where offline social contacts form the basis for origin and growth, family, friends, and acquaintances work together and introduce each other to others (similar to traditional criminal networks). Only a few networks comprise solely offline social relationships. Most networks use online meeting places to acquire specialist knowledge and skills that they cannot find within their offline social contacts, for example purchasing advanced malware or hacking tools. A dichotomy can also be seen in networks where online contacts form the basis for the network's origin and growth. Members of these networks get to know each other online, for example through chat channels or forums. A minority of the networks seem to be able to carry out the criminal activities with only online contacts. Not only the core members of these networks get to know each other online, but also all the enablers are recruited online. Other networks, however, have a mix of online and offline contacts; core members get to know each other online and some enablers are recruited online, but other enablers are recruited within offline social networks (see also, for example, Lusthaus and Varese 2017; Lusthaus 2019). The latter is especially true for networks of money mules, recruiters and cashers.

Online meeting places remove the traditional limitations of social networks. In many ways, these meeting places do not differ from traditional offline criminal meeting places, also called 'offender convergence settings' (see Felson 2003, 2006): once you are inside, you can contact others, buy criminal tools, and explore new markets. However, access to online meeting places seems to be easier than access to offline criminal meeting places (Leukfeldt et al. 2017d, e). For the curious loner, it is easier to **331** hang around on public forums and ask questions than to do the same in a bar full of criminals. It is also important to note that online meeting places have a learning function and that a subculture exists in which the sharing

Erasmus University Rotterdam

of information about criminal opportunities is fairly normal (Chu et al. 2010; Holt and Kilger 2008; Holt et al. 2012; Hutchings and Holt 2015; Hutchings 2014; Leukfeldt et al. 2017b, 2017d; Soudijn and Zegers 2012). Someone who wants to learn can therefore go to a forum, ask questions, and look up information on the discussion sections of the forum. You can also pay people to learn new skills (Hutchings and Holt 2015; Chu et al. 2010; Holt and Lampke 2010; Hutchings and Holt 2015). Lastly, rating and review systems allow reliable co-offenders to be found (Soudijn and Zegers 2012; Herley & Florencio, 2010; Wehinger 2011; Yip et al. 2012; Lusthaus 2012; Dupont et al. 2016; Décary-Hétu and Dupont 2012, 2013; Holt 2013; Holt and Smirnova 2014; Holt et al. 2015; Chu et al. 2010; Ablon et al. 2014).

Commentators note that it is obvious that traditional organised crime is moving more and more to the online world (for example, Grabosky 2007; McCusker 2006; Lusthaus 2013; Broadhurst et al. 2014; EPO 2016). However, to date, little empirical research on this topic has been done. Empirical studies show that traditional criminal networks that are involved in all sorts of crime, use IT to improve their crime scripts (for example, Odinot et al. 2017; Bulanova-Hristova et al. 2016; Leukfeldt 2014; Leukfeldt et al. 2017a, b, c, d). Networks involved in human smuggling and drug trafficking, for example, use the Internet to communicate encrypted or use online meeting places to recruit new co-offenders (Odinot et al. 2017; Bulanova-Hristova et al. 2016; Lavorgna 2014a, b, 2015a, b). Furthermore, the study of Bijlenga and Kleemans (2017) shows that traditional criminals are able to recruit IT-experts 'in the grey zone' easily because some software or tools that can be abused by criminals are offered legally on the Internet or by so-called Spy-shops (that often offer extra services for their customers).

DATA AND METHODS

Our empirical data consist of large-scale criminal investigations into organised crime. These cases are part of the Dutch Organised Crime Monitor (DOCM). The DOCM is an ongoing research project into the nature of organised crime in the Netherlands. In five data sweeps, 180 cases of organised crime were analysed, each including several and sometimes dozens of individual suspects. In each case, the police files were analysed, containing the results of all policing activities that were deployed, such as wiretapping, monitoring of internet traffic, undercover policing, interrogations of suspects, confiscation, and financial information. For this article, we used the 30 cases analysed in the fifth and most recent data sweep. These 30 cases, based on criminal investigations completed in the period 2011–2016,[1] include various forms of organised crime, such as various types of drug trafficking, illegal

---

1. Criminal investigations in organized crime can take several years before they are completed. For this data sweep, we used investigations completed in the period 2011–2016 and two slightly 'older' cases (regarding important investigations that had not been analyzed in the earlier data sweeps).

arms trade, 332 human trafficking, fraud and money laundering, and cybercrime (for more information, see Kruisbergen et al. 2018).

The selection of 30 cases for the fifth wave of data collection came about after an intensive inventory of criminal investigations. This inventory took place through interviews with and visits to specialised units, and different national and regional units within the police and Public Prosecution Service. Discussions were held with specialists in the field of cybercrime, cocaine and heroin, synthetic drugs and hemp, fraud and money laundering, robberies, and human trafficking. Ultimately, this inventory was carried out at all ten regions of the police / Public Prosecution Service and a number of national units.

The inventory produced a 'long list' of about 70 cases, of which 30 were eventually selected. Different criteria played a role in this selection (and in the longlist). Some important criteria are:
– There is a criminal partnership of multiple actors.
– The criminal investigation has been completed (arrest of main suspects) in 2011 or later. Nevertheless, two 'older' cases were also included, as these cases had substantial added value and had not yet been included in the previous data sweeps.
– The case has 'rich information'. Often by using, for example, a telephone and / or internet tap, bugging face-to-face meetings, undercover trajectories, or the seizure of administration, some investigations provide a good view of the modus operandi of the network and the structure of the network.
– The degree to which the case adds value by looking at specific aspects, such as interconnectedness between offenders and their environment ('under' and 'upper world'), shielding against the authorities, criminal money flows, an international component, or a new or interesting modus operandi or criminal group.
– Various types of offenses should be included. Therefore, not only drug cases are selected, but also cases related to, for example, cybercrime, money laundering, and fraud.

An analytical framework was used to systematically analyse the cases. The complete framework is described in Kruisbergen et al. (2018). For this specific study, we used a part of this framework, focusing on ties between members of networks, processes of origin and growth, and the use of offline and online offender convergence settings:
– Composition of the network: how are the suspects related, their role and/or function within the network (subgroups, core functions, facilitators, periphery)?
– Structure of the criminal network (e.g. standalone unit, fluid cooperation based on a specific goal).

– Is there hierarchy and/or mutual dependency?
– How, when, and where did the network start?
– Do the suspects have a common or different background? (family, neighbourhood, friends, occupation, etc). If not, in what ways are the suspects related?
– What kept the members of the criminal network together? (social ties, economic advantages, fear, etc).
– Describe the (digital) offender convergence settings used by the criminals.

333 The DOCM covers criminal investigations into criminal networks that have been completed by the police, i.e. where the investigation team has collected enough evidence for the Public Prosecution Service to decide to prosecute, even though a court judgment may not necessarily have yet been issued. Waiting for a court judgment would have meant that only a few cases would have been available for analysis, as it can take years for suspects to be finally convicted (after appeal). For the analysis of these criminal investigations, permission has been granted by the Netherlands Public Prosecution Service. Before publishing results, a special procedure of checks and double-checks seeks to prevent disproportionate harm to the interests of suspects and/or criminal investigation strategies. For a more extensive review of these methodological questions, see Kleemans (2014).

We distinguished four categories of cases, depending on the role IT played. The first category comprised 23 cases of *traditional organised crime*; in other words, cases without a strong IT component. These included cases of offline drug trafficking (cases 158, 159, 161–164, 167, 169–172, 175, and 176), human smuggling/trafficking (case 160), money laundering (cases 157, 166, 168, 177, 178, and 180), and other/combined crimes (cases 165, 174, and 179). The second category comprised three cases of *traditional organised crime* in which IT was an important innovative element in the modus operandi. One of these cases concerned an offender group manipulating the handling of incoming containers by hacking the network of a port terminal (case 151). A second case concerned people involved in a dark web market on which drugs, for example, were traded (case 152). The third case revolved around a modern variant of money laundering, entailing bitcoin exchangers who helped their customers anonymously exchange bitcoins for cash. The information available indicated that these customers earned their bitcoins through online drug trading (case 173). The third category comprised two cases of *organised low-tech cybercrime*. One of these cases concerned a variant of 'skimming' (also known as 'shimming') in which the data traffic between the EMV chip on the card and the terminal in which it was used was intercepted (case 154). The second case concerned phishing operations, in which criminals sought, for example, to obtain people's online banking credentials (case 156). The fourth category included two cases of *organised high-tech cybercrime*. Both cases focused on banking malware, i.e. criminals using malicious software to manipulate payments made via internet banking (cases 153 and 155).

Criminal investigation files are thus the most important data source within the monitor. The use of police data for research purposes naturally has certain limitations. The most fundamental limitation concerns the aforementioned fact that investigation files ultimately only concern persons and activities that came to the attention of the police and about which the police wanted and could gather information. This fact can lead to a bias in the research results. Activities and offenders who fall outside the view and/or priorities of the police are also not available for analysis. However, this selective view also entails an important advantage for gathering knowledge. Anyone who wants to delve into criminal phenomena is confronted with the 'walls of silence' surrounding criminal activities, particularly when it comes to organised crime (van de Bunt 2007, 2010). Only the police have far-reaching powers to break through these 'walls' through the use of special investigation methods. A researcher having access to criminal investigation files benefits from these exclusive powers and can thus also gain an exclusive insight into the activities of offenders or in the way in which they relate to each other and their surroundings.

RESULTS

334 In this section, we discuss the results of our empirical analyses. The "Structure" section focuses on the structure and composition of the criminal networks in the 30 cases we studied. The origin and growth of these networks are discussed in the "Origin and growth processes" section.

Structure

Traditional organised crime
The picture shown by the cases relating to traditional organised crime does not differ from that shown by the cases in the previous DOCM reports. There are no mafia-like, pyramid-shaped organisational structures, but instead more or less structured criminal networks with key players and criminal enablers on which others depend. The way in which criminals cooperate was also seen to depend on the nature of the criminal activities that are carried out.

Traditional organised crime with a cyber element
The network from case 151 concerned a fairly traditional criminal network involved in international drug trafficking, and was similar to cases in the previous data sweeps. It was a well-organised collaboration in which criminals worked together in separate subgroups. Approximately 50 people were linked to this criminal cooperation in the investigation. The difference with other networks involved in traditional drug trafficking is that this network used the services of two hackers

to locate and pick up containers of drugs before the regular transport company reached the cargo.

The investigation focused on offender A and related persons. Offender A was one of the core members of the criminal collaboration, handling the transport of cocaine from South America to the Netherlands and Belgium on behalf of other criminals. Offender A and other core members were in contact with various people providing criminal services. The core members had contacts, for example, with suppliers of drugs in Colombia, used interpreters for communications, (presumably) used people working at shipyards or the port to falsify transport documents, and controlled drivers who actually drove containers containing drugs from one point to another. Lastly, core members and facilitators used all kinds of legal constructions, as well as 'straw men', to stay under the radar. In other words, the criminal collaboration in this case was very similar to that in traditional criminal networks. The only difference was that hackers were used to locate and pick up containers of drugs in harbours before the regular transport company reached the cargo.

The central feature in case 152 was an online market place where drugs and weapons were traded. The criminal investigation focused on the Dutch members who had developed and were managing the online market. The collaboration involved three core members and an enabler. Two of the core members were the creators of this specific online market and had developed a first version of the online platform, which was not good enough to use. Although these two core members had a high degree of IT knowledge, they needed the help of an enabler, who was a long-term acquaintance of 335 one of the core members, to create an effective online market. Without him, the market would not have been able to function as they wanted. The third core member had no IT knowledge, but a criminal background and past experience in offline drug trafficking.

The online platform was divided into a market place section and a discussion section. Drugs, for example, were offered within the market place section, where sellers placed advertisements and buyers could contact the sellers. In the discussion section, members could find information on various topics (for example, the best way to send drugs), create new discussion topics, and find information about sellers. In this case, the collaboration between the offenders formed the organised 'reverse side' of a forum they managed and also used themselves. In this way, they expanded the opportunities to deal drugs, while the online market also generated revenue for the offenders.

The criminal network in case 173 was involved in converting bitcoins into cash. The bitcoins were presumably obtained by, for example, selling drugs on online criminal markets on the dark web. The criminal investigation focused on five main suspects who exchanged bitcoins, jointly and individually, over a longer period of time. The main suspects placed advertisements on various online platforms, where they advertised opportunities to exchange bitcoins for cash. Although they

used publicly accessible websites, the group's clients meant they probably also advertised on forums on the dark web. These bitcoin exchangers actually functioned as enablers for all kinds of other criminal networks and independently operating criminals.

The investigation discussed only the cooperation involving several online drug traffickers. Despite investigators describing one of the core members as the coordinator, there seemed to be no clear hierarchy within the group of core members. The core members sometimes worked together, but often also worked independently and had their own customers. The core members used money mules' bank accounts to exchange the bitcoins for cash.

Organised cybercrime: low-tech

The criminal network in case 154 adapted card readers issued by a Dutch bank for logging in to online bank accounts. The network consisted of three layers: five core members, one enabler, and six lower-level suspects. This network had been working together for about a year and a half. A hierarchy existed among the core members. One core member was the coordinator and had contacts with the enabler. This enabler operated from the UK for various networks and provided crucial services to these networks. The core members had no technical knowledge and were dependent on the enabler, who adapted the card readers, gave the core members clear instructions about how to act, and managed the database containing the data obtained through the use of adapted card readers. The other core members were described as team leaders managing teams of lower-level suspects. The task of these suspects was to enter physical bank offices to exchange the card readers and retrieve them after a period of time.

The criminal network in case 156 was involved in phishing attacks on customers of Dutch banks and consisted of four layers: a group of core members, professional enablers, recruited enablers, and money mules. The eight core members cooperated in a more or less stable composition for at least a year and a half (the duration of the investigation). Remarkably, none of the core members had a high degree of IT expertise.

336 In contrast to the malware networks in cases 153 and 155, the core members in case 156 did not use forums to contact enablers with technical knowledge. Instead, they used a friend of an acquaintance of a core member from Nigeria who was able to build phishing websites for Dutch banks. The core members also used an enabler to supply false identity documents. How the contact with this enabler came about was unclear. The core members also used the services of many others, including people working at call centres of Dutch banks who supplied information on accounts and increased cash withdrawal limits (making it easier to cash stolen money), postal workers intercepting officially requested log-in credentials, 'callers' who had to telephone potential victims to obtain transaction codes, and people

recruiting money mules or supervising the cashing process. All these enablers were recruited through informal contacts. The bottom layer of the network consisted of money mules providing their bank account to the core members of the criminal group. The money mules were used to interrupt the money trail from the victims to the core members.

Organised cybercrime: high-tech
Both criminal networks in cases 153 and 155 used malware to steal money from online bank accounts of customers of Dutch banks and had four layers. The top layer consisted of the core members of the network who controlled the others within the network and coordinated the attacks.

In case 153, the network consisted of four core members, while the network in case 155 had five core members. In both networks, the core members did not appear to have an exceptionally high degree of technical knowledge. Some core members, however, clearly had affinity with the criminal opportunities IT offers and were, for example, active on forums containing information about committing all kinds of cybercrimes, as well as downloading videos explaining how certain forms of malware work. The professional enablers were located in the layer below (or next to) the core members. These offenders offered their criminal services to various networks. In both cases 153 and 155, core members used online forums to find enablers with a high degree of technical expertise. Given the core members' limited technical knowledge, they needed enablers to be able to carry out the malware attacks. The network in case 153 used various enablers to, for example, purchase malware, rent a botnet and buy falsified identity cards. The network in case 155, by contrast, used a forum only to buy a specific type of malware. One of the core members then adapted it to attack Dutch banks.

The networks in cases 153 and 155 also used the services of people who did not offer these services to a multitude of networks. These persons were recruited by the core members and, as a rule, were part of the social network of one or more core members. The network in case 153, for example, used a postman who intercepted packets that had been purchased through fraudulent transfers from victims' accounts. This postman was a neighbour of one of the core members. The network in case 155 used a person who recruited money mules. These money mules provided their bank accounts to the core members so that money from victims' accounts could be cashed. The recruiter had been involved in criminal activities for some time and so knew one of the core members, who had previously been involved in bankruptcy frauds.

The bottom layer of the networks in cases 153 and 155 consisted of money mules who made their bank accounts available to core members. These money mules were **337** used to interrupt the money trail from the victims to the core members. Money was transferred from the victims' accounts to the money mules'

accounts. Subsequently, the money was cashed as soon as possible. Money mules were recruited within the social networks of core members and enablers. This involved both offline social contacts (friends, people from the neighbourhood, etc.) and online social contacts (posts about making quick money on social media). One of the network's recruiters in case 155, for example, recruited new money mules by approaching acquaintances. If someone cooperated, the friends of that person were then also approached. Communications between the core members demonstrated that recruiters were deliberately looking for people who were easily influenced, for example people with high debts or psychological problems, or drug addicts. The file contained examples of money mules with debts, a homeless person, and someone in an assisted-living programme.

Origin and growth processes

In this section, we discuss the processes of origin and growth, how new core members and enablers are recruited, how trust is gained, and to what extent criminal networks are locally embedded.

Traditional organised crime

Previous reports of the DOCM showed the importance of existing social relationships within criminal networks. Social ties are often crucial for the processes of origin and growth of criminal networks: family, friends and acquaintances work together and introduce each other to others. Where existing social relationships fail, 'outsiders' (others than family members, friends, or regular business partners) are deployed, with criminal meeting places playing an important role in this process.

The picture showed by the new cases relating to traditional organised crime does not differ from that shown by the cases in the previous monitor reports. The importance of social relations is also clearly visible in these cases, as is the importance of criminal meeting places.

Traditional organised crime with a cyber element

Case 151 concerned a criminal network involved in international drug trafficking. This criminal collaboration, or subgroups of this collaboration, had been involved in drug trafficking and other criminal activities for some time. Most of the suspects were from the Netherlands, but some were from Belgium, Spain, Turkey, Cape Verde, Serbia, Albania, Bulgaria, Indonesia and Colombia. Although it is unclear how the network originated, it seems to be a fairly classic example of a criminal collaboration in which social ties play an important role. The majority of the approximately 50 people linked to this criminal collaboration had previous drug-related criminal activities in common. As well as some of the members of the criminal collaboration having been active in the criminal environment for some time and having got to know each other this way, there were various family and friendship relationships

within the network. For example, C was a brother of T, while E was the husband of Z, W was the son of X, ZZ was the father of ZY, ZR was the father of ZQ, and ZM was the former brother-in-law of B. ZV 338 said he had known X and O for 20 years through playing football, while N had known M for five years from the pub, and ZI said he also knew G from the pub.

A special feature of this criminal collaboration was that the core members used two hackers who helped them to intercept and pick up containers of drugs before the regular transport company arrived to collect the cargo in the port. These hackers were two foreigners who had been hired by a Dutch bank to develop systems. One enabler played a crucial role in establishing contacts between the IT specialists and the members of the criminal network. Exactly how and why this suspect contacted these two IT specialists is unknown.

The criminal collaboration in case 152 also related to drug trafficking. This network used an online market to sell drugs. The three core members were the developers of the market and had roles as administrator and moderator. Offender B, who said he had a rare disease and stayed at home, seems to have been pivotal to the gathering of the core members. B and C (who lived in Germany) knew each other through forums. Both were previously active on a market place where drugs were traded. When that market was about to go offline, these core members decided to develop a new online platform. B and A, a person with a criminal past and who had been active in drug trafficking for a long time, had known each other for years. It is unclear how this contact was forged. Despite two core members having coding skills and a high level of technical expertise, they were not able to build a good online platform and needed the help of E, who knew 'B' through online forums. B and E found each other through a shared interest in mining and trading bitcoins. In the past, they had already programmed together and had a lot of things to discuss with each other. B wanted to use E's programming expertise. According to E, it started with programming one module, quickly followed by more. At a certain moment, a point was reached where B himself could no longer make changes to the online platform because he did not have enough knowledge to do so.

The criminal network in case study 173 dealt, among other things, with the exchanging of bitcoins, obtained through sales of drugs on online criminal markets on the dark web, for cash. The core members all knew each other through offline social contacts. Three of the core members had had the same part-time job at a food wholesaler for several years. Through their shared interests, they came into contact with each other and a friendship arose. The other two exchangers were a childhood friend of the three core members and a brother. The exchangers used, among other things, the bank accounts of money mules to obtain large amounts of cash. Offender A, who was seen as the coordinator of the exchangers, mainly used people from a specific ethnic background.

In addition, the criminal investigation specifically focused on several drug dealers who used online markets on the dark web to sell their illegal drugs. One of the ways the drugs they sold on the online markets were paid for was in bitcoins. The sellers used the services of the bitcoin exchangers to exchange this cryptocurrency for 'real' cash.

The initial contacts between the drug traders and bitcoin exchangers were online. Although the bitcoin exchangers had placed ads on forums, these online contacts were quickly followed by meetings in the physical world. During these meetings, which often took place at, for example, Starbucks or McDonalds, one party transferred bitcoins, on the spot, to the other party's wallet. Subsequently, cash was handed over. The bitcoin exchanger had previously withdrawn that money from cash dispensers (in several small amounts) or brought cash with him. To check whether new customers **339** were reliable, the bitcoin exchangers asked questions and checked reviews and other available information about the new customers. They also appeared to do long-term business with a few regular customers, sometimes exchanging tens of thousands of euros a week.

Despite the global nature of the dark web and bitcoins, the bitcoin exchangers in this criminal investigation operated in a limited market, with the Dutch bitcoin exchangers mainly working for customers in the Netherlands, Belgium, Germany, Italy, Northern France, and Luxembourg.

Organised cybercrime: low-tech
The criminal network in case 154 consisted of five core members, an enabler, and various lower-level suspects. The core members and lower-level suspects were connected through family and friendship ties, and were mainly Romanians residing in the Netherlands and originating from the same region in Romania. C and F, for example, were brothers. C, D and H were friends and grew up together. C arranged a job in construction for D, while H and I had attended the same primary school. B, C and H had previously been arrested in Romania for traditional skimming activities (installing skimming equipment at payment terminals). The only member born and raised in the Netherlands had a romantic relationship with an acquaintance of D.

The members of this criminal group were constantly looking for new opportunities to earn money. Some of them worked in construction, but were also involved in various criminal activities, such as human trafficking, prostitution, and drug trafficking. At a certain point, B bought skimmed data from bank cards from a criminal group in the UK. However, these cards did not appear to work. Through contacts in the criminal environment he then came into contact with A, who worked from the UK for various local groups involved in skimming. A then developed software for skimming equipment, gave the core members of other networks instructions, and managed the database of skimmed data.

Case 156 concerned a network performing phishing attacks. A typical feature of this network was that the members knew each other through informal contacts in the offline world. This was true both for the core members, and also for the enablers and money mules used. Members knew each other because, for example, they had family ties, came from the same neighbourhood and hung around together, or because they were at the same school or sports club. Although it was unclear how exactly the eight core members met each other, they all originated from the same Amsterdam neighbourhood and had been active in the criminal environment for a long time. The criminal investigation showed, for example, that they had performed or carried out various other criminal activities in varying compositions, such as drug trafficking, skimming, and fraud with telephone subscriptions.

Enablers, such as bank employees who supplied information from accounts and were able to increase cash withdrawal limits, and postal employees who intercepted log-in credentials sent by post, were specifically recruited by the core members or people who knew the core members: the enablers were repeatedly approached on the street and asked to cooperate. The bank employees lived in the neighbourhoods where the core members were also active. The bank employees stated during questioning that they were simply asked to provide information about account numbers. Bank `340` employees were also offered financial compensation. Sometimes a pretext was first used to find out whether a bank employee could access relevant information; for example, 'My ex owes me money. She says she hasn't got any money, but I don't believe that. Can you check that?' As soon as it was known that the enabler could indeed access specific information, pressure was exerted on the enabler to actually provide information.

Money mules who made their accounts available to 'cash' money were also recruited through informal contacts. New money mules were openly recruited in school playgrounds, and at sports clubs and night clubs. The core members and recruiters also used social media to approach acquaintances and strangers. Several money mules indicated that it was quite normal to be approached by people wanting them to cooperate with the fraud scheme and to let them use their bank accounts.

Organised cybercrime: high-tech
The criminal networks in cases 153 and 155 used malware to steal money from online bank accounts of Dutch bank customers. In both cases, the core members were all Dutch. The core members knew each other through offline and online social contacts and used online markets to purchase malware.

In case 153, for example, there were four core members who knew each other through social contacts. A and B were the core members who carried out the technical part of the offence. They purchased and adapted the malware and coordinated the attacks. It is unclear how the two came into contact with each other. However, both studied economics at different universities. B and D knew each other from

school, while A and C knew each other from the 'rap scene', where people were reported to openly talk about making money by providing bank cards to enable money to be cashed. C indicated that he initially approached A through social media. The core members used a postman who intercepted packets that had been purchased through fraudulent transfers from victims' accounts. This postman was the neighbour of one of the core members. While money mules were also recruited from social networks, the police files stated that contacts were also made through social media and online games.

The two core members who were responsible for the technical part of the offence did not have sufficient technical expertise to carry out the malware attack themselves. However, two core members had 'affinity with this matter' and were active on forums. This way, they were able to reach out to the right enablers and purchase suitable tools. A, for example, had contacts via forums with people who could provide log-in details for customers of Dutch banks and with whom he also discussed the opportunities to use stolen credit card information to purchase goods in web shops. Two other online contacts were the developer or seller of malware that the group used to gain access to online bank accounts and the administrator of a botnet of which the infected computers were part. Both contacts got some of the proceeds from the malware attacks. Lastly, A knew a Russian able to forge identity documents. All the contacts that started on forums were continued through chat programs with encrypted communication.

Case 155 concerned a network of five core members who all had connections from the offline world. A, who can be viewed as the coordinator of this network, had contacts with someone with a technical background (E) and people with a financial background (B and C). He knew all these people because they had worked for the same 341 companies. The final core member (D) had a long criminal career and had contacts both with a professional enabler who operated from the UK and laundered money and with a Dutch recruiter of money mules, and also had his own network of money mules that could be used to 'cash' money.

CONCLUSION AND DISCUSSION

In this article, we described what is known from previous empirical research into criminal networks in organised crime and the extent to which the literature on cybercrime paints the same or a different picture. We also analysed criminal networks from 30 police investigations, distinguishing between traditional organised crime, traditional organised crime where the use of IT is an important innovative element, organised low-tech cybercrime, and organised high-tech cybercrime.

The article provides insight into criminal collaborations based on a unique dataset. However, the methodology we used also has several limitations. Therefore, before presenting the conclusions, we will first discuss the disadvantages of this

methodology. First, we have insight only into criminal collaborations that have been investigated by the police, so we do not know anything about networks that never came to the attention of the police. Our cases also contain a limited number of types of cybercrime; none of them, for example, involve botnets, ransomware, or DDoS attacks. It may well be the case that such networks have a different structure or that the processes of origin and growth differ in at least some ways. Future research in this area should, therefore, include such types of cybercrime. Finally, we were only able to analyse a limited number of cybercrime cases and cases in which IT is an innovative element. As police investigations will continue, the future may hopefully bring more empirical case material that will become available for scientific research, in the Netherlands and elsewhere.

The majority of the networks analysed were clearly found to have a more or less permanent group of core members working together over a longer period of time. This is in line with earlier findings (see, for example, Bulanova-Hristova and Kasper 2016, Bulanova-Hristova et al. 2016; Leukfeldt et al. 2017a, d). Furthermore, all the networks included dependency relationships, with some members being more important than others, and core members relying on enablers.

Compared to cases of traditional organised crime, the importance of technical knowledge and technical skills is evident. It is striking, however, that the offenders themselves often do not have much technical knowledge; instead, they obtain this knowledge through enablers. In the high-tech cybercrimes analysed, core members gained technical expertise through the use of online markets, whereas offenders in the low-tech cybercrime cases used contacts from the offline criminal environment. In the former cases, the search for technical knowledge took place through online interactions, while in the latter cases it was through offline interactions. This view of cybercriminal networks as networks of which the majority of members don't have high technical expertise is fairly new and strengthens the picture painted by recent studies of Lusthaus (2019) and Leukfeldt et al. (2017a, c, d).

In general, in line with both studies into traditional criminal networks and more recent empirical work into cybercriminal networks, it is clear from the analysed cases 342 that offline social relationships play an important role in the processes of origin and growth. Core members in particular know each other through their offline social networks. There were also examples, however, where social media platforms and online games were used to make contacts. A characteristic feature in some of the networks involved in committing cybercrime or dealing with traditional crime with an innovative IT component is that such networks are often a 'mix' in terms of composition. On the one hand, members have already earned their spurs by committing traditional crime and have all kinds of contacts in the underworld. On the other hand, there are often very few members with the required degree of technical expertise. Particularly for high-tech networks, therefore, online criminal

markets play an important role in finding enablers with the technical expertise needed to carry out the attacks.

Local embeddedness appears to be present in almost all the cases analysed. While it is no surprise that this is present in the case of traditional offline organised crime (see, for example, Kleemans and de Poot 2008; van de Bunt and Kleemans 2007), in other cases this local embeddedness is less obvious (exceptions are empirical studies of Lusthaus). For example, networks dealing with cybercrimes, both high-tech and low-tech variants, are characterised by core members from the Netherlands who get to know each other in the offline world. These core members know their way around online criminal markets on the dark web, but also recruit enablers and money mules from within their own offline social network. Finally, the Dutch online sellers of drugs mainly limited themselves to selling in the Netherlands and other European countries (usually those within 'driving range' of the Netherlands, such as Belgium, Germany, and France). The same applies to the bitcoin exchangers working for people trading on international online drug markets. These individuals mainly worked for customers who were relatively close and located in the Netherlands, Belgium, Germany, Italy, Northern France, or Luxembourg. The borderless opportunities of cybercrimes appear, therefore, to be exploited through networks also demonstrating local embeddedness.

Compliance with ethical standards

Conflict of interest E. Rutger Leukfeldt declares that he has no conflict of interest.

Edward R. Kleemans declares that he has no conflict of interest.

Edwin W. Kruisbergen declares that he has no conflict of interest.

Robert A. Roks declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors. For the analysis of criminal investigations, permission has been granted by the Netherlands Public Prosecution Service.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

Ablon, L., Libicki, M.C., & Golay, A.A. (2014). *Markets for cybercrime tools and stolen data*. Hackers' Bazaar. RAND: www.rand.org

Albini JL (1971) *The American mafia: genesis of a legend*. Appleton, New York

Bichler G, Malm A, Cooper T (2017) Drug supply networks: a systematic review of the organizational structure of illicit drug trade. *Crime Sci* 6(2). https://doi.org/10.1186/s40163-017-0063-3

Bijlenga, N., & Kleemans, E.R. (2017). *European Journal of Criminal Policy and research*, https://doi.org/10.1007/s10610-017-9356-z

343 Bouchard M, Morselli C (2014) Opportunistic structures of organized crime. In: Paoli L (ed) *The Oxford handbook of organized crime*. Oxford University Press, Oxford / New York, pp 288–302

Broadhurst R, Grabosky P, Alazab M, Chon S (2014) Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *Int J Cyber Criminol* 8(1):1–20

Bulanova-Hristova, G., & Kasper, K., (2016). Cyber-OC in Germany. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, & L. Korsell *(red), Cyber-OC - Scope and manifestations in selected EU member states* (p. 165–220). Wiesbaden: Bundeskriminalamt

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., de Poot, C., Werner, W., & Korsell, L. (Eds.) (2016). *Cyber-OC - scope and manifestations in selected EU member states*. Wiesbaden: Bundeskriminalamt

Burt RS (1992) *Structural holes*. Harvard University Press, Cambridge

Chu, B., Holt, T.J., & Ahn, G.J. (2010). *Examining the creation, distribution, and function of malware on-line. Technical Report for National Institute of Justice*. NIJ Grant No. 2007-IJ-CX-0018. Available at http://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf

Cressey DR (1969) *Theft of the nation: the structure and operations of organized crime in America*. Harper & Row, New York

Décary-Hétu D, Dupont B (2012) The social network of hackers. *Global Crime* 13(3):160–175

Décary-Hétu D, Dupont B (2013) Reputation in a dark network of online criminals. *Global Crime* 14(2–3): 175–196

Décary-Hétu D, Morselli C, Leman-Langlois S (2012) Welcome to the scene: a study of social organization and recognition among Warez hackers. *J Res Crime Delinq* 49(3):359–382

Dupont B, Côté AM, Savine C, Décary-Hétu D (2016) The ecology of trust among hackers. *Global Crime* 17(2):129–151

Edwards A, Levi M (2008) Researching the Organization of Serious Crimes. *Criminol Crim Just* 8(4):363–388

European Police Office (2016). *Internet organised crime threat assessment (IOCTA) 2016*. Den Haag: European police office

Felson M (2003) The process of co-offending. In: Smith MJ, Cornish DB (eds) *Theory for practice in situational crime prevention (volume 16)*. Willan Publishing, Devon, pp 149–168

Felson, M. (2006). *The ecosystem for organized crime (HEUNI paper no. 26)*. Helsinki: HEUNI

Grabosky P (2007) The internet, technology, and organized crime. *Asian Criminology* 2(2):145–161

Holt TJ (2013) Exploring the social organisation and structure of stolen data markets. *Global Crime* 14(2–3): 155–174

Holt TJ, Kilger M (2008) *Techcrafters and Makecrafters: a comparison of two populations of hackers*. Wistdcs, p.67-78. In: 2008 WOMBAT workshop on information security threats data collection and sharing

Holt JT, Lampke E (2010) Exploring stolen data markets online: products and market forces. *Crim Justice Stud* 23(1):33–50

Holt TJ, Smirnova O (2014) *Examining the structure, organization, and processes of the international market for stolen data*. U.S. Department of Justice, Washington

Holt TJ, Strumsky D, Smirnova O, Kilger M (2012) Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology (IJCC)* 6(1):891–903

Holt TJ, Smirnova O, Chua YT, Copes H (2015) Examining the risk reduction strategies of actors in online criminal markets. *Global Crime* 16(2):81–103

Hutchings A (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime Law Soc Chang* 62(1):1–20

Hutchings A, Holt TJ (2015) A crime script analysis of the online stolen data market. *Br J Criminol* 55(3): 596–614

Ianni FAJ, Reuss-Ianni E (1972) *A family business: kinship and social control in organized crime*. Routledge and Kegan Paul, London

Kleemans ER (2014) Organized crime research: Challenging assumptions and informing policy. In: Knutsson J, Cockbain E (eds) *Applied police research: challenges and opportunities. crime science series*. Willan, Cullompton

Kleemans ER, de Poot CJ (2008) Criminal careers in organized crime and social opportunity structure. *Eur J Criminol* 5(1):69–98

Kleemans ER, van de Bunt HG (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(1):19–36

344 Kleemans, E.R., Berg, E.A.I.M. van den, & Bunt, H.G. van de (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. [Organised crime in the Netherlands. Report based on the Monitor Organised Crime] Den Haag: WODC

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*. [Organised crime in the Netherlands. 2nd report bases on the Monitor organised crime] Den Haag: WODC

Kruisbergen, E.W., Van de Bunt, H.G., & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. [Organised crime in the Netherlands. 4th report based on the monitor organised crime] Den Haag: Boom Lemma

Kruisbergen EW, Leukfeldt ER, Kleemans ER, Roks RA (2018) *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. WODC, Den Haag

Lavorgna, A. (2013). *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*. University of Trento. Doctoral School of International Studies

Lavorgna A (2014a) Internet-mediated drug trafficking; towards a better understanding of new criminal dynamics. *Trends in Organized Crime* 17(4):250–270

Lavorgna A (2014b) Wildlife trafficking in the internet age: the changing structure of criminal opportunities. *Crime Science* 3(5):1–12

Lavorgna A (2015a) Organised crime goes online: realities and challenges. *Journal of Money Laundering Control* 18(2):153–168

Lavorgna A (2015b) The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. *Eur J Criminol* 12(2):226–241

Leukfeldt ER (2014) Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime* 17(4): 231–249

Leukfeldt, E.R. (red.) (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing

Leukfeldt ER, Lavorgna A, Kleemans ER (2017a) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research* 23(3):287–300

Leukfeldt ER, Kleemans ER, Stol WP (2017b) A typology of cybercriminal networks: from low tech locals to high tech specialists. *Crime Law Soc Chang*. https://doi.org/10.1007/s10611-016-9646-2

Leukfeldt, E.R., E.R. Kleemans, & W.P. Stol (2017c) Cybercriminal networks, social ties and on-line forums: social ties versus digital ties within phishing and malware networks. *Br J Criminol*. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E.R., E.R. Kleemans & W.P. Stol (2017d) *Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis*. Crime, Law and Social Change. https://doi.org/10.1007/s10611-016-9647-1

Leukfeldt ER, Kleemans ER, Stol WP (2017e) The use of online crime markets by cybercriminal networks: a view from within. *Am Behav Sci*

Lu Y, Luo X, Polgar M, Cao Y (2010) Social network analysis of a criminal hacker community. *J Comput Inf Syst* 51(2):31–41

Lusthaus J (2012) Trust in the world of cybercrime. *Global Crime* 13(2):71–94

Lusthaus J (2013) How organised is organised cybercrime? *Global Crime* 14(1):52–60

Lusthaus J (2019) Industry of anonymity. *Inside the business of cybercrime*. Harvard University Press, Cambridge

Lusthaus J, Varese F (2017) *Offline and local: the hidden face of cybercrime*. Policing: A Journal of Policy and Practice. https://doi.org/10.1093/police/pax042

McCusker R (2006) Transnational organised cyber crime. *Distinguishing threat from reality, in: Crime, Law and Social Change* 46(4):257–273

Morselli C (2005) *Contacts, opportunities, and criminal Enterprise*. University of Toronto Press, Toronto

Morselli (2009) *Inside criminal networks*. Springer Verlag, New York

Odinot G, Verhoeven MA, Pool RLD, De Poot CJ (2017) *Organised cybercrime in the Netherlands: empirical findings and implications for law enforcement*. WODC, Den Haag

Paoli L (2003) *Mafia brotherhoods: organized crime, Italian style*. Oxford University Press, New York

Paoli L (ed) (2014) *The Oxford handbook of organized crime*. Oxford University Press, Oxford

Przepiorka W, Norbutas L, Corten R (2017) Order without law: reputation promotes cooperation in a Cryptomarket for illegal drugs. *Eur Sociol Rev* doi: 10.1093/esr/jcx072

Reuter P (1983) *Disorganized crime: illegal markets and the mafia*. MIT Press, Cambridge

Smith, D.C., Jr. (1975). *The mafia mystique*. New York: Basic Books

345 Soudijn MRJ, Monsma E (2012) Virtuele ontmoetingsuimtes voor cybercriminelen. [Virtual meeting places for cybercriminals. *Tijdschrift voor Criminologie* 54(4):349–360

Soudijn MRJ, Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. *Trends in Organized Crime* 15(2–3):111–129

Töttel U, Bulanova-Hristova G, Flach G (eds) (2016) *Research conferences on organised crime at the Bundeskriminalamt in Germany, volume III, transnational organised crime, 2013–2015*. Bundeskriminalamt (available as pdf at, Wies baden https://www.polizeide/SharedDocs/Downloads/EN/Publications/Other/ResearchConferencesOnOrganised-Crime2013-2015.html

van de Bunt HG (2007) Muren van Stilzwijgen. In: van de Bunt HG, Spierenburg P, van Swaan-ingen R (eds) *Drie perspectieven op sociale controle*, pp 133–136 Den Haag: Boom Juridische Uitgevers

van de Bunt HG (2010) Walls of secrecy and silence: the Madoff case and cartels in the construction industry. *Criminol Public Policy* 9(3):435–453

Bunt, H.G. van de, & Kleemans, E.R. (2007). *Georganiseerde criminaliteit in Nederland: Derde rapportage op basis van deMonitor Georganiseerde Criminaliteit.* [Organised Crime in the Netherlands, 3rd report based on the Monitor Organised Crime] Den Haag: Boom Juridische uitgevers

Varese F (2011) *Mafias on the move.* Princeton University Press, Princeton NJ / Oxford

Wehinger, F. (2011). *The dark net: Self-regulation dynamics of illegal online markets for identities and related services.* Intelligence and security informatics conference. https://doi.org/10.1109/EISIC.2011.54

Werner, Y. & Korsell, L. (2016). Cyber-OC in Sweden. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, & L. Korsell *(red), Cyber-OC - Scope and manifestations in selected EU member states* (p. 101–164). Wiesbaden: Bundeskriminalamt

Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. *IEEE International Conference on Intelligence and Security Informatics (ISI)*, 60–65

PUBLICATION HISTORY