Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions

Debate

Organised Cybercrime and Social Opportunity

Structures: A Proposal for Future Research Directions

Rutger Leukfeldt*

Abstract: Little empirical research has been done on organised cybercrime. Anecdotes, unsubstantiated assumptions and unverifiable reports from technology companies dominate views on this topic. This article goes back to basics and outlines what the expectations are according to criminological theory. These expectations can be used as a framework for empirical studies. Theory shows that at least two different types of networks are likely to exist: (1) locally rooted all-rounders and (2) international specialists. This is confirmed by a number of case studies analysed in this article. Offender convergence settings seem to play a crucial role. Therefore, perhaps the most important question for future empirical research is what role these meeting places play in the development of cybercriminal networks. Furthermore, the question is whether more types of networks exist and if they have different characteristics (structure, hierarchy, type of offenders). Systematic analyses of cybercriminal networks may provide an important insight into these matters and may help us understand how cybercriminal networks arise and develop.

Keywords: Organised crime – cybercrime – criminal networks – social opportunity – structure

*Rutger Leukfeldt is a researcher at the Cyber Safety Research Group of NHL University of Applied Sciences and the Dutch Police Academy. He is also a PhD-candidate at the Open University of the Netherlands. Email: E.R.Leukfeldt@nhl.nl

The European Review of Organised Crime 2(2), 2015, 91-103

ISSN: 2312-1653

Introduction

The image of the classic Italian-American Mafia family with one leader who controls the captains and soldiers who are in the hierarchy below him has long dominated the public view on organised crime. Two committees of the United States of America's Senate explain this perception: in 1950, the Kefauver Committee held a public inquiry that concluded that organised crime in America was committed by one national Italian syndicate while second committee, called the McLellan Committee (1963), relied heavily on the statements of Joseph Valachi, who was part of a Genovese crime family. This committee confirmed the Kefauver picture of organised crime.

Scientific studies nuanced the prevailing image of this form of organised crime (Fijnaut et al., 1996). Studies showed that it was more complicated than a simple pyramid-like crime family structure; the picture was more complex. These insights changed investigative and intervention strategies. A closed mafia family with a clear hierarchy requires a different approach than that of a more fluid network of criminals, who occasionally work together[1].

Presently, history seems to be repeating itself. There is a new crime area that is shrouded in mystery: cybercrime—and particularly organised forms of cybercrime[2]. Commentators acknowledged several decades ago that criminals (ab)use new technology (for example, Akdeniz, 1996; Wall, 1997; Mann and Sutton, 1998; Gattiker and Kelley, 1999; Capeller, 2001; Grabosky, 2001). It is, however, remarkable that empirical research into criminal networks that operate over the internet is scarce. As McCusker (2006) and Van der Hulst and Neve (2008) have already concluded, there is insufficient data available to establish links between organised crime and cybercrime. Cybercriminal networks gain more and more attention from scholars from different disciplines studies (among some recent studies, see Peretti, 2008; Holt and Lampke, 2009; Lu et al., 2010; Soudijn and Zegers, 2012; Décary-Hetú and Dupont, 2012; Yip et al,. 2012; Lusthaus, 2012; Afroz, 2013; Leukfeldt, 2014). However, a large part of the literature available is based on logical reasoning, hypotheses, assumptions, and anecdotes. Just as it was back in the 20th century regarding offline organised crime, in the 21st century organised cybercrime is full of myths. A study in which forty interviews with experts were held with representatives from the justice sector, the banking sector, the private security industry and researchers in the field of cybercrime, for example shows that there are many different stories circulating about such groups (Leukfeldt, 2013). These range from pyramid-like organisations with one elusive mastermind to fluid networks that are constantly in different combinations carrying out attacks without central control; or international networks with non-Dutch perpetrators to locally organised Dutch networks and links with the top 600 of the most common offenders in Amsterdam; and from recruiting money mules using digital means to recruitment in schoolyards. These divergent images are probably partly caused by the many anecdotes that exist in the cybercrime field and the multitude of grey literature (e.g., books like DarkMarket, but also trend reports from Symantec, McAfee, and Microsoft— organisations whose core business is to protect us from the same threats they describe).

It is clear that more empirical research is needed to clarify the picture of organised forms of cybercrime. Therefore, this article provides a theoretical framework to study cybercriminal networks empirically. The next section goes back to basics and presents criminological theory about criminal

networks. Thereafter, based on criminological theory and available scientific cybercrime case studies, the impact of digitisation on criminal networks will be analysed. The last section contains the conclusion and discussion part of this article.

Criminal Networks: Social Opportunity Structures

In criminology, there does not exist one unambiguous answer to the question why people exhibit criminal behaviour and what the underlying factors are that produce this behaviour. Besides general theories that explain why people commit crime under certain circumstances, there are also theories that focus specifically on the development and functioning of criminal groups.

Empirical research shows that social ties and social opportunities play an important role within the formation and functioning of criminal networks. Social ties provide access to criminal opportunities and the social network is an opportunity structure that facilitates various types of crime (Ianni and Reuss-Ianni, 1972; Kleemans and De Poot, 2008; Edwards and Levi, 2008; Bouchard and Morselli, 2014). Criminal organisations, therefore, should be seen in their social and societal context. It is assumed that aspects central to this include the offenders themselves, the illegal partnership in which they operate and the interaction with their social environment. Kleemans and De Poot (2008) use the concept of social opportunity structures for this purpose.

The concept of social opportunity structures combines opportunity theory with social network theory. Opportunity theory (Felson and Clarke, 1998) is a further development of the routine activities theory. This theory is based on one principle: temptation and opportunities to prompt people to actually do this crime. There are also a number of theories that underlie the social network theory (for a more comprehensive theoretical reflection, see for example Van der Hulst, 2008; McGloin and Kirk, 2010; Scott and Carrington, 2011). An influential theory is the rational choice theory (Coleman, 1973; 1990). This theory assumes that people are rational, goal-oriented beings who are guided by a cost-benefit analysis. Relations with other people are, according to Van der Hulst, an instrumental means to achieving goals. In line with this, social exchange theory explains that people are constantly exchanging all kinds of tangible and intangible goods or services with each other (Blau, 1964; Cook and Whitmeyer, 1992). According to Van der Hulst (2004; 2008), this ranges from money or information (instrumental resources) to giving or receiving social support (an expressive resource). The benefits arising from social relationships are called “social capital”: “If you can’t do something by yourself, then use others who do have the necessary resources to help you” (Van der Hulst, 2008:12). Social capital consists of contacts with others that are of value because of their socioeconomic status, education, specific knowledge and skills, because they are financially wealthy or have (political) influence. According to the theory of social capital (Van der Hulst, 2008), people who have many valuable contacts are more successful in our society. This is true not only for individuals but also for groups, neighbourhoods and (criminal) organisations.

Social Opportunities and Cybercriminal Networks

The social opportunities structure perspective has been created based on decades of systematic empirical investigation into organised crime (Kleemans et al., 1998; 2002; Kleemans and Van de Bunt, 1999; 2003; Van de Bunt and Kleemans, 2007; Edwards and Levi, 2008; Kruisbergen et al., 2012; Bouchard and Morselli, 2014). This section outlines expectations regarding cybercriminal networks based on this empirical foundation.

In this section, the structure, recruitment, and growth of criminal networks will be discussed. First we describe what is known from the literature about traditional criminal networks, followed by case studies which show the similarities and differences when it comes to cybercriminal networks.

The structure of cybercriminal networks: fluid networks and nodes

In empirical research into criminal networks in the offline world, Kleemans et al. (1998, 2002), Van de Bunt and Kleemans (2007) and Kruisbergen et al. (2012) found transnational partnerships that were less hierarchical, less durable, and less fixeddelineated than is implied by traditional models. Despite the lack of pyramid-like structures, the researchers did find dependency relationships. Some people have a more central role than others within a network. These individuals are nodes within the network and may have a role in several different networks. This central role belongs to those who have resources on which others depend: money, knowledge, or contacts (indeed, social capital, see Van der Hulst, 2008). Roles such as financers, financial advisors, underground bankers, document forgers and transporters exemplify this. Van de Bunt and Kleemans (2007) add that there are people who are important to criminal networks because they can bridge gaps in social structures, for example, geographic and/or social barriers between countries, between different ethnic groups, and between the lower and upper world.

It can be assumed that cybercriminal networks have key actors with a central role because of their specific social capital. Several case studies show that the internet provides an opportunity structure for decentralised, flexible networks of loosely organised criminals who collaborate and distribute work based on knowledge and skills. The study of Soudijn and Monsma (2012), for example, describes a social network analysis of an online forum of criminals engaged in identity theft (the forum was intercepted by the Dutch High Tech Crime Team). The authors conducted a social network analysis and determined among other things the out-degree, in-degree and betweenness (a way to map the centrality characteristics of a network). The analysis shows that forum members over the years continue to expand the number of relationships they have. It also appears that forum members are on average located relatively close to other possible pairs. The members, according to the authors, fully utilise the possibilities to build new contacts and expand their network.

Veterans and members with higher status take a more central position. However, the authors emphasise that newcomers manage to secure a central position relatively quickly. Furthermore, the authors doubt whether individuals who can bridge holes in social structures are still so important. This is in contrast to traditional criminal networks. Lu et al. (2010) analysed the social network of a group of cyber criminals who operated on the Shadow Crew forum, a forum on which, among other things, stolen identity information was exchanged. The analysis of Lu et al is based on open sources (newspaper reports, articles, and court reports). These authors also determined the out-degree, in-degree and betweenness of members. In addition, they looked at the closeness centrality (which is the distance from one actor to other actors in the network) and the eigenvector centrality (the number of connections from a person to central people in the network). In addition, subgroups within the social network were also investigated to see whether they existed. Analysis showed that it is a decentralised network. However, there are a number of nodes: actors with a leading role or with a brokerage function within the network. Different actors could be pinpointed who had other members under their influence. In addition, a number of subgroups within the social network could be identified.

Yip et al. (2012) analysed four criminal forums which were logged by the English police. The authors had access to the anonymous private messaging records from four carding fora: Shadow Crew, Carderplanet, Cardersmarket, and DarkMarket. Based on private messages between the members of the fora, the authors looked at different characteristics of the network (e.g., degree distribution, assortativity, rich club phenomenon, and cohesive subgroups). These authors also conclude that many members have lots of contacts and that there are few members with a central role. The authors note, however, that reputation and trust within the forum is important and reliable sellers therefore have to be members of the forum for a long time to build up a good reputation.

The studies described in this section show that, just as in traditional networks, there are still important actors (nodes) with a role as bridge builder. The structure of traditional and cybercriminal networks do have similarities. However, the role of these central actors might be of less importance because members of fora can grow their own network (and thus gain social capital) relatively fast. For the growth of a network, this would mean that the traditional restrictions of social networks become less important. Of course, this only applies to criminals who already have access to the forum. To get into a forum, an existing member must vouch for the aspirant member. New members therefore must already know someone in that specific criminal world. This raises the question of whether cyber networks are more fluid than traditional networks.

Recruitment and growth

People get involved in criminal networks in different ways (Kleemans et al., 1998; 2002; Van de Bunt and Kleemans, 2007; Kruisbergen et al., 2012; Edwards and Levi, 2008; Bouchard and Morselli, 2014). It is usually not a question of military-like recruitment with corresponding growth opportunities. Social relations and network dynamics ensure that the recruitment of new offenders and the creation of new partnerships are not the same as traditional models claim. Kleemans et al.

(1998) showed that family, friends and acquaintances work together and introduce each other to others. Van de Bunt and Kleemans (2007) analysed 92 starters in organised crime and concluded that they became involved in organised crime in different ways: through pre-existing social relationships, work and work-related relationships, hobbies or other activities, life events (e.g., bankruptcy) or by deliberate recruitment. No empirical research has been done on the opportunity structures that provide people with entry into a cybercriminal network. Based on literature of traditional criminal networks, the expectation is that social ties provide the opportunity structure for entering a cybercriminal network. On the other hand, however, the internet eliminates the barriers of time and space and makes it possible to have accomplices throughout the world. Indeed, new digital offender convergence settings have arisen where criminals can meet, recruit new members and plan new attacks (Peretti, 2008; Holt and Lampke, 2009; Soudijn and Zegers, 2012; Soudijn and Monsma, 2012).

The case studied in Leukfeldt (2014) shows that social relationships may indeed be important for the recruitment and growth of cybercriminal networks. Despite the fact that the criminals where involved in phishing, the recruitment of new criminals largely took place on the streets. All kinds of acquaintances from the traditional Amsterdam criminal environment are used to carry out the non-digital part of the crime (cashing money, recruiting money mules, getting information about potential victims) and meetings with facilitators take place in real world cafes. As mentioned before, Soudijn and Monsma (2012) and Yip et al. (2012) show, however, that the process to get into a criminal partnership can be different in the digital world. Newcomers are able to get into contact with existing members relatively quickly and are able to create a central role for themselves. The authors note that, in contrast to physical networks, central people are not that important. Apparently, getting new contacts is easier in the virtual world then it was in the physical world. The accumulation of social capital is thus still important, but this process can be faster in digital offenders convergence settings than before.

The central role of offender convergence settings: building trust and bridging gaps

The literature shows that social relationships play an important role in the development of criminal networks. Existing contacts, however, do not always provide enough possibilities, especially in transnational crimes. The problem with social relationships, according to Van de Bunt and Kleemans (2007), is that they are highly clustered. They can, for example, be limited to relationships with people in the same country or region. The capabilities of any social cluster are therefore limited. Hence, relationships have to be formed with “outsiders”. Eventually, in order to grow and to get more criminal opportunities, contact must be made outside the existing social relations.

When it comes to new contacts, places where criminals meet play an important role. These types of meeting places are referred to as offender convergence settings. According to Felson (2003) offender convergence settings are important because they provide structure and continuity.

Offender convergence settings ensure that newcomers can establish links with criminals present there and enter existing criminal networks or form new criminal alliances (Felson, 2003; 2006; Von Lampe, 2009). Offender convergence settings are physical locations where criminals can meet, for example, a cafe or coffee shop.

The internet has its own offender convergence settings, for example, fora where cybercriminals meet, exchange information or make plans for committing crimes (Peretti, 2008; Holt and Lampke, 2009; Lu at al., 2010; Soudijn and Zegers, 2012; Soudijn and Monsma, 2012; Decary-Hetu and Dupont, 2012; Yip et al., 2012; Lusthaus, 2012; Afroz et al., 2013). These studies show that fora play an important role in enabling international attacks. Key actors provide their specific expertise and their own social networks including criminals with whom they have worked before.

Trust plays a major role when it comes to looking for reliable accomplices. Therefore, an outsider's reputation is very important. Soudijn and Zegers (2012), Soudijn and Monsma (2012), and Yip et al. (2012) showed how the search for other reliable criminals on different fora works. The reliability of a member can be determined using a peer-review system and various statuses a member could earn. Members can rate offered goods and services. Someone who has many positive reviews is seen as more reliable than someone who has not. The status indicates the reliability of a member and is also related with the rights that member has on the forum. Statuses include newcomers, members, trusted members, but also scammers. Over the years, one's status may change. The peer reviews and statuses are linked to the username.

Offender convergence settings, therefore, ensure that new criminal contacts can be acquired, that new social capital enters the criminal group and that restrictions of social networks can be bridged. Empirical research into traditional organised crime shows that access to those meeting places affects the growth and development of a network. In their analysis of 68 executives within organised crime, Van de Bunt and Kleemans (2007) show that a part of this group grew to become "local heroes" while another part gained a position at a national or even international level. Within their own region, the "local heroes" make profits from many different criminal activities, but they have no contacts outside their region and have no expertise on which others depend. A condition for growing into the international level is having contacts with brokers who give access to new export markets, or who have capital or expertise.

Literature on cybercriminal networks show that fora can serve as offender convergence settings for cybercriminals and play an important role in most of the cases studied (Peretti, 2008; Holt and Lampke, 2009; Soudijn and Zegers, 2012; Soudijn and Monsma, 2012). Fora enable criminals from different countries with different expertise to meet. This does not mean that all existing cybercriminal networks use such fora. Nor is it known whether the criminals in these fora also meet each other via offline offender convergence settings. The study of Leukfeldt (2014), for example, shows that a Dutch group of phishers met each other in the streets of Amsterdam and only used the internet to commit their frauds. An interesting question therefore is whether online and offline offender convergence settings play a role in cybercriminal networks and, if so, which role they play.

If not all criminal networks (are able to) use fora, it is likely that the cybercriminal networks have local and international partnerships, just as they do in traditional organised crime. So the questions are whether cyber criminals (only) come together online, which sub variants there are (the initial encounter online, then an offline collaboration, etc.) and what this means for the growth and criminal opportunities of the criminal network.

Conclusion and Discussion

Although more and more scholars have discovered the cybercrime field, there still is too little empirical research to make robust statements about cybercriminal networks. Therefore, this article outlines what to expect from cybercrime groups, based on criminological theory on criminal networks. These expectations can be used as a basis for further empirical studies.

To understand the nature of cybercriminal networks, it is important to understand the extent to which social opportunities play a role in the origin and growth of cybercriminal networks in our digitised society. These opportunities may affect the network at various levels. On the one hand, they may affect the structure of a network (pyramidal, fluid with important actors, completely fluid), but on the other hand they can also affect which type of criminals become part of the network (because growth and recruitment are different).

Research into traditional criminal networks shows that these networks are not static and pyramidal; they are more fluid than that. However, within these fluid networks there are still a few players who perform the important function of broker (arranging contacts between criminals in different countries, providing new markets, etc.). Some case studies of cybercriminal networks show that criminals are now able to set up an international operation through a forum relatively easily. Authors also suggest that the function of broker has diminished. As a result, a shift may take place from fluid networks with some key players (brokers) to completely fluid networks where all participants are able to get into contact with each other. Fora could therefore provide the opportunity structure for a new type of criminal network. Unfortunately, existing case studies alone are not enough to get a clear picture. First ,a systematic review of current cybercriminal networks will have to be done in order to map all types of networks. The characteristics of a network can be related to the origin and growth of a network. Are the “old fashioned” social ties still that significant to cybercriminals who can meet each other online? What role do digital offender convergence settings play within cybercriminal networks, and what does this mean for the recruitment of new criminals?

Based on theories about criminal networks, it is expected that there are at least two types of networks. This picture is confirmed by the cases presented in this article. Perhaps the single most important question in empirical research should be about the role that digital offender convergence settings play within cybercriminal networks. Access to brokers who bridge gaps between social

networks determine the growth and development of criminal networks. If not all criminal networks are able to use such online venues, then—just like in traditional organised crime—local cyber partnerships will exist alongside international networks. The question is whether these different types of cybercriminal networks also have different characteristics (structure, type offenders, etc.) and whether there are other (intermediate) variants. Systematic analysis of cybercriminal networks can offer insight here, for instance, in the way research into traditional organised crime has been done for decades in the Netherlands (Fijnaut et al. 1996; Kleemans et al., 2002; Van de Bunt and Kleemans, 2007; Kruisbergen et al., 2012).

Answering the questions formulated in this last section should clarify the role social opportunities play in the origin and growth of cybercriminal networks. This will also reveal the role of the internet and whether the importance of social relationships has diminished. At the moment there is too little knowledge about this. Increasing knowledge about these elements will ensure that we are able to better understand what cybercriminal network are really like, and what countermeasures can be taken. This is not only of academic interest; it also provides those law enforcement an insight into which counter strategies work best. It goes without saying that an international network of experts will offer different opportunities and challenges for law enforcement agencies than locally rooted networks of criminal allrounders.

References

Afroz S, Garg V, McCoy D, and Greenstadt R (2013) *Honor Among Thieves: A Common's Analysis of Cybercrime Economies.* IEEE eCrime Research Summit, San Francisco, CA.

Akdeniz Y (1996) Computer Pornography: a Comparative Study of the US and the UK Obscenity Laws and Child Pornography Laws in Relation to the Internet.

International Review of Law Computers & Technology 10 (2): 235-261.

Andresen MA and Felson M (2010) Situational crime prevention and co-offending. *Crime patterns and analysis* 3(1): 3-13.

Blau PM (1964) *Exchange and power in social life*. New York: John Wiley and Sons.

Bouchard M and Morselli C (2014). Opportunistic structures of organized crime. In Paoli L (ed.) *The Oxford Handbook of Organized Crime*. Oxford / New York: Oxford University Press.

Capeller W (2001) Not Such a Neat Net: Some Comments on Virtual Criminality. In: *Social and Legal Studies* 10: 229-42.

Coleman J (1973) *The mathematics of collective action*. London: Heinemann.

Coleman J (1990) *Foundations of social theory*. Cambridge (MA): Harvard University Press.

Cook KS and Whitmeyer JM (1992) Two approaches to social structure: Exchange theory and network analysis. *Annual Review of Sociology* 18: 109-127.

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

Edwards A and Levi M (2008) Researching the organization of serious crimes.

Criminology and Criminal Justice 8(4): 363-388.

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

Felson M (2006) *The ecosystem for organized crime* (HEUNI paper nr 26). Helsinki: HEUNI.

Felson M and Clarke RV (1998) Opportunity makes the thief: Practical theory for crime prevention. In: B. Webb (red.) *Police Research Series*, paper 98. London: Home Office.

Fijnaut CJCF, Bovenkerk F, Bruinsma GJN, and Van de Bunt HG (1996) *Georganiseerde criminaliteit in Nederland, eindrapport, bijlage VII van:*

Enquêtecommissie opsporingsmethoden, Inzake Opsporing. [Organized crime in the Netherlands] Den Haag: du Uitgevers.

Gattiker UE and Kelley H (1999) Morality and computers: Attitudes and differences in judgments. In: *Information System Research* 10(3): 233-254.

Grabosky PN (2001) Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies* 10: 251-56.

Holt JT and Lampke E (2009) Exploring stolen data markets online: products and market forces. *Criminal Justice Studies 23*(1): 33-50.

Kleemans ER and De Poot CJ (2008) Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology* 5(1): 69-98.

Kleemans ER and Van de Bunt HG (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(2): 19-36.

Kleemans ER and Van de Bunt HG (2003) The social organisation of human trafficking. In Siegel D, Van de Bunt HG, and Zaitch D (ed.) *Global organized crime: Trends and developments.* Boston: Kluwer Academic Publishers.

Kleemans ER, Brienen MEI, Van de Bunt HG, Kouwenberg RF, Paulides G, and Barensen J (2002) *Georganiseerde criminaliteit in Nederland. Ttweede rapportage op basis van de WODC-monitor.* [Organized crime in the Netherlands. Second report based on the WODC monitor] Den Haag: WODC.

Kleemans ER, Van der Berg AEIM, and Van de Bunt HG (1998) Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC monitor. [Organized crime in the Netherlands. Report based on the WODC monitor] Den Haag: WODC.

Kruisbergen EW, Van de Bunt HG, Kleemans ER, and Kouwenberg RF (2012)

Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit. [Organized crime in the Netherlands.

Fourth report based on the WODC monitor] Den Haag: Boom Lemma.

Leukfeldt ER (2013) Cybercriminele samenwerkingsverbanden. Barrières tegen cybercrime in het digitale betalingsverkeer. Verslag van het eerst jaar van KVDB-deelproject 1 (interne notitie). [Cybercriminal networks. Barriers against cybercrime and online banking. Report KVDB year one] Heerlen/Leeuwarden/Apeldoorn: Open Universiteit / NHL Hogeschool / Politieacademie.

Leukfeldt ER (2014) *Cybercrime and social ties*. Phishing in Amsterdam. *Trends in Organized Crime* (online first). DOI: 10.1007/s12117-014-9229-5.

Lu Y, Luo X, Polgar M, and Cao Y (2010) Social network analysis of a criminal hacker community. *Journal of Computer Information Systems* (2010): 31-41. Lusthaus J (2012) Trust in the world of cybercrime. *Global Crime* 13(2): 71-94.

Mann D and Sutton M (1998) Netcrime: More Change in the Organization of Thieving. *British Journal of Criminology* 38: 201-29.

McCusker R (2006) Transnational organised cyber crime: distinguishing threat from reality. *Crime Law and Social Change* 46(4-5): 257-273.

McGloin JM and Kirk DS (2010) An Overview of Social Network Analysis. *Journal of Criminal Justice Education* 21(2): 169-181.

Peretti KK (2008) Data breaches: What the underground world of “carding” reveals.

Santa Clara Computer and High Technology Law Journal 25: 345-414.

Reiss AJ (1988) Co-offending and criminal careers. In Tonry M and Morris N (eds.) *Crime and Justice. A Review of Research*. Chicago: Chicago University Press. Reiss AJ and Farrington DP (1991) Advancing knowledge about co-offending:

results from a prospective longitudinal survey of London males. *Journal of criminal law and criminology* 82: 360-395.

Scott J and Carrington PJ (2011) *The SAGE Handbook of Social Network Analysis*. London: SAGE Publications.

Soudijn MRJ and Monsma E (2012) Virtuele ontmoetingsuimtes voor cybercriminelen. In: *Tijdschrift voor Criminologie*. [Vitual meeting places for cyber criminals] 54(4): 349-360.

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

Van de Bunt HG and Kleemans ER (2007) *Georganiseerde criminaliteit in Nederland, derde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [Organized crime in the Netherlands. Third report based on the Monitor Organized Crime] Den Haag: WODC.

Van der Hulst R.C and Neve RJM (2008) *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders.* [High tech crime: review of the literature of types of crime and their offenders] Den Haag: WODC.

Van der Hulst RC (2004) *Gender differences in workplace authority: An empirical study on social networks*. Groningen: Rijksuniversiteit Groningen.

Van der Hulst RC (2008) Sociale netwerkanalyse en de bestrijding van criminaliteit en terrorisme. [Social network analysis and the fight against crime and terrorism] *Justitiële verkenningen* 34(5): 3-20.

Von Lampe K (2009) Human capital and social capital in criminal networks:

introduction to the special issue on the 7th Blankensee Colloquium. *Trends in Organized Crime* 12(2): 93-100.

Wall DS (1997) Policing the virtual community: the Internet, Cyber Crimes and the policing of Cyberspace. In Francis P Davies P and Jupp V (eds.) *Policing Futures, the Police, Law Enforcement and the Twenty-First Century*. London: Macmillan.

Wall DS (2001) Cybercrimes and the Internet. In Wall DS (ed.) *Crime and the Internet*. New York: Routledge.

Weerman F and Kleemans ER (2002) Criminele groepen en samenwerkingsverbanden. Een overzicht. [Criminal groups and criminal organisations. An overview] *Tijdschrift voor Criminologie*, 44(2), 114-127.

Yip M Shadbolt N and Webber C (2012) Structural Analysis of Online Criminal Social Networks. ISI 2012, June 11-14, 2012, Washington.