VU Research Portal

Cybercriminal networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks

Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.PH.

published in

British Journal of Criminology
2017

DOI (link to publisher)

[10.1093/bjc/azw009](https://doi.org/10.1093/bjc/azw009)

document version

Publisher's PDF, also known as Version of record

document license

Article 25fa Dutch Copyright Act

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. PH. (2017). Cybercriminal networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, 57(3), 704-722. <https://doi.org/10.1093/bjc/azw009>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

CYBERCRIMINAL NETWORKS, SOCIAL TIES AND ONLINE FORUMS: SOCIAL TIES VERSUS DIGITAL TIES WITHIN PHISHING AND MALWARE NETWORKS

E. RUTGER LEUKFELDT*, EDWARD R. KLEEMANS and WOUTER P. STOL

Online forums serve as offender convergence settings for cybercriminals, but it is unknown whether all cybercriminal networks use forums. Important questions are how cybercriminals meet, how cybercriminal networks develop and what this means for the criminal capabilities of these networks. To gain insight into these questions, we analysed 18 criminal investigations into phishing and malware networks and developed four models of growth. Social ties still play an important role in the origin and growth of the majority of networks. Forums, however, also play a significant role in a number of networks, for example, to find suitable co-offenders or to get into contact with enablers. Criminals with access to forums are able to increase criminal capabilities of their network relatively quickly.

Keywords: cybercrime, criminal networks, social opportunity structure, online forums, phishing, online banking

Introduction

Have cybercrime and the digital era changed the ways in which criminals meet and collaborate? Empirical research has provided ample evidence that social ties play a crucial role in the formation and functioning of criminal networks (see, for example, Ianni and Reuss-Ianni 1972; Edwards and Levi 2008; Kleemans and De Poot 2008; Bouchard and Morselli 2014). However, the Internet and Information and Communication Technology (ICT) now make it possible for people to connect without the restrictions of geographical proximity and existing social networks (see Wall 2007; Holt and Bossler 2014; Williams 2016). What then does this mean for criminal networks?

Traditional origin and growth processes rely heavily on building trust and are related to existing social contacts such as family, friends and co-workers, while ‘offender convergence settings’—physical locations, such as cafes and bars, where criminals can meet—are used to forge contacts outside people’s initial social cluster (Felson 2003). The Internet provides specific offender convergence settings, such as forums where hackers and carders can meet to exchange information or make plans for committing crimes (Peretti 2008; Holt and Lampke 2009; Lu *et al.* 2010; Décary-Hetú and Dupont 2012; Soudijn and Monsma 2012; Soudijn and Zegers 2012; Yip *et al.* 2012).

*E. Rutger Leukfeldt, PhD candidate, Open University of the Netherlands, PO Box 2960, 6401 DL Heerlen, the Netherlands, Researcher, Cyber Safety Research Group of NHL University of Applied Sciences, PO Box 1080, 8900 CB Leeuwarden, the Netherlands and Police Academy of the Netherlands, PO Box 834, 7301 BB Apeldoorn, the Netherlands; e.r.leukfeldt@nhl.nl; Edward R. Kleemans, Professor, Serious and Organized Crime and Criminal Justice, VU University Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, the Netherlands; Wouter P. Stol, Professor, Police Studies, Open University of the Netherlands, PO Box 2960, 6401 DL Heerlen, the Netherlands, Head, Cyber Safety Research Group of NHL University of Applied Sciences, PO Box 1080, 8900 CB Leeuwarden, the Netherlands and Police Academy of the Netherlands, PO Box 834, 7301 BB Apeldoorn, the Netherlands.

Cybercriminals can also browse through forum lists of other (trusted) criminals, each with their own specialities and ratings from earlier jobs or services. But do all cybercriminal networks use these forums? How relevant have social ties remained within cybercriminal networks? And what do these developments mean for the growth and criminal opportunities of cybercriminal networks?

This article aims to unravel the ties within certain forms of cybercriminal networks. It is not, however, comprehensive as there are simply too many different types of networks. These range, for example, from networks threatening to shut down the websites or online systems of banks or major retailers to networks engaged in producing and distributing child pornography. As this study is part of the Research Programme on the Safety and Security of Online Banking, it examines networks carrying out phishing and malware attacks on online banking systems. Phishing is the process whereby criminals use digital means such as e-mail to try to retrieve users' personal information by posing as a trusted authority (see, for example, [Lastdrager 2014](#)). The criminal may send an e-mail that appears to originate from a trusted party such as a bank. This e-mail refers to a problem with the user's online bank account (such as the need for a security upgrade), combined with a request for the user to take immediate action to resolve the issue (for example, by logging in using the link in the e-mail to update the account security). The aim of the attack is to intercept user credentials. These can also, however, be intercepted in a more technological way as criminals can use 'malware' (malicious software) such as viruses, worms, Trojan horses and spyware to obtain access to credentials or manipulate entire online banking sessions.

This article provides an analysis of cybercriminal networks, based on 18 criminal investigations conducted by the Dutch police, in order to gain insight into ties between members, the origin and growth of the networks and the use of digital offender convergence settings. Section '(Cyber)criminal Networks and Social Opportunity Structures' outlines what is known about the origin and growth of traditional criminal networks and the role of offender convergence settings, while Section 'Data and Methods' describes the data and methods used in this study. Section 'Empirical Results' focuses on the composition, origin and growth of cybercriminal networks and describes the role played by forums in such networks, while Section 'Conclusion and Discussion' contains the main conclusions and suggests aspects for further research.

(Cyber)criminal Networks and Social Opportunity Structures

Criminal networks and social opportunity structures

Besides general theories seeking to explain why people commit crimes in certain circumstances, there are also criminological theories focusing specifically on the development and functioning of criminal networks. [Kleemans and Van de Bunt \(1999\)](#), for example, emphasize the importance of social relationships and explain why criminal organizations should be viewed within their social and societal context, with the central aspects being taken to include offenders themselves, the illegal partnerships in which they operate and the interaction with their social environment. [Kleemans and De Poot \(2008\)](#) refer to the concept of the 'social opportunity structure' as playing a major role in criminal networks. Social ties provide access to criminal opportunities and the social

network is an opportunity structure that facilitates various types of crime (for an overview, see [McGloin and Kirk 2010](#); [Scott and Carrington 2011](#)).

As social ties seem to play an important role in traditional criminal networks, this article seeks to unravel the ties within cybercriminal networks by looking at them from various perspectives. First, of course, there are the direct ties between members of the network. Are they, for example, family of each other, co-workers or complete strangers? A second way is to look at the origin of the network. Why are these individuals working together? How, where and why did their cooperation start? The recruitment process is also important. How are new members recruited after the core members of the network get together? Finally, the role of forums is of interest. Which forums do criminals use, and what does this mean for the ties within the network?

These elements—direct ties, origin, growth and use of forums—are interlinked and influence each other, and are each discussed separately. Based on the literature, this section¹ briefly describes what is known about the origin and growth of traditional criminal networks and the role of offender convergence settings. Where possible, case studies of cybercriminal networks are examined so as to establish whether these traditional views also apply to such networks.

Origin and growth

Empirical research into criminal networks shows that there are various ways in which people become involved in these networks. It is not usually a question of military-like recruitment, with corresponding growth opportunities. [Kleemans and Van de Bunt \(1999\)](#) found that family, friends and acquaintances worked together and introduced each other to others. [Kleemans and De Poot \(2008\)](#) analysed 92 starters in organized crime and concluded that there were various ways in which individuals became involved in crime. These included through pre-existing social relationships, work and work-related relationships, hobbies or leisure activities, life events such as bankruptcy, and also sometimes through deliberate recruitment.

However, the studies by [Lu et al. \(2010\)](#), [Soudijn and Monsma \(2012\)](#) and [Yip et al. \(2012\)](#) showed that the process of becoming involved in all sorts of cybercriminal partnerships can be different from traditional criminal networks. In the digital world, newcomers are able to get into contact with existing members relatively quickly and establish a central role for themselves. The authors noted that, in contrast to ‘real-life’ (i.e. physical) networks, central persons are not that important in the virtual world, where it seems to be easier to develop new contacts.

Conversely, the phishing case studied by [Leukfeldt \(2014\)](#) showed that social relationships may still be important for the recruitment and growth of cybercriminal networks. Despite criminals being involved in phishing, most recruitment of new criminals was found to take place on the streets. All kinds of acquaintances from the traditional Amsterdam criminal environment were used to carry out the non-digital parts of the crime, such as cashing money, recruiting money mules and obtaining information about potential victims, while meetings with enablers took place in cafes. These case studies found differences in the ties within cybercriminal networks. The questions that

¹This section is partly based on [Leukfeldt \(2015\)](#).

need to be answered include the importance of central nodes within cybercriminal networks and the role of social relationships in the origin and growth of such networks.

Digital offender convergence settings

Social relationships play an important role in the development of criminal networks. Existing contacts, however, do not always provide enough opportunities, especially in transnational crime. The problem with social relationships is that these are highly clustered (Kleemans 2007: 178–80) and may be restricted to people in the same region. The capabilities of any social cluster are limited; eventually, in order to grow and to create more criminal opportunities, contacts must be developed beyond existing social relations and, therefore, with ‘outsiders’.

Places where criminals meet play an important role in the establishing of new contacts. These meeting places, referred to as ‘offender convergence settings’, are physical locations where criminals can meet, such as a cafe or bar. According to Felson (2003), these settings are important because they provide structure and continuity by enabling newcomers to establish links with criminals present in these settings and to become part of existing criminal networks or form new criminal alliances (Felson 2003; 2006; Von Lampe 2009).

The Internet has created specific offender convergence settings in the shape of forums where hackers and carders can meet, exchange information and make plans for committing crimes (Peretti 2008; Holt and Lampke 2009; Lu *et al.* 2010; Decary-Hetu and Dupont 2012; Soudijn and Monsma 2012; Soudijn and Zegers 2012; Yip *et al.* 2012). These studies found that forums play an important role in enabling international attacks as key actors use them to provide their specific expertise and their own social networks, including criminals with whom they have previously co-operated. The study by Soudijn and Zegers (2012), for example, showed how criminals from Eastern Europe used a forum to find the co-offenders they needed to successfully execute malware attacks on bank customers in Western Europe. The activities performed by members of this forum included spamming services to enable contact with suitable targets, as well as money laundering services for transferring and laundering money stolen from victims in Western Europe.

Forums consequently ensure that new criminal contacts can be acquired, new social capital enters the criminal group and natural restrictions on social networks can be mitigated. Empirical research into traditional organized crime shows that access to these meeting places affects the growth and development of a network. In their analysis of 68 ‘executives’ involved in organized crime, Kleemans and De Poot (2008) showed that some members of this group remained ‘local heroes’, whereas others gained positions at national or even international levels. ‘Local heroes’ make profits from many different criminal activities within their own region but have no contacts outside that region and no expertise on which others depend. They are therefore unable to grow to an international level or to forge contacts with brokers who provide access to new export markets, or who have capital or expertise.

Literature on cybercriminal networks shows that forums can serve as digital offender convergence settings for cybercriminals; indeed they played an important role in most of the cases studied (Peretti 2008; Holt and Lampke 2009; Soudijn and Monsma 2012; Soudijn and Zegers 2012). Forums enable criminals from different countries and with

different expertise to meet. This does not mean, however, that all cybercriminal networks use such forums, and it is also unclear as to whether criminals on these forums also meet each other offline. Leukfeldt (2014) found, for example, that a Dutch group of phishers got to know each other in the streets of Amsterdam and used the Internet only to commit their fraud, not to meet each other or recruit new members. As stated in the introduction to this article, an interesting question is whether online and offline offender convergence settings play a role in cybercriminal networks and, if so, which role? If not all criminal networks use forums, there is likely to be a difference between cybercriminal networks based on local networks and cybercriminal networks based on international partnerships, just like in traditional organized crime networks. The question to be asked, therefore, is whether cybercriminals meet only online, how their collaboration develops (for example, an initial online encounter, followed by offline collaboration) and what this means for the growth in and criminal opportunities available to cybercriminal networks.

Data and Methods

Eighteen Dutch police files were systematically analysed in order to gain insight into the direct ties, the origin and growth of criminal networks and their use of forums. These police files provided unique knowledge about cybercriminal networks and their members because of the wide-ranging use of investigative methods such as wiretaps and IP taps, observation, undercover policing and house searches.

Police investigations are not publicly available. The Public Prosecution Service first has to give permission for a police investigation to be scientifically analysed, while the research proposal also has to be assessed by the Dutch Ministry of Security and Justice's Research and Documentation Centre (WODC). WODC gives advice on the quality (specifically the scientific quality) of the research proposal and the research topic (including a view on the value it adds to current research projects).

The police investigations had to be analysed in buildings of the police department or the Public Prosecution Service. The researcher was then allowed to read the files of the police investigation and make notes on his own laptop. Any information recorded had to be anonymized. This meant that names of offenders were coded (e.g. CM1 for a core member, or MM1 for a money mule), while no information on, for example, addresses or social security numbers could be recorded. The anonymized information taken from the police investigations was stored on an encrypted hard drive on the researcher's laptop.

Case selection

It was decided for the purposes of this research to use investigations into criminal networks that the police had already completed.² By 'completed' we mean that the investigation team had collected enough evidence for the Public Prosecution Service to decide to prosecute, although a court judgement may not necessarily have yet been issued. Waiting for a court judgement would have meant that only a few cases would

²By a 'network' we mean two or more cooperating persons performing criminal activities during an extended period of time.

have been available for analysis as it can take years for suspects to be finally convicted (after appeal) (for a more extensive review of these methodological questions, see [Kleemans 2014](#)).

There is no central registration system in the Netherlands that allows for a quick overview of all criminal investigations into phishing and malware networks. The selection of cases was, therefore, carried out using the snowball method, with the starting points being cybercrime and fraud teams on a national, regional or interregional level. Based on existing contacts within the Dutch police, the Police Academy and the Public Prosecution Service, the researcher asked team leaders and senior investigators in these teams whether they knew of any investigations into networks that used phishing or malware to attack users of online banking. An online database of court documents was examined, while a media analysis was also conducted in order to find news reports about relevant cases. This resulted in ten criminal investigations being identified. During the file study, people involved in the criminal investigation were asked whether they knew of any other phishing or malware cases. This resulted in a further eight cases, thus producing information on a total of 18 criminal investigations into relevant networks. These investigations had lasted for between six months and three years and were all carried out between 2004 and 2014.

The 18 investigations into criminal networks involved phishing attacks (ten cases), malware attacks (five cases) and criminal service providers involved in both phishing and malware attacks (three cases). The latter three networks each carried out a specific part of the criminal process, such as recruiting money mules or money laundering. The police investigations did not always cover an entire network. As in all investigations, limited capacity and budgets meant that the police had to decide to focus on specific parts of the network.

Analytical framework

The criminal investigation files contained records of interrogations and information obtained by means of special investigative powers. These records included transcripts of wiretaps, Internet traffic and other surveillance reports. The file analysis involved using an analytical framework to systematically gather the relevant information. Although the framework was developed on the basis of the literature, it was highly dependent on the analytical framework used in the Dutch Organised Crime Monitor, a long-running programme researching the nature of organized crime in the Netherlands (see, for example, [Kruisbergen et al. 2012](#); [Kleemans 2014](#)). The framework includes topics such as the composition and structure of criminal networks, the origin and growth of networks and the use of offender convergence settings (see [Appendix 1](#)).

Interviews

The analyses of the criminal investigation were complemented by interviews with the Public Prosecution Service, police team leaders and senior detectives (including financial and digital experts). The analytical framework used was the same as for the files. It was decided to conduct interviews because the information in the police files focused on providing evidence of criminal activities, which meant that other

information relevant to a scientific analysis may not necessarily have been included. Ties between members, for example, were not always described in detail in the files, although the actors on the law enforcement side may have had a clear picture of these ties. In addition to providing basic information on the number of suspects and the amounts of money involved, these interviews also revealed data on relationships within the network, binding mechanisms and opportunity structures that were otherwise less visible.

Empirical Results

Our study aimed to find out whether cybercriminal groups emerge and grow through social opportunity structures or whether the use of digital criminal offender convergence settings means these social ties are no longer needed. We therefore investigated the origin and growth of each network separately.

Various roles can be distinguished within these networks: core members, enablers and money mules. The core members were those members of the network who initiated and coordinated attacks on online banking and directed other members of the network. Without the core members, the criminal activity in the studied investigations could not have been committed. To gain more insight into the origin of networks, which is central to Section ‘Origin of networks’, we therefore needed to find out more about these core members.

The growth of networks is discussed in Section ‘Growth of networks and recruitment’, not only in relation to the core members but also in relation to the recruitment of group members with other roles. In addition to the core members, the criminal networks in our analysis included enablers and money mules. Enablers provide the core members with the (illegal) services that are necessary in order to enable the criminal activities to be performed, whereas money mules are employed by core members or enablers to disguise the financial trail.³

Origin of networks

Criminal investigations do not always provide a clear picture of how cybercriminal networks have emerged. The supplementary interviews with police officers and prosecutors also provided little insight into the origins of these networks. One explanation for this is that a police investigation aims specifically to find out *who* has performed certain criminal activities. The criminal investigations analysed focused on fraud, money laundering, hacking and/or participation in a criminal organization, and in none of these crimes was it crucial to demonstrate *how* the network had been formed.

³ In cybercrime literature, the term ‘money mule’ is often used to describe these offenders (see Choo 2008; Aston *et al.* 2009; McCombie 2011; Soudijn and Zegers 2012; Leukfeldt 2014). In our opinion, ‘money mule’ is not entirely the right term as these offenders are not used to physically move money from one place to another but instead solely to disguise the financial trail from bank accounts of victims to the core members. Offender ‘A’, for example, gives core member ‘X’ control over his bank account in exchange for money. After a successful phishing or malware attack, money from the victim’s account is transferred to the account of offender ‘A’. The money from that account is cashed as soon as possible. The stack of cash is then delivered to the core members by cashier ‘B’. In literature (and police practice), offender ‘A’ is often referred to as the money mule and, as the term is so widely used, we have also chosen to use it in this article.

Although no direct insight was gained into how the criminal networks in this study had emerged, several observations can be made about their early days. In many of the networks analysed, core members appeared to have been active in the criminal environment for some time and knew each other from the neighbourhood they grew up in or lived in or from previous criminal activities. The core members of nine of the eighteen networks, for example, had been active in the criminal underworld in some major Dutch cities and carried out all sorts of criminal activities within their own regions (networks 1, 2, 3, 4, 8, 9, 11, 14 and 16). Network 9, for example, was a criminal youth gang whose members, in addition to all kinds of traditional crimes such as street robberies and shoplifting, were involved in recruiting money mules and cashing money stolen from online bank accounts. Network 10 was an offshoot of a phishing network that previously operated from Amsterdam, with one of the three core members of this network having started out as a money mule in an Amsterdam network and later being active as a recruiter for other phishing networks. He, his wife and a friend (the core members of network 10) attacked online bank customers across the Netherlands.

Forums also played a role in the origin of three networks. Network 11, for instance, emerged because the Dutch core member was looking on the Internet for ways to commit fraud. Through various forums he discovered opportunities to do so. An earlier police investigation showed that this core member had previously purchased credit card information on the Internet and produced fake credit cards, while Internet taps showed that he was constantly looking for new ways to make easy money. Through various forums he learned how to carry out phishing and malware attacks and found suitable accomplices in other countries, including the people from Germany and Turkey with whom he worked during the attacks that were central to the police investigation analysed.

Forums also played a central role in networks 6 and 7. The core members of network 6 searched on forums for people to provide specific, illegal services that the members could use in attacks on banks all over Europe. We do not know whether the core members met through a forum, but it is certainly clear that at least one of them offered his services on forums before the attacks described in our police file were carried out. It is also clear that the network would not have been able to execute these attacks without the forums that were used to recruit other criminals ('enablers') with the specific knowledge needed for this purpose (see also the next section). In the case of network 7, members met, formed new alliances and exchanged information through a criminal forum.

Networks can be divided into those formed through physical contacts and those formed through digital contacts. Most of the networks in our analysis arose because core members knew each other from the criminal underworld and were already involved in all kinds of criminal activities in the physical world. This is remarkable, given that the networks were selected to be part of our analysis specifically because they had committed cybercrimes. The core members were simply looking for ways to make easy money and seemed to consider using phishing or malware to steal money from online bank accounts as just one of those ways. With three exceptions, it remains unclear as to what exactly caused the core members to switch from criminal activities in the physical world to phishing or malware attacks. These three exceptions originated because core members went searching for suitable co-offenders on forums. Although these networks were also looking for ways to make easy money, they focused specifically on opportunities created by the Internet, where the core members obtained information on criminal capabilities and searched for suitable co-offenders.

Growth of networks and recruitment

As all the analysed networks showed, the growth of networks relates mainly to the recruitment of enablers and money mules. Enablers can be divided into professional enablers and recruited enablers. Both types provide services to the core members, with the difference being that professional enablers offer their services to all kinds of networks, whereas recruited enablers are invited by core members to provide specific services. These latter enablers are people, such as bank call centre or phone shop employees or postal workers, whose work or contacts mean they have access to relevant information. They often receive a small fee for their services and are used by one specific network only.

Similar to the differences in the origins of networks, networks can also grow in a range of different ways: some grow predominantly along traditional lines (through social contacts), whereas others grow through the use of forums. However, these two extremes on the continuum mask some of the more subtle ways in which other suitable co-offenders may be recruited.

Figure 1 identifies four models of growth; the recruitment process is divided into two main categories (recruitment primarily through social opportunity structures, and recruitment primarily through forums), and each of these 'extreme' categories has two overlapping subcategories.

The first main category is the traditional growth model of social contacts, with the two subcategories of (1) growth based only on social contacts, and (2) growth based on social contacts as a base and with forums being used to obtain specific knowledge or tools. Most networks in our analysis grew based on social contacts only, with suitable co-offenders being recruited in this way in 13 of the networks, (1–5, 8–10, 12, 14 and 16–18). Recruitment also took place through social contacts in two other networks (13 and 15), but the core members of these latter networks used forums to search for criminals offering specialist services, such as specific malware.

The second main category comprises networks that grew through the use of forums. Within this category, a distinction can be made between (1) growth solely based on forums and (2) growth using forums as a base and with social contacts then being used for local embedding. In network 11, for example, the core members from the different countries got together through a forum, where they also bought malware, but relied on social contacts to recruit enablers and money mules in the countries they attacked. Networks 6 and 7 grew entirely through forums; the core members of network 6 recruited all kinds of criminals able to supply specific services through a forum, while network 7 involved a forum where criminals met to buy and sell services and tools, and to exchange knowledge on attack methods.

FIG. 1. Four models of growth.

Growth entirely through social contacts

Thirteen of the investigated networks grew entirely through social contacts. Most (nine) of these networks performed phishing attacks, whereas three of them provided services to both phishing and malware groups, and one network carried out malware attacks. The recruitment of professional and recruited enablers and money mules is described below.

Professional enablers

The investigations into networks that grew through social contacts usually revealed little about the recruitment of professional enablers. Although most of the networks used these enablers (in order, for example, to obtain false identity papers), these individuals did not come under scrutiny during the criminal investigation. The investigation into network 1, however, provided some insight into how an enabler providing ICT services was recruited.

Network 1 performed low-tech attacks, in which victims received an e-mail stating that the security of the bank where they had an online account needed to be updated. The e-mail told victims to click on a link in the e-mail to log in to the bank's new 'secure' website and start the security update. Although victims thought they were logging in to the trusted site of the bank, in reality they were entering their login data on a phishing website controlled by the criminal group. This gave the criminals control over the victim's bank account. Before, however, any money could be transferred, transaction authentication codes were needed. The victim therefore got a phone call from a member of the criminal network, who pretended to be an employee of the bank. The caller referred in this conversation to the recent security update and was able, if necessary, to provide information about the victim's account that only the bank would know (such as the type of account and details of the most recent transactions), but which was also known by the criminals because by then they had control over the account. The caller told the victim that all that was needed to complete the security update was a security code. Once the victim generated this code and gave it to the caller, sums of money were transferred from the victim's account to the money mule's account.

Although network 1 did not use malware or other high-tech methods to gain control over online bank accounts, its core members depended on phishing websites that looked exactly the same as the website of the bank where the victims had an account. Tapped telephone conversations showed that the core members themselves did not have the skills to create such a website. Therefore, a core member called a friend in Nigeria. This friend introduced another friend who was able to produce the phishing websites required.

Recruited enablers

The networks in our analysis that grew solely through social contacts made more frequent use of recruited enablers than that of professional enablers. These recruited enablers were always from within the core members' social network (see, for example, Box 1). Core members recruited new enablers from among their family or acquaintances, at sports clubs or schools and on the streets. Interviews and intercepted conversations showed that recruited enablers, such as cashiers, bank employees, postal workers and callers deployed by a network, also actively looked for new people to offer the same kind of services.

As the core members recruited through their social networks, the numbers and types of enablers that they could use were limited. Enablers recruited in these situations were often found, therefore, to be used for multiple activities. Network 1, for example, used bank employees not only to provide information about interesting bank accounts but also to increase transfer and cashing limits or to carry out address changes so that official mail from the bank could be diverted to the core members. Networks 1, 10 and 13 also used postal employees to capture post containing login information for new online bank accounts or to intercept other interesting packages, such as electronics or clothes. It is important to note that these bank employees and postal workers were not necessarily linked to the criminal groups' crime script. The attacks could also be executed without these enablers as demonstrated by the fact that other networks using the same crime script were able to carry out their attacks without them. It would seem that the networks that used such recruited enablers did so mainly because they were easily accessible for the core members and could be used to facilitate the attack.

Box 1. Recruitment of Bank Employee

A bank employee said 'About a year ago I had a conversation with an old friend, Roy. I ran into him in the street. We talked about various things, including work. I told them I worked at [Bank 1]. Ten days later I met Roy again and he said that his ex was trolling him and that he didn't have access to his money. He asked if I could check his account balance for him, which I did. Two weeks later, a car with people in it who said they were friends of Roy stopped in front of my door. I was also asked to sort out two bank accounts for them. I didn't want to do this, but the men scared me. They gave me a note with two account numbers on it and said they wanted information about the balance, the account holder's initials and the type of account'.

Money mules

Social contacts also played a role in the recruitment of money mules by the networks analysed. Just like recruited enablers, money mules were approached in schools, at sports or night clubs or just on the street by core members, enablers or money mules, who were already being used by the criminal network. The contacts between a main recruiter, local recruiters and money mules⁴ can be seen in network 2, which was engaged in phishing attacks. The core members operated from a major city in the west of the Netherlands, while the cashers and money mules were located in a northern province. The main recruiter (in other words, the link between the core members and the local recruiters, cashers and money mules) said that he came into contact with the people in the north 'through the music scene'. A northern recruiter stated that:

Sometime last year I went with my friend to a party in [city in the west]. In the cafe I met a guy [the main recruiter] and had a conversation with him. At one point I asked him how I could make money. The man replied that it was easy. I had already told him I lived in [place in the north] and that I made money dealing drugs. The man said he could make us rich, really rich, and in an easy way. He said

⁴The examples in this section are from one investigation into the recruitment of money mules in one region in the Netherlands. However, other investigations in other regions in the Netherlands confirm this picture.

he put money on debit cards and cashed the money right away. The owner of the card then received a certain percentage.

In network 2, potential money mules were told they would earn a certain amount of money and that they would never be caught. The main recruiter (from the west of the country) in particular and also the local recruiters, who associated a lot with the main recruiter, were greatly respected by the local youth. They drove expensive cars, wore designer clothes and spent a lot of money when going out. Young people envied the lifestyle of these offenders or also liked the idea of making easy money. They were often approached on the street, at hangouts, or when going out or at school. If someone agreed, contacts were maintained through the message function on mobile phones. Suitable money mules were also contacted by phone or on the Internet. Youngsters got messages from friends or vague acquaintances asking for bank cards ('Who wants to make easy money?'). The actual encounter between the money mules and recruiters was always at a physical location, and this principle was also seen in other networks.

Growth based on social contacts; forums for recruiting specialists

Although two of the networks analysed (networks 13 and 15) grew mainly through social contacts, they used forums to recruit specialists. In network 13, one core member controlled all the others (enablers and money mules) in the network. This network carried out both phishing and malware attacks. The core member had the technical knowledge required to develop phishing sites, including databases to store data. He frequently visited hackers' forums and websites on which stolen credit card information was sold. On one of these forums, he bought e-mail addresses to send his phishing mails to and also bought malware. During one of the interrogations he said that he programmed computers as a hobby and that he learned to do this by searching for examples on the Internet.

Network 15 grew mainly through social contacts but also used forums to purchase specific illegal services. This network carried out malware attacks in the Netherlands. All the core members appeared to know each other before this particular network started. The majority of the enablers and all the money mules were recruited through social contacts. According to the police file, core members 1 and 3 knew each other from a company where they had both worked. Core members 1 and 2 knew each other from the financial world. Core member 2 had a construction company and was hired from time to time by core member 1 to do work. Core members 1, 2 and 3 later also worked together for another company. In addition to business contacts, these criminals appear to have got together privately as photos found by detectives showed these members in various joint activities, including a dinner at someone's home and on a boat. Some of the core members also went on holiday abroad together.

Professional enablers

The core member of network 13 used professional enablers found on forums. His IP address was tapped for about a month, during which time he logged on to forums on a daily basis and posted several requests on one forum, including a request for information on how to send bulk e-mails. He also posted a request asking for a programmer able to develop a specific piece of software for use on a homemade phishing site. This core member used other forums to look for key loggers. The Internet tap also showed

that he downloaded malware from the forum and then used a search engine to find out what this type of malware could do. An unknown user on a forum asked the core member if he wanted to work on a new 'project' with a botnet. It is unclear whether this project was actually executed. The core member held Skype calls on cybercrimes with various individuals who were not part of network 13, as well as giving someone instructions on the best way to spam people. Different methods were then tried out. The core member also used the forum to distribute hacking tools, some of which he used in phishing attacks on a Dutch bank. One of the other members of the forum sent the core member a private message indicating that he was interested in a new 'project' involving a pop-up window. It is unclear whether they actually worked together.

The core members of network 15 also used forums. One of the core members of this network was responsible for managing and operating the specific malware used by this group, as well as for ensuring that the other core members could communicate with each other in an encrypted way and that all data stored were encrypted. An Internet tap revealed that he also bought other malware and found other service providers on a forum, including someone able to test whether malware was detected by virus scanners and a bitcoin mix service that concealed bitcoins' origins.

Recruited enablers

The core member of network 13 used a recruiter/casher to find money mules and to steal money from victims' bank accounts. In other crimes this core member committed, such as using fake credit cards to purchase goods, he used postal workers. According to the police respondents, he knew all these enablers because they came from the same ethnic group and all lived in a particular neighbourhood in Amsterdam.

A number of core members of network 15 were engaged in recruiting money mules and cashing money from money mules' accounts. However, they also used someone in a northern province to recruit new money mules and cash money. This recruiter helped money mules to register businesses and open corporate bank accounts. A similar construction was also used by this network in the United Kingdom, where one enabler was responsible for this process. It is unclear how the core members of this network got to know these enablers.

Money mules

The money mules in network 15 were recruited through social contacts. Interrogations of the money mules deployed by this network found that they were generally people who were in debt and were told that they could make easy money by allowing their bank accounts to be used or by registering a business in their name.

Growth based on forums, with social contacts used to recruit local criminals

Network 11 appears to have come into existence after its core members met each other on the Internet. The Dutch core member stated in one of his interrogations that he had been looking for opportunities to commit fraud on the Internet. This was also evident from intercepted conversations with the German core member and a core member in Turkey, with whom the Dutch core member had contact on the Internet. These three core members discussed future attacks in several countries; this included sharing ideas and discussing new ways to make money through Internet fraud. The Dutch core

member also had contacts on all kinds of forums with people outside network 11 on how payment systems could be attacked and credit cards misused. The core members made full use of the opportunities for meeting other criminals on forums. The fact that they used the Internet to make new contacts does not mean, however, that they had high levels of technical skills as intercepted conversations showed, for example, that the offenders did not exactly understand how the Trojan they used worked (they had to use a search engine to find out about this). They were consequently dependent on other people, with technical expertise, to adapt the Trojans to new software updates.

Professional enablers

The core members of network 11 purchased various Trojans, login details of Dutch bank customers and credit card data on forums, where they placed calls for certain services or responded to services offered and then negotiated on the forum with those offering these services. The Dutch core member also had phone contact with a professional enabler who provided a caller. The latter could be used to steal the codes required for transferring amounts from online bank accounts to accounts held by money mules. How this contact was established is unclear. What was evident from discussions between the core member and the enabler was that the latter had been increasingly involved in phishing attacks and gave the core member tips on how best to use the caller.

Recruited enablers

The core member of network 11 needed a 'SIM swap' to perform a specific attack variant, whereby criminals used phishing mails and phishing websites to steal credentials from users. This involved adding an additional entry field in which the victim had to enter his phone number during the login process. The one-time transaction authentication code (which is required to transfer money) was sent to this phone number. A new SIM card was then requested by the criminals on the victim's behalf. From then on, the transaction authentication codes were sent to a phone owned by the criminals. In order to carry out this type of attack, the Dutch core member approached someone who had previously worked for the core member as a money mule and who had a friend who worked at a telecom company. They approached this man and the core member asked him what kind of changes he could make in the system. Although this friend seems not to have had enough rights in the system to do this, he knew someone else (V4, a trainee store manager) who was able to make the necessary changes and so had access to all the store's systems. The core member asked V4 whether he could make some SIM swaps for him. V4 said he wanted to think about it first. A few days later the core member called V4 and said he would pay him €500 for the SIM swaps. V4 agreed and so the core member passed certain information, such as names and phone numbers, to him. They then agreed to meet in the city centre to exchange the money and new SIM cards.

Money mules

The core members of network 11 were active in the Netherlands, Germany and Turkey and relied on local people to execute attacks in the Netherlands. The recruited enablers and money mules active in the Netherlands were all directly linked to the Dutch core member. The latter knew some of the co-offenders because they had been to school together or had been friends for a long time. All these offenders were already active in

the criminal underworld, but it was the core member's knowledge that enabled them to carry out the specific parts of the fraud process in this case.

Growth entirely through forums

Core members

Networks 6 and 7 grew entirely through forums. The core members of network 6 came from an Eastern European country and attacked bank customers in several other European countries. They used a forum to recruit criminals with the expertise needed to perform the attacks in all these countries. This expertise included the ability to create phishing sites, to translate texts and to launder money. Network 7 was based around a criminal forum where all kinds of people interested in phishing and malware attacks came together.

Enablers

The core members of network 6 used a forum to search for individuals able to perform specific illegal services. One of these individuals was an enabler who was used to coordinate the cashing of money in Russia and elsewhere in Europe. This enabler offered his specialized financial services (including providing money mules, but also exchanging electronic currencies into cash) on various forums and websites. After deducting his commission, he returned the money to his clients in the form of cash deposits, virtual currencies or bank cards. The core members also bought translation services on the forum so that texts for recruiting new money mules could be translated into Dutch, English and Russian. Finally, a core member used the forum to contact an unknown person who offered paid spamming services for recruiting money mules and who was able to reach millions of e-mail addresses.

Network 7 grew entirely through a forum where criminals got together to trade identity information and services designed to intercept this information. This forum comprised sections offering services and sections containing information on all sorts of criminal technologies; in essence, therefore, a combination of a marketplace and a 'Wikipedia for cybercriminals', with many different forms of cybercrime being discussed and wide-ranging services being offered. A potential new member could be accepted only if vouched for by two existing members. This meant that the potential member already had to know other members of the forum. To be admitted as a service provider, a person had to be vouched for by three members. New services were tested by the forum administrators, who wrote reviews on them. In total, 1,855 members (both active and inactive) were affiliated to the forum.

Money mules

The Dutch money mules used by network 7 were recruited via e-mails sent out in large numbers. The e-mail message stated that new employees were being sought for an international company that had recently started operations in the Netherlands. The new employee's task was to provide a bank account in the Netherlands to which money from customers could be paid. This money then had to be transferred by the employee to the account of the company, which was abroad. The employee was allowed to keep five per cent of the transferred money, with the e-mail promising a guaranteed minimum monthly salary of \$2,000.

To gain more insight into the recruitment process, a Dutch police officer signed up as a new employee on the website mentioned in the e-mail. The next e-mail included a contract that had to be signed and returned to the company. This e-mail also repeated the percentage that the employee was allowed to keep and that the money the employee received on his bank account had to be transferred to the company via a specific bank. After the contract had been signed, the new employee received a further e-mail asking for information about his bank account, account type (business or private), the limit for transfers, and the SWIFT and IBAN numbers. After this information had been sent to the company, another e-mail was sent; this stated that €9,447 had been transferred to the employee's account. The employee was allowed to keep €473 of this amount and had to transfer the rest to the company via a specific bank.

Discussion and Conclusion

The aim of our study was to investigate whether cybercriminal groups emerged and grew through social opportunity structures or whether the use of forums meant that these social ties were no longer needed. To gain insight into these issues, we analysed 18 criminal investigations into networks that had carried out attacks on online banking, with the aim of gaining insight into the origin and growth processes of these networks.

Although our analysis of these criminal investigations provides unique insight into the origin and growth of cybercriminal networks, it also has some limitations (see, for example, Kleemans 2014). As it was based on criminal investigations and interviews with people involved in carrying out such investigations, we gained knowledge only about the criminal networks known to the police. Hence, no knowledge was gained about those networks that had so far been able to remain undetected. It may also be queried whether the findings of our analyses could be an artefact of the police investigations (because the police may have preferred to investigate cases involving more traditional criminals rather than international online forums). Follow-up research into these networks is consequently needed to complete the picture. This could be done by involving commercial security companies, for example, in future scientific studies.

Another limitation is that the study was conducted solely in the Netherlands. The same study in a different country could paint a different picture owing to differences in policing priorities and knowledge of or expertise in cybercrime. Our study shows that criminal investigations can be used to gain insight into the origin and growth of networks, and the methods and analytical framework we used can also be used in other countries.

Finally, all the criminal investigations analysed involved phishing and malware attacks on online banking. We consequently do not know whether criminal networks engaged in other forms of cybercrime, such as those using ransomware or distributed denial of service attacks to extort businesses, show different patterns of origin and growth. Future research should therefore focus also on criminal networks committing other types of cybercrime.

Our analyses show that the role of social ties in the origin and growth of cybercriminal networks is certainly still important, with social ties appearing to play a salient role in the majority of the networks. Many of the networks in our analysis emerged and grew because core members knew each other from the traditional (offline) criminal underworld. Enablers and money mules were also often recruited through existing social networks. That does not mean, however, that forums play only a marginal role. Indeed,

they were found to play a significant role in a number of networks by, for example, enabling individuals to find suitable co-offenders in other countries. Forums also provide a marketplace to buy and sell criminal tools or services and can be used to gain knowledge about criminal opportunities. Various networks that grew through social contacts used forums to obtain specific knowledge or to buy tools, thus allowing core members with access to forums to increase the criminal capabilities of their network relatively quickly.

Both social ties and forums were used by the analysed networks to recruit new members. Four types of growth were identified: (1) growth entirely through social contacts, (2) social contacts as a base and forums to recruit specialists, (3) forums as a base and social contacts to recruit local criminals and (4) growth entirely through forums. In thirteen of the eighteen networks, criminals recruited only through social ties, whereas recruitment in two of the other networks was mainly through social contacts, with forums being used to find specialized enablers. In one network, the core members first got together on a forum but then used their social networks to recruit local enablers and money mules. The remaining two networks did all their recruitment through forums, where core members looked for suitable co-offenders and enablers with specific knowledge within their own offline social network.

Phishing and malware attacks were carried out by various types of networks. Remarkably, however, large numbers of these attacks were attributable to criminals without exceptional technical knowledge. The core members of these networks had long criminal careers in the offline world and a track record of all kinds of financial and economic crimes and were looking to make easy money rather than specifically deciding to commit cybercrimes. Our analysis showed that only one person with technical expertise (who may be either a core member or an enabler) was needed to carry out these cyberattacks.

Although the majority of networks still recruited suitable co-offenders through social contacts and forums did not play an important role in all the cybercriminal networks analysed, forums represent a new way for networks to become established and to grow beyond the traditional range of social contacts. Some networks made full use of these new opportunities (for example, to establish new alliances), while others used forums only to come into contact with criminals with specialist knowledge. As there is already an extensive body of knowledge concerning the growth of criminal networks through social contacts, it is important now to gain more insight into the role specifically played by forums in the origin and growth of cybercriminal networks.

Forums would seem to make it easier for loners or small groups to find suitable co-offenders and, potentially, to allow such networks to grow quickly. There is always somebody available on these forums who can carry out the specific parts of the criminal process for which the core members do not have the knowledge or capabilities.

Forums are also used to acquire knowledge and skills. In the digital era, forums are replacing prisons as the 'university for cybercriminals'. Loners experimenting out of curiosity with all sorts of legal or illegal technical tools can end up in criminal networks through forums. More insight is therefore needed into what prompts individual criminals to become active on forums.

It will also be useful to examine what exactly happens on forums. This analysis will go beyond the analyses of social networks that have been carried out in the past. Knowledge about the type of criminals that communicate with each other on forums

and the number of attacks originating from forums will provide more insight into the importance of forums for criminal networks. Are they mainly used, for example, by curious individuals? Or are they populated by petty thieves buying a few credit cards and experimenting with key loggers? Or, alternatively, are we dealing with professional networks that systematically attack organizations?

Funding

This work was supported by the Dutch banking sector, represented by the Dutch Banking Association (NVB), the Police Academy and the Cybercrime Program of the Dutch police.

Appendix 1: Analytical Framework

Direct ties

Describe the composition of the network: how are the suspects related, their role and/or function within the network (subgroups, core functions, facilitators, periphery).
Describe the structure of the criminal network (standalone unit, fluid cooperation based on a specific goal).
Is there a hierarchy and/or mutual dependency?

Origin and growth

How, when and where did the network start?
Do the suspects have a common background? (family, neighbourhood, friends, occupation etc.). If not, in what way are the suspects related?
What kept the members of the criminal network together? (social ties, economic advantages, fear, etc).
Describe the period/duration of the activities.
Describe changes within the composition of the criminal network.
How are new members being recruited?

Offender convergence settings

Describe the (digital) offender convergence setting used by the criminals.

REFERENCES

- ASTON, M., MCCOMBIE, S., REARDON, B. and WATTERS, P. (2009), 'A Preliminary Profiling of Internet Money Mules: An Australian Perspective', *Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, IEEE Computer Society: 482–7.
- BOUCHARD, M. and MORSELLI, C. (2014), 'Opportunistic Structures of Organized Crime', in L. Paoli, ed., *The Oxford Handbook of Organized Crime*, 288–302. Oxford University Press.
- CHOO, K. K. R. (2008), 'Organised Crime Groups in Cyberspace: A Typology', *Trends in Organised Crime*, 11: 270–95.
- DÉCARY-HETÚ, D. and DUPONT, B. (2012), 'The Social Network of Hackers', *Global Crime*, 13: 160–75.
- EDWARDS, A. and LEVI, M. (2008), 'Researching the Organization of Serious Crimes', *Criminology and Criminal Justice*, 8: 363–88.
- FELSON, M. (2003), 'The Process of Co-offending', in M. J. Smith and D.B. Cornish, eds, *Theory for Practice in Situational Crime Prevention*, Vol. 16, 149–68. Willan Publishing.
- . (2006), *The Ecosystem for Organized Crime*. HEUNI paper nr 26. HEUNI.
- HOLT, J. T. and LAMPKE, E. (2009), 'Exploring Stolen Data Markets Online: Products and Market Forces', *Criminal Justice Studies*, 23: 33–50.

- HOLT, T. J. and BOSSLER, A. M. (2014), 'An Assessment of the Current State of Cybercrime Scholarship', *Deviant Behavior*, 35: 20–40.
- IANNI, F. A. J. and REUSS-IANNI, E. (1972), *A Family Business*. Russel Sage.
- KLEEMANS, E. R. (2007), 'Organized Crime, Transit Crime, and Racketeering', *Crime and Justice. A Review of Research*, 35: 163–215.
- . (2014), 'Organized Crime Research: Challenging Assumptions and Informing Policy', in J. Knutsson and E. Cockbain, eds, *Applied Police Research: Challenges and Opportunities. Crime Science Series*. Willan.
- KLEEMANS, E. R. and DE POOT, C. J. (2008), 'Criminal Careers in Organized Crime and Social Opportunity Structure', *European Journal of Criminology*, 5: 69–98.
- KLEEMANS, E. R. and VAN DE BUNT, H. G. (1999), 'The Social Embeddedness of Organized Crime', *Transnational Organized Crime*, 5: 19–36.
- KRUISBERGEN, E. W., VAN DE BUNT, H. G. and KLEEMANS, E. R. (2012), 'Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit', *Fourth Report on Organized Crime in the Netherlands*. Boom Lemma.
- LASTDRAGER, E. E. H. (2014), 'Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature', *Crime Science*, 3: 1–6.
- LEUKFELDT, E. R. (2014), 'Cybercrime and Social Ties. Phishing in Amsterdam', *Trends in Organized Crime*, 17: 231–49.
- . (2015) Organised Cybercrime and Social Opportunity Structures. A Proposal for Future Research Directions. *European Review of Organised Crime*, 2: 91–103.
- LU, Y., LUO, X., POLGAR, M. and CAO, Y. (2010), 'Social Network Analysis of a Criminal Hacker Community', *Journal of Computer Information Systems*, 51: 31–41.
- MCCOMBIE, S. J. (2011), 'Phishing the Long Line. Transnational Cybercrime from Eastern Europe to Australia', PhD thesis, Macquarie University, Department of Computing.
- MCGLOIN, J. M. and KIRK, D. S. (2010), 'An Overview of Social Network Analysis', *Journal of Criminal Justice Education*, 21: 169–81.
- PERETTI, K. K. (2008), 'Data breaches: What the Underground World of "Carding" Reveals', *Santa Clara Computer and High Technology Law Journal*, 25: 345–414.
- SCOTT, J. and CARRINGTON, P. J. (2011), *The SAGE Handbook of Social Network Analysis*. SAGE Publications.
- SOUDIJN, M. R. J. and MONSMA, E. (2012), 'Virtuele ontmoetingsuimtes voor cyber-criminelen' [Virtual Meeting Places for Cyber Criminals], *Tijdschrift voor Criminologie*, 54: 349–60.
- SOUDIJN, M. R. J. and ZEGERS, B. C. H. T. (2012), 'Cybercrime and Virtual Offender Convergence Settings', *Trends in Organized Crime*, 15: 111–29.
- 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: 93–100.
- WALL, D. S. (2007), *Cybercrime. The Transformation of Crime in the Information Age*. Polity Press.
- WILLIAMS, M. L. (2016), 'Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level', *British Journal of Criminology*, 56: 21–48.
- YIP, M., SHADBOLT, N. and WEBBER, C. (2012), 'Structural Analysis of Online Criminal Social Networks', IEEE International Conference on Intelligence and Security Informatics (ISI), 11–14 June 2012.