Crime Law Soc Change (2017) 67:39–53
DOI 10.1007/s10611-016-9663-1

Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis

E. Rutger Leukfeldt[1,2] · Edward R. Kleemans[1,3] · Wouter P. Stol[2]

Published online: 26 November 2016

Abstract Two recent studies which are part of the Dutch Research Program on the Safety and Security of Online Banking, present empirical material regarding the origin, growth and criminal capabilities of cybercriminal networks carrying out attacks on customers of financial institutions. This article extrapolates upon the analysis of Dutch cases and complements the existing picture by providing insight into 22 cybercriminal networks active in Germany, the United Kingdom and the United States. The analysis regarding origin and growth shows that social ties play an important role in the majority of networks. These networks usually originate and grow either by means of social contacts alone or by the combined use of social contacts and forums (to recruit specialists). Equally, however, forums play a vital role within the majority of the networks by offering a place where co-offenders can meet, recruit and trade criminal 'services'. Moreover, those networks where origin and growth is primarily based on forums appear capable of creating more flexible forms of cooperation between key members and enablers, thereby facilitating a limited number of core members to become international players. Analysis of the capabilities of criminal networks shows that all networks are primarily targeted towards customers of financial institutions, but most networks are not restricted to one type of crime. Core members are often involved in other forms of offline and online crime. The majority of networks fall into the high-tech category of networks, mostly international, high-tech networks. These are networks with core members, enablers, and victims originating from different countries.

✉ E. Rutger Leukfeldt
RLeukfeldt@nscr.nl

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

[2] Open University of the Netherlands, Valkenburgerweg 177, 6401 Heerlen, DL, The Netherlands

[3] VU University Amsterdam, De Boelelaan 1105, 1081 Amsterdam, HV, The Netherlands

Keywords Cybercrime · Criminal networks · Social opportunity structures · Offender convergence settings · Phishing · Malware

Introduction

This article focuses on cybercriminal networks, more specifically, the origin, growth and criminal capabilities of these networks. The traditional idea is that origin and growth of criminal networks mainly operate through pre-existing social relationships; work and work-related relationships; hobbies or other activities. Cybercriminals, however, use internet forums as both a meeting place and a market place [1–9]. These forums use elaborate systems to show the 'credibility' of their members. For example, member ranking systems, ratings from earlier jobs, comments from buyers and official tests of products by administrators. Forums, therefore, provide an environment in which criminals are able to learn new tricks, plan attacks, search for co-offenders with specific knowledge or buy criminal tools. Consequently, traditional recruitment processes are changing and such change raises an interesting question: how do these developments affect the origin, growth and criminal capabilities of cybercriminal networks?

Two recent studies which are part of the Dutch Research Program on the Safety and Security of Online Banking present empirical material regarding the origin, growth and criminal capabilities of cybercriminal networks carrying out phishing and malware attacks on online banking systems in the Netherlands [4, 5].[1] Analysis of the Dutch cases shows that while social ties still play an important role in the origin and growth of the majority of networks, internet forums play a significant role in a number of networks e.g. by finding suitable co-offenders or promoting contact with enablers. Significantly, criminals with access to forums can increase criminal capabilities of their network relatively quickly. This also has implications for the criminal capabilities of networks. Different types of networks can be distinguished, ranging from locally rooted networks carrying out low-tech attacks with a high degree of direct offender-victim interaction, to international networks carrying out high-tech attacks without such interaction.

This article builds upon the recent analysis of Dutch cases and complements the existing picture of cybercriminal networks by providing insight into cybercriminal networks active in Germany, the United Kingdom (UK) and the United States (US). First, "Prior empirical research in the Netherlands" section gives a brief overview of the main findings of the analysis of the Dutch cases. "Data and methods" section contains a description of the methods used for this study. "Results" section presents the empirical results regarding origin, growth and criminal capabilities of the German, UK and US networks. Finally, "Conclusion and discussion" section contains the conclusion and discussion, which covers the results of both Dutch and the German, UK and US cases.

[1] 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, [12]). 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.

Prior empirical research in the Netherlands

The current article advances the work of Leukfeldt et al. [4, 5]. These articles give insight into the composition, origin and growth, and criminal capabilities of criminal networks carrying out financial cybercrimes in the Netherlands. The authors analyzed eighteen Dutch police files. These police files provided unique information about cybercriminal networks and their members largely as a result of the wide use of investigative methods such as wiretaps and IP taps, observation, undercover policing, and house searches. The files were systematically investigated using an analytical framework. This section briefly describes the main analyzed results of these 18 Dutch cases.

The structure of networks

Within all networks, there are dependency relationships and different functions. In addition to a comparatively fixed group of core members, the composition of the networks regularly changes. Subgroups of core members execute secondary criminal activities, and individual core members work together with criminals from outside the criminal network to commit a wide range of crimes. Furthermore, new enablers are recruited when crime scripts change in response to new security measures, core members are constantly recruiting new enablers, and there is a constant flow of new money mules.

Four positions can be recognized within all networks: core members, professional enablers, recruited enablers, and money mules. Core members are those members of the network initiating and coordinating attacks on online banking. Without these core members, crime in the analyzed investigations would be impossible, and they perform a directive role for other members of the network. Individuals providing services to the criminal network are in the layer below the core members. These services are necessary to execute the criminal activities. Within this group, a distinction can be made between professional enablers and recruited enablers. The first group offers services to the core members and other criminals on their own initiative (e.g. fake identity documents). The latter group provides much simpler services to the core members, and they are encouraged by the core members to do this (e.g. provide useful intelligence). Finally, money mules are the bottom layer of the networks. As a rule, these people are used by the core members or by enablers to interrupt the financial trail leading back to the core members.

Origin and growth of networks

The role of social ties in the origin and growth of cybercriminal networks certainly remains important. In the majority of networks, social ties appear to play an important role. A large number of networks in the analysis of Dutch cases have emerged and grown because core members know each other from the (offline) criminal underworld. Enablers and money mules are also often recruited through existing social networks. That does not mean, however, that forums play a marginal role. Indeed, forums play a significant role in a number of networks. For example, forums enable individuals to find suitable co-offenders in other countries. Furthermore, they provide a marketplace for buying and selling criminal tools and services and can be used to acquire information about criminal opportunities. Various networks based on social contacts use forums to acquire specific knowledge or to buy tools. Hence, core members with access to forums are able to increase the criminal capabilities of their network relatively quickly compared to core members without access to forums.

Both social ties and forums are used to recruit new members. In this respect, four types of growth may be distinguished: (1) completely 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, (4) completely through forums. In the majority of networks, suitable co-offenders are still recruited through social contacts. Forums do not play an important role in all cybercriminal networks. Forums, however, do enable novel origin and network growth beyond traditional social contact. Some networks fully use these new opportunities, for example, to establish new alliances, while other networks use forums only to come into contact with criminals with specialist knowledge.

Different types of networks are involved in phishing and malware attacks. Remarkably, however, criminals without exceptional technical knowledge are largely responsible for these attacks. The core members of these networks have a long criminal career in the offline world and have manifold financial and economic crimes on their track record. From the evidence it can be deduced that the aim of these criminals is to earn easy money. They did not take a deliberate decision to commit cybercrimes as such. The analyses reveal that only one person with technical expertise is needed to carry out these cyber-attacks (who may be a core member or an enabler).

Criminal capabilities

All networks are engaged in attacks on online banking. Although the scripts of all criminal networks are roughly similar, there are some important differences. The differences between these two types of attacks relate to the extent of ICT use during the attack, as well as the degree to which criminals have direct contact with the victims. The crime scripts can, therefore, be divided into two main categories: low-tech attacks and high-tech attacks. Moreover, each category of attacks can be subdivided by focusing on the degree of interaction between offenders and victims. As a result, 4 attack variants can be identified: low-tech attacks with a high degree of direct interaction between attacker and victim, low-tech attacks with a low degree of direct interaction, high-tech attacks with a low degree of interaction and high-tech attacks without interaction.

To determine how ‘international’ a network is, we looked at the countries from which network members operated and from where victims originated. The low-tech networks are responsible for the majority of attacks on victims in the Netherlands. In 11 cases, the core members operate from the Netherlands and only use enablers and money mules that have been recruited in the Netherlands. The 7 other networks have core members, professional enablers, recruited enablers or money mules operating outside of the Netherlands (or having been recruited outside of the Netherlands). One of these networks performs low-tech attacks.

The criminal activities of the networks are not always limited to phishing or malware attacks. In over half of the cases, it is clear that core members also perform other criminal activities. It seems to be a matter of ad hoc alliances: subgroups of core members working together on specific types of crime. Sometimes core members collaborate with people outside the core group of the analyzed network. Most criminal activities relate to financial crimes, but other activities like human trafficking or drug trafficking can also be distinguished.

Data and methods

This article compares characteristics of cybercriminal networks that were active in the Netherlands with cybercriminal networks in Germany, the UK, and the US. Therefore, this article uses the same analytical framework as used in the original analyses of Dutch cases.

There is a difference between the methods used to gain insight into the cybercriminal networks in the Netherlands and the countries described in this article. In the Netherlands, we had access to police files. The Dutch police files provided unique insight into cybercriminal networks and their members due to the wide-ranging use of investigative methods such as wiretaps and IP taps, observation, undercover policing, and house searches. The analyses of the Dutch criminal investigations were complemented by interviews with the Public Prosecution Service, police team leaders, and senior detectives (including financial and digital experts). This was done because the information in the police files focused on providing evidence of criminal activities, which meant that other information relevant to a scientific analysis was not necessarily included. Ties between members, for example, were not always described in detail in the files, although law enforcement actors may have had a clear picture of them. 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.

In Germany, the UK, and the US, we did not have direct access to police files. Instead, cybercriminal networks were reconstructed solely based on interviews with case officers and/or Public Prosecutors involved in the criminal cases. Furthermore, where possible, official court documents about the cases were analyzed.

Although the method used to analyze the German, UK, and US cases did not provide us with such a detailed picture as the Dutch analyses, the current article does have added value. Firstly, the combination of methods (police files and interviews) used in the Dutch analyses showed that interviews were a good method for gaining insight into cybercriminal networks. On top of that, as mentioned above, the interviews sometimes provide better data about origin and growth and/or ties between members. Secondly, the current article provides a broader picture of cybercriminal networks. It increases current knowledge about cybercriminal networks active in or related to three other countries. Indeed, the main problem with the findings of the networks active in the Netherlands is that the study was conducted solely in the Netherlands; the same study in a different country could paint a different picture due to differences in access to information, policing priorities, and knowledge of or expertise in cybercrime.

The framework was highly dependent on the analytical framework used in the Dutch Organized Crime Monitor, a long-running research program into the nature of organized crime in the Netherlands (see e.g. Kleemans et al. [10]; Kruisbergen et al. [11]).

To make the analysis framework fit the current study, questions about the influence of digitization were added (e.g. the role of forums, the role of the internet in the recruitment of new members, etc.). Topics include the composition and structure of criminal networks, the origin and growth of networks and the use of offender convergence settings. The complete framework can be found in Appendix 1.

In total, 22 cases were analyzed: 9 in the UK, 10 in the US, and 3 in Germany. In these countries case officers were interviewed in order to gain more insight into direct ties, origin and growth, use of forums, and criminal capabilities of criminal networks. The interviews with Dutch case officers and Public Prosecutors showed that these in-depth interviews provide enough information to get a complete picture of the criminal network investigated. Court documents and open source information (e.g. news articles about the case) were used to complement the information provided by the respondents. The 22 cases analyzed covered the period 2003–2014. The interviews about these cases were conducted between March 2014 and November 2015.

Contacts with law enforcement agencies in the different countries were made using existing contacts within the Dutch police (especially the Dutch High Tech Crime Unit) and the Dutch Police Academy. Similar to the selection of Dutch investigations, it was also difficult in these countries to get an overview of completed criminal investigations into cybercriminal networks. Therefore, we used the snowball method. First contact was made with cybercrime teams at the national level: in the UK the NCA (National Crime Agency), in the US the USSS (United States Secret Service) and FBI (Federal Bureau of Investigation), and in Germany the BKA (Bundeskriminalamt). After a first meeting with the team leader, follow-up appointments were scheduled with case officers who had been involved in relevant criminal investigations. With the NCA an agreement was drafted concerning data collection and the use of data.

In the next part of the article, we describe the results of our analyses. Throughout the text, we refer to specific criminal networks. Networks with number 1 to 9 inclusive are part of UK investigations, networks 10 to 19 are part of US investigations, and networks 20 to 22 originate from German investigations.

Results

Origin and growth

The Dutch cases showed four types of growth: (1) completely 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) completely through forums. The UK, US and German networks can also be broken down into these four categories. Regarding 21 networks, we have information about the origin and growth processes.

Origin and growth: social ties

Social ties play an important role in the origin and growth of 16 networks. In eight of these networks, origin and growth is entirely based on social ties. Within eight other networks, social ties form the base, while forums are used for the recruitment of enablers. In these networks, core members and sometimes the most important enablers know each other because they grew up in the same community, have committed offline crimes together or have been in the same prison.

Network 1, for example, is composed of members originating from the Nigerian immigrant community in London. All three core members participated in computer science related degrees at universities. Two of the core members met each other at university during their studies. The core members posted fake job advertisements on online job sites. Clicking on links in the adverts resulted in malware infection. The malware was purchased through a forum. With the help of employees within banks recruited from within the same community, transfer limits of victims' accounts were increased. The core members themselves then recruited money mules within their community. Often, according to respondents, they looked for young and gullible women.

Network 6 and 7 consist of core members who know each other from the underworld of respectively Vietnam and London. Both networks consist of a stable group of core members who have been working together for some time and using enablers – who, for example, provide money laundering services or networks of money mules – they know from the criminal underworld.

Another example is network 11. The two leading core members of this network, establishing and controlling a major international platform on which (cyber) criminals could make payments to each other anonymously, grew up in the same neighborhood.

The two core members of network 13 went to the same university. These core members hack into databases from large companies to steal large quantities of debit card and credit card information. They sell these data in bulk to five wholesalers they all know from the 'offline world'.

Origin and growth: forums

Five networks mainly use forums for origin and growth. Within four of those networks, the core members know each other through forums and recruit enablers to help them carry out specific parts of the crime script. One network (network 15) has only one core member. This core member used forums to find enablers and sell stolen personal data.

Network 3 is a network using homemade malware to steal user credentials from infected computers, and manipulating internet banking sessions. Two of the four core members have known each other online for a long time. They met each other in a chat group on a forum where advanced programmers discuss coding. They have never met in real life according to the respondent. Through other forums they contacted two other coders who help to programme specific parts of the malware.

Network 20 has the same kind of history. Two of the five core members of this network have known each other for years because they are active in online communities and many are active on chat channels about programming, hacking, and fraud. The other three core members joined the group later, but according to the respondent, all have prominent reputations in the online community and have committed various digital crimes (for example, DDoS attacks, ripping movies, and fraud on online auction sites). The network uses an exchanger (a person converting digital currency into real money) on a regular basis. This exchanger advertises his services on several forums.

In conclusion, social ties play an important role in origin and growth processes of 16 cybercriminal networks, while the origin and growth of five networks are primarily based on forums. It is striking that within these cases, examples of prolonged, repeated interaction through online communities can be distinguished, in addition to a more ad hoc search for suitable co-offenders and enablers.

Roles and functions

Regarding all 22 networks, we have specific information about roles and functions. Three networks solely consist of one group of core members. The core members of these networks are able to perform all the steps in the crime script. In all three cases, these networks are specialized in a particular service and also commit fraud. Network 3, for example, develops malware and sells this malware on forums. The group also uses this malware to harvest credentials of customers of financial institutions and markets these credentials via a forum. Network 16 is engaged in the purchase and sale of customer data from financial institutions and provides services to change virtual money into real money and vice versa. Finally, network 18 manages a botnet which can be rented by third parties, for example, to send spam or carry out DDoS attacks. This network also steals user credentials from the computers that are part of the botnet and manipulates Internet banking sessions.

Core members of seven networks use enablers and core members of two other networks to directly manage and control money mules. Core members use enablers for different services: recruitment and/or management of money mules (8), money laundering (3), exchanging digital currency (3), digital tools (3), customer data of financial institutions (2), hacking (2), bank employees being able to alter account settings (2), postal workers being able to intercept post from financial institutions (2), telephone callers (1), and identity forgers (1).

Similar to all Dutch networks, ten of the networks consist of a group of core members, (professional or recruited) enablers, and money mules. The core members are the group of criminals who initiate the criminal activity and without whom the particular offense from the analyzed investigation would not have been committed. Enablers provide specific criminal services. Based on the interviews, it is difficult to distinguish between professional and recruited enablers. Money mules are used to conceal the money trail to the core members (for more information, see [5, 13]).

Structure

As in the Dutch cases, there are dependency relationships and different functions within most networks. In 20 networks, we have specific information about their structure: 16 have a relatively fixed group of core members; and 4 networks consist of core members who co-operate together on an ad hoc basis alongside other criminals.

The networks consisting of subgroups of core members working on an ad hoc basis with each other use forums to find suitable co-offenders (both core members and enablers). These networks are all part of category 3 or 4 types of growth: forums as a base and social contacts to recruit local criminals; and growth completely through forums, respectively. Network 12, for example, is a fluid network of cooperating individual offenders using a forum to find the best criminals to carry out a phishing attack. At the time of the investigation, the network consisted of 10 people. One core member is the coordinator who plans and manages the involvement of others and is in charge of, for example, the distribution of the money. The 'others' are enablers who provide e-mail addresses, create phishing websites, translate texts, put data on credit cards or manage networks of money mules etc. The harvested credentials of banking customers are then partially abused by the core members themselves and partly sold via a forum. In addition to this, core members also use a forum to buy credit card information stolen by other networks.

Network 20 consists of a group of five core members. All core members have already committed various digital crimes and have "won their spurs" in the online hacking community. Two core members have known each other for years and met online through a chatroom on programming. For this specific attack, these two core members enlisted the help of three others because the latter had the capacity to adjust specific parts of malware owned by the two core members.

It would appear that social ties are an important factor for a stable group of core members. Networks with a solid group of core members are usually networks of category 1 and 2: growth completely through social contacts; or social contacts as a base and forums to recruit specialists. Eight networks have members that have been active in the criminal environment and committed miscellaneous offline crime. They originate from the same communities within big cities and/or know each other from jail or earlier criminal jobs. In a number of networks, there is also a link with traditional organized crime. Network 7, for example, consists of core members who have known each other for many years from the London underworld and have strong ties with traditional organized crime in London. For their crime script, these core members need enablers providing hacking services, recruited through existing criminal contacts from a different country. Network 9 and 10 originate from a traditional criminal network that committed all sorts of offline crimes. According to respondents, they are probably also associated with traditional organized crime in Russia. Finally, network 22, a locally operating network in Berlin, has close links with a criminal motorcycle club. The motorcycle club is responsible for managing money mules.

There are also networks with a stable group of core members in which real-world social ties do not play a role. Within these networks, online contacts form the basis. Network 15, for example, consisted originally of one core member stealing user credentials on his own and selling these on his own website. This core member recruited three others online who were running a franchise of the websites established by the original core member. In addition, the four core members of network 3 originally met on a forum, but have been working together for a long time. They have developed malware allowing them to capture user information and manipulate internet banking sessions. They use a forum to sell the malware they have developed.

Criminal capabilities

In order to gain more insight into the criminal capabilities of the networks, we looked at the crime scripts, international components, and the degree of specialization of networks.

All networks are engaged in attacks on customers of financial institutions. In the Dutch cases, the attacks boiled down to phishing and malware attacks. This is also true for most of the international cases. Three networks carry out phishing attacks and 10 networks carry out malware attacks (of which two networks do not attack customers directly, but infect bank computers). Four networks hack into databases containing credit and debit card information, or hire hackers to do so. Four networks buy credit and debit card information on forums. One network operates solely as an enabler for a specific part of the crime script for other networks and does not carry out attacks itself.

The crime scripts can be divided into two categories: networks attacking customers of banks (using malware and phishing attacks) and networks attacking companies controlling financial data of customers i.e. hacking into databases containing credit card and debit card information or hacking directly into the bank systems.

There is a difference between the attacks in the degree of offender-victim interaction. This means there is a difference in user protection against attacks. Phishing attacks require a high degree of offender-victim interaction. Firstly, the victim has to respond to an email and log on to a phishing website to provide login credentials. Secondly, the criminals have to acquire one time security codes to transfer money to money mule accounts. This requires criminals to telephone victims, pose as a bank employee, and convince victims to hand over these codes which can only be used within a short period of time. Malware attacks require a much lower degree of offender-victim interaction. Criminals use emails to lure victims to infected websites, or add infected attachments to emails. Once the victim surfs to the infected website or opens the infected attachment, the computer is infected and is under the control of the criminals. The crime script with the lowest degree of offender-victim interaction is hacking into companies controlling financial data of customers. In those cases, customers of financial institutions are not directly involved in the attack.

Most of the criminal networks analyzed are not dedicated to just one type of crime. Only seven of the 22 networks could be characterized as specialized. The core members of these networks commit only one type of crime whereas the core members of 15 networks are also involved in other types of crime. Nine of these networks also commit offline crime, such as drug trafficking, arranging fake marriages, fraud, robbery, and identity forgery. Core members of five networks are engaged in other forms of cybercrime e.g. renting a botnet for spamming or DDoS attacks, phishing or credit card fraud (in these cases not as the main criminal activity, but as a secondary activity), and mining bitcoins using computers which are part of a botnet.

To show the relationship between the crime scripts, international components, and the degree of specialization of networks, we created a taxonomy of the networks. In Fig. 1, 21 networks are plotted along an X-axis and Y-axis. The Y-axis represents the degree of technology use and the offender-victim interaction. We gave each network a score between 1 and 4 points for high-tech versus low-tech (Y-axis). Networks performing high-tech attacks without offender-victim interaction are given one point. Two points are for networks executing high-tech attacks with a low degree of offender-victim interaction. Three points are for networks performing low-tech attacks with a low degree of offender-victim interaction, whereas networks performing low-tech attacks with a high degree of offender-victim interaction get four points. The networks are plotted in Fig. 1.

The X-axis indicates the degree to which a network has international components. To determine how 'international' a network is, we looked at the countries from which the network members operate and from where the victims originate. The network receives 1 point if both core members and enablers operate from the country from which the police investigation originates and if victims in that country are targeted. If

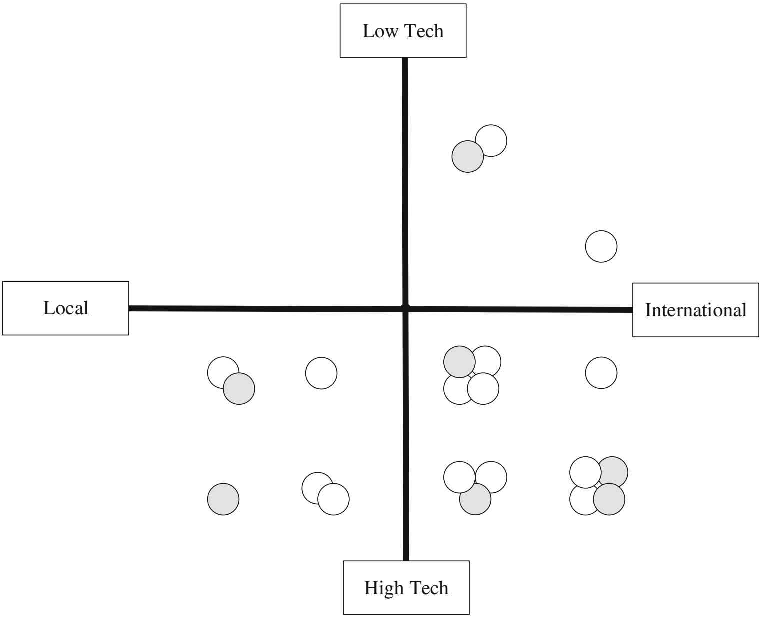

Fig. 1 Taxonomy of networks

there are (also) core members or enablers involved operating from different countries or victims in different countries, a network receives one extra point for each of these categories. In total, a maximum of 4 points is attributable. The networks are plotted in Fig. 1. Finally, Fig. 1 shows whether a network consists of specialists who are engaged in a singular type of attack (shaded) or one that deploys all kinds of criminal activities.

Figure 1 shows the majority of analyzed networks fall into the category of high-tech networks, mostly international high-tech networks. These are networks in which core members, enablers, and victims originate from different countries. None of the networks fall into the category of local low-tech networks. This is a clear difference from the Dutch cases, of which over half of the networks fall into that category (this difference will be discussed below). Finally, in all three categories, there are specialized and non-specialized networks.

Conclusion and discussion

The aim of this study was to complement the current picture of the origin, growth and criminal capabilities of cybercriminal networks. Using the same analytical framework as Leukfeldt et al. [4, 5], we analyzed 22 criminal investigations into cybercriminal networks operating in the UK, US, and Germany. Although the current analysis provides valuable insight into the origin, growth, and criminal capabilities of cybercriminal networks, it also has several limitations (for a more detailed overview of pros and cons of the use of police files see, for example, [14]).

Research limitations

Firstly, there may be a selection effect. The existing contacts with police, especially within the high-tech crime unit, might have led to criminal investigations of high-tech networks. By using the snowball method within a limited time frame, it is possible that we were directed to 'interesting' and 'spectacular' cases. This may explain differences with the Dutch cases; there was more time available for the selection of Dutch cases, resulting in identifying all investigations into cybercriminal networks and thereby examining a cross-section of cases handled by Dutch police. Rationing of cases for prosecution may play a role as well, as the international cases were selected through national agencies (such as, e.g., the NCA in the UK). This may explain why category 1 networks were absent in the international sample, whereas for the Dutch cases, this was an important category. The importance of this article, however, clearly does not lie in 'quantifying' statements. Its aim is to provide more insight into the different types of origin and growth processes and the related criminal capabilities of cybercriminal networks. The results can serve as a starting point for future studies into the functioning of cybercriminal networks.

Furthermore, this analysis is limited to criminal networks engaged in attacks on (customers of) financial institutions (i.e. phishing or malware attacks and hacking into credit and debit card databases). Therefore, it is unknown whether these findings apply to other types of networks, for example, networks of cyber extortionists or distributors of child pornography.

Finally, this analysis only covers cybercriminal networks which are part of a criminal investigation. Therefore, there is only insight into those networks which are under investigation by the police. Networks that remain under the radar of police are not included in the analysis. Future research should also focus on networks not known to the police. This could, for example, be done in cooperation with commercial security companies monitoring parts of the Internet (including digital meeting places) for their clients.

Conclusions

The analysis of the UK, US, and German networks confirm the picture of four different types of growth that were derived from analysis of the Dutch cases: (1) completely 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, (4) completely through forums.

The picture of real-world social ties playing an important role in the majority of networks can be confirmed: this is true for 16 of the 21 networks where we have information about origin and growth. For eight networks, origin and growth were entirely based on social ties and in 8 other networks social ties are the base, whereas forums are used for the recruitment of enablers. For five networks, origin and growth are primarily through forums. Using these digital meeting places, core members meet, recruit enablers and/or sell their criminal services or stolen personal data. It is striking in these cases to find examples of prolonged, repeated interaction through online communities, in addition to the more ad hoc searching and finding of suitable co-offenders and enablers on forums.

Analysis further shows that forums play an important role for the majority of the cybercrime networks. Forums play a role in 18 of the 22 networks and are used by the networks for different purposes: recruiting enablers (4), purchasing tools and services (9) and selling tools and services (9). The four networks that do not use forums at all originate and grow from social ties alone.

In addition, forums appear to provide a more fluid form of cooperation of key members and enablers. A limited number of core members (or even a loner) can thus become international players. Alongside access to a forum it would appear that only one good technician who makes malware, manages a botnet, or hacks into databases is required.

In contrast to the Dutch cases, the structure of the other networks seems to be more diverse, sometimes lacking core members, enablers, and money mules. Core members sometimes perform all aspects of the crime script themselves but even here forums play an important role. On the one hand, this is because there are specialists creating malware or stealing large quantities of financial data by hacking into databases. These groups sell their data to others who resell it on to criminal groups or loners. It is unnecessary, therefore, for these groups to have an entire network of enablers and money mules. On the other hand, there are groups which do not steal information from individuals themselves, but simply purchase the information on a forum or through reliable partners. These groups are dependent on others, but need only a limited number of enablers to carry out their crime scripts.

All networks engaged in attacks on customers of financial institutions. The crime scripts can be divided into two categories: networks using malware and phishing attacks to attack customers of banks, and networks attacking companies controlling financial data of customers. These different crime scripts relate to a different degree of offender-victim interaction and thus a difference in the opportunity for users to protect themselves against attacks. Phishing attacks require a high degree of offender-victim interaction, malware attacks require a much lower degree of offender-victim interaction, whereas hacking into companies controlling financial data of customers, requires no offender-victim interaction at all.

It is also striking that, compared to the Dutch cases, the networks in the US, UK, and Germany more often seem to carry out high-tech attacks. Only 3 of the 22 networks carry out low-tech phishing attacks. The networks are also much more international in nature than the Dutch networks analyzed. Core members, enablers, or victims are from different countries. This finding might be caused by the aforementioned selection effect: the existing contacts with police might have led to more high-tech cases or 'interesting' and 'spectacular' cases.

Discussion

Real world social ties continue to be important in the origin and growth processes of cybercriminal networks. Forums, however, seem to be crucial for a change in the origin and growth of networks, and thereby criminal possibilities. For the majority of the cybercriminal networks, forums play a role in one way or another: as a 'social' meeting place, for buying services, or as a platform for selling stolen goods.

The networks whose origin and growth mainly take place on forums form a special group: they are more fluid than the other networks and a network with a relatively small group of core members is capable of becoming an international player. Indeed, forums ensure that traditional limitations of social ties - especially contacts outside the initial social cluster and recruitment processes dependent upon trust-building - can be overcome. In other words, forums seem to make it possible to quickly make new contacts and expand criminal possibilities.

The members of criminal organizations in which forums play a significant role, would often appear to have been from an early age interested in information technology and often frequent chat groups related to programming. Consequently, it may be interesting to study the young people who are exploring the possibilities of programming or other applications of new technology and, in particular, processes which facilitate or prevent crossing the line to becoming involved in cybercriminal activities.

Notably, it is striking that the networks whose core members met online, are not always fluid in nature. Within these networks we can find examples of relatively stable groups of core members and enablers. Thus, not only real-world social ties enable a stable network, but on some occasions, also virtual-world social ties can operate in a similar way.

An entirely different question is the relative importance of what is going on at forums (see, e.g., [2]). Are forums not simply filled with what is referred to as 'low-hanging fruit'? It is, after all, remarkable that the analyzed networks responsible for stealing millions of credit and debit card credentials, or infecting millions of computers with malware, do not sell this data directly on forums. Instead, they sell their business or services through several layers of intermediaries. Indeed, the source of evil is not on the forum. More research into the role of forums within cybercriminal networks should provide more insight into this challenging issue.

Appendix 1: Analytical framework

Direct ties

- Describe the composition of the criminal 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 criminal cooperation start?
- Do the suspects have a common background? (Family, neighborhood, friends, occupation, place of origin, etc.). If not, in what way are the suspects related and how did the cooperation start?
- What kept the members of the criminal network together? (e.g. 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.

Modus operandi

- Describe the main criminal activities of the network (describe the MO in detail in the next section)
- Describe secondary criminal activities of the network and individual offenders.
- What is the working area of the network (region, country, interaction, certain banks).
- Who are the suitable targets for this network? (which type of people are attacked).

References

1. Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175.
2. Dupont, B., Côté, A., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129–151.
3. Holt, J. T., & Lampke, E. (2009). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50.
4. Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016a). Cybercriminal networks, social ties and online forums. Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. doi:10.1093/bjc/azw009.
5. Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2016b). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. doi:10.1007/s10611-016-9646-2.
6. Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31–41.
7. Peretti, K. K. (2008). Data breaches: what the underground world of "carding" reveals. *Santa Clara Computer and High Technology Law Journal, 25*(2), 345–414.
8. Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2), 111–129.
9. Yip, M., Shadbolt, N., & Webber, C. (2012). *Structural Analysis of Online Criminal Social Networks.* Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI) 2012, 60–65. June 11–14, 2012, Washington.
10. Kleemans, E. R., van de Bunt, H. G., & van den Berg, E. A. I. M. (1998). *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC Monitor* [Organized Crime in the Netherlands]. The Hague: Ministry of Justice / WODC.
11. Kruisbergen, E. W., van de Bunt, H. G., & Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit* [Organized Crime in the Netherlands]. The Hague: WODC.
12. Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(9), 1–6.
13. Leukfeldt, E. R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime, 17*(4), 231–249.
14. Kleemans, E. R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson & E. Cockbain (Eds.), *Applied police research: challenges and opportunities. Crime science series*. Cullompton: Willan.