Original Manuscript

Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline

International Journal of Offender Therapy and Comparative Criminology
1–17

DOI: 10.1177/0306624X19895886
journals.sagepub.com/home/ijo
SAGE

E. R. Leukfeldt[1,2] and Thomas J. Holt[3]

Abstract

This study focuses on the organization practices of networks of cybercriminals engaged in serious financial offenses, through a qualitative analysis of the Best and Luckenbill's sociological framework. The study utilized data collected regarding 18 separate criminals investigations from the Netherlands. The results demonstrate that the participants within these networks operated at various stages of deviant sophistication. Surprisingly, the majority of networks exhibit organizational sophistication based on their division of labor and extended duration over time. In fact, most of this sample could be classified as "teams" or "formal organizations." Furthermore, in contrast with prior studies, no loners were present and only a few networks could be classified as "colleagues" or "peers."

Keywords

cybercrime, cybercriminal network, social organization, hacking, phishing, malware

Criminological inquiry on cybercrime has increased dramatically over the last decade, with some emphasis on economic-motivated offenses (e.g., Holt & Bossler, 2016; Yar, 2013). There are a range of cybercrimes that generate revenue for offenders through the theft and resale of information or the facilitation of fraudulent financial transactions,

[1]Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, The Netherlands
[2]The Hague University of Applied Sciences, The Netherlands
[3]Michigan State University, East Lansing, USA

Corresponding Author:
E. R. Leukfeldt, Netherlands Institute for the Study of Crime and Law Enforcement, De Boelelaan 1077a, 1081 HV Amsterdam, The Netherlands.
Email: rleukfeldt@nscr.nl

including phishing, computer hacking, and the use of malicious software that captures keystrokes and sensitive user information (e.g., Dupont et al., 2017; Holt, 2013; Holt & Lampke, 2010; Hutchings & Holt, 2015; Leukfeldt, 2017; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d; van Hardeveld et al., 2017).

Estimates of the economic impact of these offenses are massive, though debated due to the difficulty in identifying the exact costs to industry and financial institutions (Levi et al., 2016). As a result, the potential harm caused is often expressed in ranges rather than exact figures. For instance, estimates suggest the United States lost between US$57 and US$109 billion in 2016 due to cyberattacks (Council of Economic Advisors, 2018), while global harm ranged between US$445 and US$600 billion in harm to consumers and corporations in 2017 (McAfee & CSIS, 2018).

Actors engaged in financial cybercrimes must have some degree of technical skills to facilitate the offense, or have ties to those who can complete the act on their behalf. The rise of cybercrime markets created a point of connection between technical and nontechnical audiences and engendered a profitable form of offending (Holt, 2013; Hutchings & Holt, 2015; Levi et al., 2016). As a result, policymakers and law enforcement agencies now focus on the organizational dynamics of cybercrime to assess the potential associations between traditional organized crime groups and cybercriminal enterprises (Holt, 2013; Lavorgna, 2015; Lavorgna & Sergi, 2016; Leukfeldt et al., 2017). There is limited empirical evidence of their linkage, though anecdotal evidence argues that traditional organized crime groups operating offline have become involved in cybercrimes and that cybercriminals may operate in structures similar to organized crime groups such as the mafia (Lavorgna, 2015; Lavorgna & Sergi, 2016).

Criminological scholarship examining the organizational patterns of economic cybercriminals has primarily focused on the network ties between actors, finding links between online and offline offenders bridged via forums or online communities (Dupont et al., 2017; Décary-Hétu & Dupont, 2013; Holt, 2013; Holt et al., 2012; Leukfeldt et al., 2017a, 2017b, 2017d; Yip et al., 2013). Local network ties existing in the real world can be sufficient to facilitate financial cybercrimes (Leukfeldt, 2014; Leukfeldt et al., 2017a, 2017c; Lusthaus & Varese, 2017). These studies are valuable, though a portion of this literature is also based on anecdotal or circumstantial evidence (Broadhurst et al., 2014) or on analyses of policy documents (Lavorgna, 2015; Lavorgna & Sergi, 2016).

The majority of these studies also utilize broad definitions of organization that limit their utility in discussion of "organized crime." As a consequence, the notion of organized crime groups operating online and offline persists in both the research and policy communities (Lavorgna & Sergi, 2016). Empirical research is needed that provides more clear conceptualizations of organization to understand the composition of groups and variations across offense types and over time (e.g., Holt, 2013; Leukfeldt et al., 2017).

To that end, research applying sociological models of deviant organization may be able to inform criminological investigations of economic cybercrimes (Adler & Adler, 2005; Best & Luckenbill, 1994; Decker et al., 1998; Holt, 2009; Mann & Sutton, 1998; Meyer, 1989). In particular, criminologists have utilized an organizational framework

created and subsequently revised by Best and Luckenbill (1994) to consider the associations between deviants to engage in various forms of crime online and offline. Applying such a framework to economic cybercrimes could prove essential to better understand offender organizational practices and the extent to which they may resemble organized crime groups and frameworks.

This study attempts to address this gap in the literature through an investigation of 18 offender networks that engendered malware and phishing crimes aimed at users of banks and credit card companies.[1] Police investigations from the Netherlands were used to gain insight into the social organization of cybercriminal networks. Qualitative research methods were used to analyze the materials produced by investigators, including information produced from the use of special investigative powers, such as wiretaps, IP taps, observations, house searches, and interrogations, often carried out over a prolonged period of time. The findings provided a rich and detailed picture of cooperation between criminals, and gave new insight into cybercriminal networks generally.

Examining Social Organization Frameworks

To better inform the state of research on offender organizational practices, criminologists have applied sociological models of social organization to operationalize and measure relationships between deviants, and how such relationships function online or offline (Adler & Adler, 2005; Best & Luckenbill, 1994; Decker et al., 1998; Holt, 2009; Mann & Sutton, 1998; Meyer, 1989). One of the most commonly used frameworks among criminologists was developed by Best and Luckenbill (1994) to distinguish the role of offender associations to facilitate different forms of crime and deviance. The Best and Luckenbill (1994) framework also recognizes that deviant organizations may operate differently across place or time due to variations in local law enforcement, social norms, or local custom. Thus, it provides researchers with a mutable technique to identify organizational structures based on offender relationships.

This framework emphasizes the influence of individuals in structuring the types of activities they may perform within the context of both a social network and deviant subcultures (Best & Luckenbill, 1994). Specifically, deviant acts are dependent upon the presence or absence of collegial associations between actors, any coordination between or specialized roles for participants, managerial positions, and their persistence over time. Best and Luckenbill (1994) argue that deviance can be defined based on the completion of transactions, or behavior focused toward a specific goal that will bring the participants some satisfaction (emotional, economic, or others).

The nature of the transaction necessitates a division of labor, which may vary from a single person to a complex structure of specialized roles involving dozens of participants. For instance, individual deviance requires only one person for an offense to be completed as with deviant acts like self-injury (Adler & Adler, 2005). Acts of deviant exchange require two or more actors working in concert to achieve some end. For instance, prostitution constitutes a form of deviant exchange as the customer and provider must negotiate both the sexual acts to be performed and the fee paid for services rendered (Best & Luckenbill, 1994; Holzman & Pines, 1982).

Table 1. Best and Luckenbill's Social Organization Framework.

Form of organization	Characteristics			
	Mutual association	Mutual participation	Elaborate division of labor	Extended organization
Loners	No	No	No	No
Colleagues	Yes	No	No	No
Peers	Yes	Yes	No	No
Teams	Yes	Yes	Yes	No
Formal organizations	Yes	Yes	Yes	Yes

Source. Best and Luckenbill (1994), p. 12.

Best and Luckenbill (1994) also recognize that the structure of labor is not fixed, but involves "flexible coordination": Individuals can adapt their behavior to satisfy a given situation or disruption in accepted operational practice (Best & Luckenbill, 1994, p. 75). To that end, actors engaged in deviant exchanges may have minimal social ties via a subcultural network or more deep and long-standing associations to complete complex forms of crime. The structure of social relationships may also be dependent on the specificity of their division of labor and group participation in offending. For instance, shoplifting crews require coordinated specialized roles which may persist over time if the group is successful over time (Best & Luckenbill, 1994; Krasnovsky & Lane, 1998). The longer a group engages in offenses together may, however, create risks for disruption or arrest depending on the extent to which actors know the operations of the group and their weak points.

These characteristics define Best and Luckenbill's (1994) continuum of organizational sophistication on the basis of mutual associations, participation in offending, division of labor within network, and duration over time. They argue there are five forms of deviant organization: loners, colleagues, peers, teams, and formal organizations (see Table 1). Loners are the least sophisticated organizational form, as they do not offend with others and have minimal ties to deviants generally. Colleagues are the next most sophisticated group because they create a deviant subculture based on their shared knowledge, though they do not offend together and have no division of labor. In addition, while a deviant subculture may persist over time, actor ties within the subculture do not.

Peers have all the characteristics of colleagues and offend together, though their associations are short-lived and have no organizational sophistication via a division of labor. Teams are more sophisticated than peers as they have a distinct division of labor that enables criminality and their networks persist for longer periods of time. Importantly, teams tend to involve a small number of members who actively seek money or power while avoiding detection from law enforcement (Best & Luckenbill, 1994). Finally, formal organizations are the most sophisticated deviant organization as they include a larger number of members with a specific division of labor, and last for

extended periods of time as a result of more successful operations (Best & Luckenbill, 1994).

Prior Research Examining the Organizational Characteristics of Cybercriminals

Prior research works examining the organizational practices of financially motivated forms of cybercrime have found several key characteristics that influence relationships between participants. Studies of computer hackers found that actors may operate within multiple organizational states at once (Holt, 2009; Meyer, 1989). Specifically, hackers operated within a collegial subculture where sharing information on techniques to manipulate computer hardware and software is highly valued (Holt, 2009; Meyer, 1989). Information exchanges between hackers operated primarily through forums, though some also attended events and social gatherings in the real world depending on the size of their peer networks (Holt, 2009; Steinmetz, 2016).

Although individuals had deviant social ties online and offline, the majority of actors performed hacks alone due to the physical distances between subcultural participants (Holt, 2009). The majority of hackers appeared to operate as colleagues within the Best and Luckenbill (1994) framework, though a small number of peer organizations were present based on some mutual participation in hacks against systems (Holt, 2009; Holt et al., 2017; Meyer, 1989). The generally small number of participants, lack of hierarchical leadership or division of labor, and short life span led researchers to argue these groups relatively unorganized.

Similar organizational structures have been observed in stolen data markets where individuals sell personal information and cybercrime services to interested buyers via illicit payments and trades (Dupont et al., 2017; Franklin et al., 2007; Herley & Florêncio, 2010; Holt, 2013; Holt & Lampke, 2010; Holt et al., 2016; Motoyama et al., 2011; Wehinger, 2011). Buyers and sellers largely existed as colleagues due to their mutual associations within the market and operated in short-term partnerships to achieve specific goals, such as misuse of stolen credit card numbers (Franklin et al., 2007; Holt & Lampke, 2010; Motoyama et al., 2011; Odabas et al., 2017). An individual could buy cards from one seller and then seek out an encasher or provider who would liquidate an account. Buyers could employ these sellers again, or seek out others based on the availability of products and access to resources (e.g., Holt, 2013). Thus, forums fostered a substantive division of labor between participants based on the range of products and services available (Franklin et al., 2007; Herley & Florêncio, 2010; Holt & Lampke, 2010; Motoyama et al., 2011; Odabas et al., 2017; Wehinger, 2011).

At the same time, the websites that actually host forum markets appeared to be teams or formal organizations, as they varied in their organizational complexity, presence of purposive relationships between forums, and persistence over time (Holt, 2013; Holt et al., 2016). Holt and colleagues' (2016) study of 13 forums found eight of their sample constituted formal organizations, whereas the others appeared to be

driven by teams due to their short duration and generally limited organizational complexity. Thus, cybercriminals moved between organizational forms based on the presence of multiple markets operating concurrently in time (Herley & Florêncio, 2010; Wehinger, 2011).

More targeted forms of cybercrime designed to facilitate economic gain, such as phishing and malware campaigns, may operate within similar social organization patterns. Although several studies have considered their operational practices, no researcher to date has utilized the Best and Luckenbill (1994) framework to assess their organizational composition. To that end, prior research suggested a portion of participants participated in online subcultures operating in forums and online communities where hackers and cybercriminals congregate (Leukfeldt et al., 2017b, 2017c). The subcultural ties engendered the formation of offender networks to facilitate an offense based on specialized knowledge or capabilities. Individuals could also identify co-offenders via network ties in the real world, which extended the nature of the organization beyond peers and into teams due to the integration of actors with different skills (Leukfeldt, 2014; Lusthaus & Varese, 2017).

The prospective mix of organizational complexity identified in prior studies of economically motivated cybercrime communities demonstrates the need for further systematic inquiry to identify any variations in the structure of offender associations. In addition, research is needed exploring multiple forms of cybercrime concurrently, including phishing, malware, and hacking schemes due to the potential organizational variations present. Finally, there is a need to better explicate the online and offline associations between offenders to understand how they may shape organizational behaviors generally (e.g., Holt, 2013; Leukfeldt, 2016; Leukfeldt et al., 2017b, 2017c) Thus, this qualitative study explored the social organization of multiple criminal networks involved in economic cybercrimes to improve our knowledge of the social organization of serious forms of cybercrime.

Data and Method

This study utilized data collected regarding 18 separate criminals investigations conducted in the Netherlands. The researchers had access to police files, which provided unique insights into cybercriminal networks and their composition due to the wide-ranging use of investigative methods such as wiretaps and IP taps, observation, undercover policing, and house searches. Police investigation data were not publicly available. The Public Prosecution Service first had to give permission for a police investigation to be scientifically analyzed, while the research proposal was assessed by the Dutch Ministry of Security and Justice's Research and Documentation Centre (WODC). WODC gave advice on the quality (specifically the scientific value) of the research proposal and the topic (including a view on the value it adds to current research projects). Once both approvals were provided, the police investigations had to be physically analyzed in buildings of the police department or the Public Prosecution Service. The researchers were then allowed to read the files of the police investigation and make notes on their own laptops. Any information recorded had to be anonymized. Pseudonyms were used

for each offender within the network (e.g., CM1 for a core member, or MM1 for a money mule), while no information on addresses or social security numbers could be recorded. The anonymized information taken from the police investigations was then stored on an encrypted hard drive on the researchers' laptops.

Analyses of the 18 Dutch criminal investigations were complemented by interviews with the Public Prosecution Service, police team leaders, and senior detectives. The additional data collection was performed to gather more information beyond the evidentiary focus of the police files regarding criminal activities. For instance, ties between members were not always described in detail in the files, although law enforcement actors may have had a clear picture of the underlying relationships. In addition, the interviews revealed data on relationships between actors within the network, binding mechanisms, and opportunity structures that were otherwise less visible to outsiders.

The framework that was used to systematically collect the data 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, for example, Kleemans et al., 1998; Kruisbergen et al., 2012). To make the analysis framework fit this study, questions about the influence of digitization on actor roles were added (e.g., the role of forums, the role of the internet in the recruitment of new members). Topics included the composition and structure of criminal networks, the origin and growth of networks, and any offender convergence settings online or offline, including chat channels and online meeting places on forums and markets. Although various types of online meeting places exist (e.g., open markets versus invite-only markets or markets on the surface web versus the dark web), the data we analyzed did not always contain information about these locations. The primary reason is that our original analytical framework did not included questions about these issues. We only systematically gathered information about whether or not members of the network used either offline or online meeting places and the reasons why they used these meeting places.

An additional reason for the absence of detailed information on meeting places in the data was that police investigations did not always include information about the online locations used. For instance, the interviewee may have indicated that a crypto-market was used or that the suspect bought malware on a forum but did not reveal the exact name of the site. It should be noted that there might be differences between meeting places on the surface web and dark web and between open and invitation-only meeting places (Dupont et al., 2017). Future studies of cybercriminal networks should therefore include more information about the online meeting places themselves to better understand the relationships between actors and locations across offender networks generally.

Analytic Framework

The qualitative data assembled for this analysis were analyzed using guiding questions derived from Best and Luckenbill (1994), along with questions used in social

organization analyses of gang activity (Decker et al., 1998) and computer hackers (Holt, 2009; Meyer, 1989). Organizational behaviors were operationalized and measured based on the ways that "deviant actors organize themselves to pursue their deviant activities" and how "these basic forms differ in organizational features, such as division of labor, coordination among the deviant actors, and objectives" (Best & Luckenbill, 1994, p. 12). To capture variations in organizational patterns over time, the following questions were addressed: "what conditions shape the development and transformation of organizational forms," and "how do organizational forms change over time, and what conditions account for these changes?" (Best & Luckenbill, 1994, p. 12).

Specifically, the first series of questions used centered on the complexity of division of labor, including whether deviants offended together and any evidence of their division of labor. There was also an emphasis placed on the presence of groups, their memberships, any relationships between group members, and any stratification and role specialization present (Decker et al., 1998). Second, the coordination of roles examined relationships between individuals based on stated codes or rules on the regulation of relationships, and the way these rules were defined and enforced (Decker et al., 1998). Finally, purposiveness assessed the relationships between groups and how they specify, strive toward, and achieve goals (Decker et al., 1998). This concept was addressed based on any evidence of operations and crimes performed between multiple groups, and any leisure activities involving these groups.

Findings

To present the findings of this analysis, each category of the Best and Luckenbill (1994) framework were discussed, with specific criminal networks noted to highlight their organizational composition. Appendix contained an overview of all networks, primary offense, and layers and roles within the network.

Loners and Colleagues

In examining the data, the offender networks involved fall within four of the five organizational categories noted by Best and Luckenbill (1994). None of the networks could be labeled as "loners," the least sophisticated form of organization, as all cases developed involved multiple offenders with at least some tie to one another. Only one of these networks, 13, fit within collegial structures as the offenders had a greater degree of divisions of labor and offended together. This network had a limited number of core members and enablers (four core members) who were involved in malware attacks. The core members of these networks were participants in online web forums, markets, and chat groups related to cybercrime, where they actively participated in discussions and engendered the broader cybercrime subculture (e.g., Dupont et al., 2017; Holt, 2013; Holt & Lampke, 2010). In addition, their involvement in online communities enabled them to meet co-offenders who could provide access to tools or knowledge needed to successfully carry out attacks on customers of financial institutions (Dupont et al., 2017; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d).

Although actors within the network had different roles within the course of an offense, such as coding malware, acquiring email addresses, or money laundering, they were largely interchangeable. There were also no observed hierarchical relationship structures between core members, or codified rules of engagement. For instance, one individual who used different service providers to enable malware attacks against various targets. He participated in multiple forums and markets seeking vendors to carry out paid phishing and malware attacks on customers of financial institutions.

Finally, there were a number of actors tied to the core members who were used to carry out attacks and/or to sell stolen data. These individuals were, however, facilitators for offending who were recruited via online platforms with no long-term relationships to the core members. The main actor purchased his malware from a vendor in an online market, as well as 50,000 email addresses from two different online suppliers who offered their services to any client (see also Holt, 2013; Hutchings & Holt, 2015; Leukfeldt et al., 2017b, 2017d) He also used a real-world social tie developed through mutual association in an offline immigrant community within Amsterdam to recruit money mules who could cash checks and obtain funds from the online bank accounts he acquired. Thus, the use of online and offline subcultural ties engendered organizationally unsophisticated forms of offending.

Peers

One of the networks in this sample fit into the third category of the Best and Luckenbill (1994) framework: peers. Actors within this category operated within a shared subculture as with colleagues, and they offended together, though their associations were short-lived and had no real division of labor. Instead, individuals typically played a relatively equal role in the completion of an offense regardless of the actual task they perform (Best & Luckenbill, 1994, p. 33). In addition, peer groups may have recruited others to complete the offense and provided equipment and support when needed (Best & Luckenbill, 1994).

Network 12 had a limited number of core members, ranging from one to five in total, and operated with a limited number of enablers who were often recruited from online markets. There were no observable hierarchical relationships between the core members of the group, but they seemed to be dependent on specialized knowledge held by those in the core to successfully execute their attacks.

Teams and Formal Organizations

The final categories of the Best and Luckenbill (1994) framework were teams and formal organizations. Teams were more sophisticated than peers due to the presence of a distinct division of labor between actors to enable their offending practices. The specific tasks performed differed substantially in the course of the offense, meaning individuals did not equitably share responsibility for the success of any criminal act. As a result, risk was not equitably shared within teams (as compared with peers), and

the number of participants involved should only be as large as is needed to successfully complete an offense (Best & Luckenbill, 1994, p. 53).

Formal organizations were the most sophisticated as they had all the characteristics of teams as well as a longer potential duration of offending over time. Due to the size of formal organizations, they also may have had complex interactions between participants compared with teams. For instance, a small core of members within a larger organization may have actively sought money or power while concurrently avoiding detection from law enforcement. In turn, these members allowed lower level functionaries to be exposed to higher levels of risk due to public exposure and direct involvement in offenses (Best & Luckenbill, 1994). As teams were composed of a smaller number of participants, its members faced a greater general risk of detection compared with those who may be involved in formal organizations at higher levels.

The majority of networks within this sample ($n = 32$) were classified as either a team or formal organization. It was not possible to clearly place all the networks within either category because they all had a hierarchy, a division of labor, persisted over a longer period of time, and operated with the goal to make money and stay clear of law enforcement. With this in mind, there were three main differences to account for segmentation between teams and formal organizations. The first was the formality of the hierarchy observed, as some networks had a very strict chain of command, while others were more fluid. Second, the stability of the relationships between the group of core members and enablers was an important factor as part of the same core members were involved in offending over a longer period of time, committed other crimes with criminals outside this network, and enabled work for a longer period of time for the core members. Finally, how many core members and enablers were involved was an important measure of organizational sophistication.

The majority of our networks ($n = 12$) could be classified as teams [2, 3, 4, 5, 6, 9, 10, 11, 14, 15, 16, 17]. Often these teams worked together to commit crimes over a longer period of time. All of these networks had some hierarchical structure, particularly with core members being responsible for setting up the attacks, enablers that were used by the core members to get specific knowledge or skills to execute the attacks or to buy malware or credit cards, and money mules who were used by the core members to obscure the money trail from victims to core members.

The three core members of Network 11 used malware to get access to online bank accounts. The core members bought and tested multiple variant of malware from different sellers through online markets (see also Dupont et al., 2017; Holt, 2013). Furthermore, the core members bought login credentials from other sellers on an online market with the same goal. The core members were from the Netherlands, Germany, and Turkey and met online via a forum. This was known because the Dutch core member was already under investigation by the police for credit card fraud. The Dutch core member actively sought alternative methods to commit fraud. He used online forums to get insight into the use of malware to get financial credentials and posted a number of questions. The core members used at least five different suppliers of malware and stolen data, and a number of people within their social network to recruit money mules to cash out funds victims' bank accounts.

The remaining four networks within this sample could be labeled formal organizations: 1, 7, 8, and 18. These networks had a hierarchy, a division of labor, persisted over a longer period of time, and sought to make money and stay clear of law enforcement. However, the formality of the hierarchy was stricter with greater stability between the group of core members and enablers at this level. Two of these networks (1 and 8) were essentially traditional gangs. These networks carried out both phishing and malware attacks and sold stolen credit card data. Furthermore, Network 18 carried out malware attacks. Finally, one case (7) involved a cybercriminal market place and a cryptocurrency platform.

Network 1 was an example of a network with ties to traditional offline criminal networks used to carry out phishing attacks. Network 1 consisted of eight core members, nine facilitators, and at least 50 to 60 money mules. The core members controlled the network, with a division of labor as well. For example, one core members was responsible for transferring the money from victim accounts to the money mule accounts. Other core members handled cashing the money. Still, others were responsible for recruiting new money mules or handling other recruiters.

The core members also used facilitators to execute their attacks. Two were hired by the core members to build a phishing website and to make fake identification documents. The faked documents were used to open more bank account for money mules to cash out money. Furthermore, the core members used a female "caller" who telephoned victims who entered their credentials on the phishing website. The caller pretended to be from the bank and tried to obtain one-time security code needed to transfer money. Finally, the core members used eight bank employees who were able to provide the network with detailed information from the system, and one postal employee who intercepted security codes sent to customers by post. Finally, the bottom layer of the network was composed of money mules.

Discussion and Conclusion

Over the last two decades, criminological researchers increasingly focused on the organizational behaviors of cybercriminals, especially those operating within illicit markets (e.g., Dupont et al., 2017; Holt, 2013; Holt et al., 2016; Motoyama et al., 2011; Yip et al., 2013). These studies provided insights into the quantitative networked structures of actors, though researchers question whether they operate in tandem with, or separately from traditional organized crime groups (e.g., Lavorgna, 2015; Leukfeldt et al., 2017). This study sought to consider the organization practices of networks of cybercriminals engaged in serious financial offenses, through a qualitative analysis of the Best and Luckenbill (1994) sociological framework.

The results demonstrated that the participants within these networks operated at various stages of deviant sophistication. No loners were present, reinforcing previous research on the nature of hacking and cybercriminal organizations generally (e.g., Holt, 2009; Meyer, 1989). All of the networks involved individual or group participation in online subcultures operating within forums and other communications platforms that facilitated the exchange of deviant information and resources (Dupont

et al., 2017; Holt, 2013). Only one network could be classified as "colleagues" and one as "peers" due to variations observed in the extent to which offenders within networks offended together.

The majority of the networks in this sample exhibited organizational sophistication based on their division of labor and extended duration over time. In fact, most of this sample could be classified as teams or formal organizations within the Best and Luckenbill (1994) framework. Networked participants had some degree of specialized skills which were essential to facilitate the offense, and the persistence of their relationships over time engendered long-term success and economic gain. This finding contrasted prior research suggesting that hackers operate within a collegial subculture, but perform hacks alone due to the physical distances between subcultural participants. Most hackers operated as colleagues or as peers (Holt, 2009; Holt et al., 2017; Meyer, 1989). Furthermore, research into online crime markets showed that buyers and seller largely operated as colleagues (Franklin et al., 2007; Herley & Florêncio, 2010; Holt, 2013; Holt & Lampke, 2010; Holt et al., 2016; Motoyama et al., 2011; Wehinger, 2011).

Only one of the formal organization networks within our sample involved online platforms used by cybercriminals to either buy or sell credit cards and cybercriminal tools or to facilitate these activities by providing an anonymous cryptocurrency. This finding supported prior research suggesting that the general structure of online marketplaces, such as forums, could be considered as teams or formal organizations in and of themselves (Holt, 2013; Holt et al., 2016). Although prior research has largely used public posts directly within forums without any additional empirical evidence, the interviews and materials collected in this study supported this conclusion as well. Additional research was needed with larger samples of online communities engaged in illicit activities to better assess the organizational sophistication of forums over time (Dupont et al., 2017; Holt, 2009).

In general, this study demonstrated the value of the application of a sociological model of organizational sophistication to understand offender associations and their structure (see also Adler & Adler, 2005; Decker et al., 1998; Holt, 2009). There was also a need for further research to refine this framework for online activities (see also Holt, 2013), as it proved to be difficult to place the more sophisticated networks into the discrete categories of teams or formal organizations. All of these networks had a hierarchy, a division of labor, persisted over a longer period of time, and aimed to make money and stay clear of law enforcement. It was possible to differentiate the networks on the basis of the formality of their hierarchy, as some networks maintained a very strict chain of command, while others were more fluid. Formal organizations were also classified on the basis of the stability of the group of core members and enablers over time and their involvement in the commission of crimes with criminals outside this network.

The nature of the data used in this study also presented a unique challenge to prior social organization research. The majority of prior research utilized data from online forums (Holt, 2013; Meyer, 1989) and in some cases interviews with offenders or

active community participants to assess organization (e.g., Adler & Adler, 2005; Holt, 2009). The use of police files provided distinct information that may not be evident in online data alone, or revealed via interviews with participants. At the same time, only networks known to the police could be analyzed, and insider information obtained by offenders may not be completely revealed to investigators. As a result, further study is needed utilizing unique qualitative data sources that can be triangulated to better understand organizational dynamics.

Limitations

The strength of this study, the unique data collected by law enforcement agencies using special investigative powers such as wiretaps, IP taps, house searches and observations, also limited our findings. First and foremost, the cases included in our analysis were not representative of all criminal activity related to phishing and banking malware. In the Netherlands, we were able to analyze all available cases, though it is unclear whether these findings may be generalizable to the United States, United Kingdom, and other Western nations. This might result in an over-representation of those more organized and unique networks investigated by law enforcement.

Furthermore, offender convergence settings (i.e., online meeting places) played an important role in the processes of the origin and growth of both traditional criminal networks and cybercriminal networks (e.g., Leukfeldt et al., 2017a, 2017b, 2017c). However, future network research on cybercriminal networks should include more detailed information about the online meeting places. This is particularly important as cybercriminals increasingly utilize Tor and encryption methods to better obfuscate their activities online (Hutchings & Holt, 2017). As noted in the "Data and Method" section, the police files did not always contain detailed information about the sources of meeting locations generally. We do, however, know that various types of online meeting places exist (e.g., open markets versus invite-only markets or markets on the surface web versus the deep web).

As there were no quantified metrics to assess the total number of actors or length of time needed to differentiate a team from a formal organization, additional research is needed to refine the Best and Luckenbill (1994) framework and improve the clarity of its categories (see also Holt, 2013). Further study is also needed with different forms of cybercriminal activity to assess the extent of organizationally sophisticated offender networks in cybercrime generally. This study focused only on financially motivated networks that carried out phishing, malware, or hacking activities aimed at getting credit card info are part of our analysis. Gathering data from other financially motivated cybercrimes, such as ransomware and botnets, as well as nonfinancially motivated cybercrimes affecting property, such as ideologically motivated defacement and distributed denial-of-service (DDoS)-attacks, is essential to understand the applicability of the Best and Luckenbill (1994) framework as a whole.

Appendix

Overview of Networks.

Network number	Primary offenses	Network layers[a]	Roles within the network[b]
1	Phishing	4	Coordinator, caller, casher, bank employee, post worker, developer phishing website, falsifier identity documents, money mule recruiter, money mules
2	Phishing	4	Caller, transferring money, money mule recruiter, cashing, money mules
3	Phishing	2	Casher, money mule recruiter, money mules
4	Phishing	3	Casher, money mule recruiter, money mules
5	Phishing	3	Casher, money mule recruiter, money mules
6	Malware	3	Coordinator, developer phishing website, money mule recruiter Europe, money mule recruiter Russia, translator, spammer, casher, money mules
7	Carding forum	3	Administrator, moderator, member
8	Phishing	4	Coordinator, caller, transferring money, spammer, casher, money mule recruiter, money mules
9	Phishing	4	Bank employee, casher, money mule recruiter, money mules, falsifier identity documents
10	Phishing	3	Caller, transferring money, cashing, postal employee, bank employee, money mule recruiter, money mules
11	Malware	4	Coordinator, malware writer, telecom provider, caller, money mule recruiter, money mules
12	Phishing	4	Obtain logins, falsifier identity documents, cashing, money mule recruiter, money mules
13	Malware	4	Obtain logins, spamming, malware writer, postal employee, money mule recruiter, money mules
14	Phishing	3	Bank employee, caller, transferring money, falsifier identity documents, cashing, money mule recruiter, money mules
15	Phishing	4	Coordinator, malware writer, malware adapter, cashing, money mule recruiter, money mules
16	Phishing	4	Falsifier identity documents, cashing, money mule recruiter, money mules
17	Phishing	4	Spamming, caller, cashing, money mule recruiter, money mules
18	Malware	4	Coordinator, falsifier identity documents, cashing, money mule recruiter, money mules

Note. This table does not include exact numbers of members involved in the network because the actual number of members involved in the network varies over time (e.g., because new people are recruited, existing members have fights among each other and kick certain members out). Therefore, this table includes indicators that remain stable over time and also provide insight into the size of networks: the number of layers within the network and the types of roles within each network.
[a]These layers have been described in depth by Leukfeldt et al. (2017a, 2017c) In short, Layer 1 are the core members. These members of the network initiate and coordinate the cyberattacks. Furthermore, they direct the members in the other layers of the network. Layer 2 consist of professional enablers. These enablers provide illegal services to the core members, for example, falsifying identity documents, developing malware of laundering money. These enablers are qualified "professional" because they offer their services to the core members on their own initiative and provide these services also to other individuals or networks. Layer 3 are the recruited enablers. These persons also provide illegal services to the core members, but do not do this at their own initiative. Instead, they are encouraged or forced by the core members to do this. Recruited enablers are relevant for the criminal network for various reasons, for example, because they have access to relevant financial information. Layer 4 are the money mules. Money mules are used by the core members or by enablers to interrupt the financial trail to the core members. Money mules provide their bank account (i.e., debit card and pin code) to the criminal network. Money from the accounts of victims is transferred to the accounts of money mules and is cashed as soon as possible. The digital/financial trail ends by the money mule. [b] It is possible that there are more roles within a network. The roles described here were distilled from police investigations; however, the police investigation might be limited to specific parts of the network and only include a limited number of suspects and roles.

Authors' Note

The data analyzed in this study were collected during the PhD study of the first author.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: That study 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.

ORCID iDs

E. R. Leukfeldt https://orcid.org/0000-0002-3051-0859
Thomas J. Holt https://orcid.org/0000-0002-5894-0172

Note

1. For this article, only networks that used phishing or malware to attack customers of banks or credit card companies were included. We defined phishing in this article as the process of deception, that is, impersonation, to retrieve personal information to get access to online bank accounts or credit card credentials (for an analysis of phishing definitions, see Lastdrager, 2014). Phishing often starts with a deceptive email, but fake websites and fraudulent phone calls are also used to intercept user credentials. We define malware as malicious software designed to infect a device, including viruses, worms, Trojan horses, and spyware. In this case, the malware targets online banking credentials and systems.

References

Adler, P. A., & Adler, P. (2005). Self-injurers as loners: The social organization of solitary deviance. *Deviant Behavior*, *26*(4), 345–378.

Best, J., & Luckenbill, D. F. (1994). *Organizing deviance* (2nd ed.). Prentice Hall.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*, *8*(1), 1–20.

Council of Economic Advisors. (2018). *The cost of malicious cyber activity to the U. S. economy*. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

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

Decker, S. H., Bynum, T., & Weisel, D. (1998). A tale of two cities: Gangs as organized crime groups. In J. Miller, C. L. Maxson, & M. W. Klein (Eds.), *The modern gang reader* (pp. 73–93). Roxbury Publishing.

Dupont, B., Cote, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *American Behavioral Scientist*, *61*(11), 1219–1243.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM Conference on Computer and Communications Security (CCS)* (pp. 275–288). Association for Computing Machinery.

Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of information security and privacy* (pp. 33–53). Springer.

Holt, T. J. (2009). Lone hacks or group cracks: Examining the social organization of computer hackers. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the internet* (pp. 336–355). Prentice Hall.

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

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Internet-based radicalization as enculturation to violent deviant subcultures. *Deviant Behavior*, *38*(8), 855–869.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. Springer.

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

Holzman, H. R., & Pines, S. (1982). Buying sex: The phenomenology of being a john. *Deviant Behavior*, *4*(1), 89–116.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11–30.

Kleemans, E. R., Van den Berg, E. A. I. M., Van de Bunt, H. G., Brouwers, M., Kouwenberg, R. F., & Paulides, G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor* [Organised Crime in the Netherlands: Report based on the Organised Crime Monitor]. Boom Lemma.

Krasnovsky, T., & Lane, R. C. (1998). Shoplifting: A review of the literature. *Aggression and Violent Behavior*, *33*(3), 219–235.

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

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1–10.

Lavorgna, A. (2015). Organized crime goes online: Realities and challenges. *Journal of Money Laundering Control*, *18*(2), 153–168.

Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, *10*(2), 170–187.

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

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International.

Leukfeldt, E. R. (Ed.). (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Eleven International.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*, *67*(1), 21–37.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). 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.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39–53.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017d). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, *61*(11), 1387–1402.

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

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. L. (2016). *The implications of economic cybercrime for policing*. City of London Corporation.

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

Mann, D., & Sutton, M. (1998). Netcrime: More change in the organization of thieving. *The British Journal of Criminology*, *38*(2), 201–229.

McAfee & CSIS. (2018). *Economic impact of cybercrime: No slowing down*. https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Pressandutm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21andutm_medium=emailandutm_term=0_7623d157be-bb9303ae70-

Meyer, G. R. (1989). *The social organization of the computer underground* [Master's Thesis, Northern Illinois University]. http://csrc.nist.gov/secpubs/hacker.txt

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 71–80). Association for Computing Machinery.

Odabas, M., Holt, T. J., & Breiger, R. L. (2017). Governance in online stolen data markets. In J. Beckert & M. Dewey (Eds.), *The architecture of illegal markets: Towards an economic sociology of illegality in the economy*. Oxford University Press.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. New York University Press.

van Hardeveld, G. J., van Webber, C., & O'Hara, K. (2017). Deviating from the cybercriminal script: Exploring tools of anonymity (mis) used by carders on cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244–1266.

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

Yar, M. (2013). *Cybercrime and society*. Sage.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516–539.