Deviant Behavior

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/udbh20

Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes

E.R. (Rutger) Leukfeldt & R.A. (Robert) Roks

To cite this article: E.R. (Rutger) Leukfeldt & R.A. (Robert) Roks (2021) Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes, Deviant Behavior, 42:11, 1458-1469, DOI: 10.1080/01639625.2020.1755587

To link to this article: https://doi.org/10.1080/01639625.2020.1755587

DEVIANT BEHAVIOR
2021, VOL. 42, NO. 11, 1458–1469
https://doi.org/10.1080/01639625.2020.1755587

Routledge
Taylor & Francis Group

Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes

E.R. (Rutger) Leukfeldt[a] and R.A. (Robert) Roks[b]

[a]Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam the Netherlands and Academic Director Centre of Expertise Cybersecurity, the Hague University of Applied Sciences, Amsterdam, The Netherlands; [b]Erasmus School of Law, Erasmus University Rotterdam, Rotterdam, The Netherlands

ABSTRACT

This article explores the intersections of street crimes and cybercrimes. Fourteen Dutch criminal investigations into networks that committed cybercrimes were analyzed to gain insight into offline and local dimensions of these activities. Firstly, we examined whether the networks in these cases are also involved in other criminal activities than cybercrimes. Secondly, we analyzed the origin and growth of these networks, with specific attention for the role or offline interactions on the physical streets. Thirdly, we explored whether the cases contained information that would indicate the presence of a street culture informing the activities of the offenders. Our analysis of both the criminal activities and the origin and development of the cybercriminal networks highlights the ongoing importance of the offline world. However, our results shed light on more than just the "hidden face of cybercrime." Based on their linguistic practices and motives and neutralizations, we see examples of how core members, recruiters, and money mules in different cases are embedded in Dutch street culture. Our findings, therefore, indicate that cybercrime cases could also be interpreted as digital diversifications of traditional street (economic) street crimes and, thereby, as empirical examples of street offenders adapting to the rise of technology.

ARTICLE HISTORY
Received 14 January 2020
Accepted 29 March 2020

Introduction

In "The Digital Street" (2019:ix) Lane notes how street life in the past few years has "decoupled from its geographic location to split along the physical street and the digital street." Lane postulates that the rise of digitally networked technologies, like social media platforms Facebook and Twitter, has impacted street life. Nowadays, the experiences of youth get filtered through digital technology, resulting in the street code being created in both physical and digital spaces. In line with the central premise of the work of Lane (2015, 2019)), Pyrooz, Decker, and Moule (2015) argue that the Internet has changed the opportunities available for many aspects of social life in urban environments, including in the realm of crime and deviance. In particular, Pyrooz et al. (2015: 473) note "that it is important to understand how offenders adapt and use rising powerful digital technologies, and whether this parallels or diverges from street offending." Their findings suggest that while "the Internet has reached these inner-city populations, access alone is not translating into sophisticated technological know-how" (Pyrooz, Decker, and Moule 2015: 472) and that "gangs exploit the Internet to further their collective identity rather than for instrumental means" (Pyrooz, Decker, and Moule 2015: 493).

CONTACT E.R. (Rutger) Leukfeldt RLeukfeldt@nscr.nl Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam The Netherlands and Academic Director Centre of Expertise Cybersecurity, The Hague University of Applied Sciences, Postbus 71304,1008 BH, Amsterdam, the Netherlands

To date, most of the research on the use of digital technologies by offenders has been carried out in the burgeoning field of cybercrime (for example, Holt and Bossler 2014; Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c; Lusthaus 2018). Although these studies have enhanced our understanding of criminality in cyberspace, their focus on the online aspects of these criminal activities tends to neglect "the hidden face of cybercrime" (Lusthaus and Varese 2017): the offline and local dimension (see also Lusthaus 2018: 146–170; Leukfeldt, Kleemans, and Stol 2017a, 2017b; Leukfeldt 2017). Conversely, only a few studies have explored the transforming social interactions of street-oriented individuals and gangs (Lauger and Densley 2018; Moule, Pyrooz, and Decker 2014; Patton et al. 2019; Pyrooz, Decker, and Moule 2015; Roks 2016; Storrod and Densley 2017; Stuart 2019; Urbanik and Haggerty 2018; van Hellemont 2012). Moreover, the existing research into the changing nature of street life and street culture as a result of the growth of technology has centered on expressive, symbolic aspects, such as reputation building, identity construction, and the changing dynamics of (online) violence (for an overview, see Irwin-Rogers, Densley, and Pinkney 2018; Peterson and Densley 2017). Pyrooz, Decker, and Moule (2015: 493) conclude that future research might show more advanced use of the Internet "once gangs acquire the technological knowhow to exploit the instrumental opportunities available online."

To examine the transforming social life of the street, Lane (2015: 46) bridges urban and digital approaches to street life, because "each have particular commitments in their respective fields that when combined can be mutually beneficial." In this article, we undertake a similar endeavor by bridging the study of (economic) street crimes and cybercrimes. We draw on empirical research into 14 criminal investigations in the Netherlands on cybercriminal networks that have been involved in financially motivated online crimes like phishing and the use of malware to gain access to online bank accounts. Earlier analyses of these cases have been carried out from a cybercrime-perspective, focusing on the origin, growth, and criminal capabilities of these cybercriminal networks (Leukfeldt 2014; Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c). However, the current analysis starts by looking beyond cyberspace and focusing on street crimes and street culture. To explore the intersection(s) of (economic) street crimes and cybercrimes, we zoom in on the offline and local dimensions of these (cyber)criminal activities. Firstly, we examine whether the networks in these cases are also involved in criminal activities other than cybercrime. Secondly, we discuss the origin of these networks and their recruitment processes, paying specific attention to the role of offline interactions on the physical streets of the urban environment. Lastly, we explore whether these cases reveal the presence of a street culture amongst the offenders in the networks (Hallsworth 2013; Ilan 2015). In doing so, we question whether the criminal activities that have been labeled as cybercrimes by Dutch law enforcement agencies could also be seen as digital (economic) street crimes.

This paper proceeds as follows. Firstly, we give an overview of research into economically motivated street crimes in a digitized world. Subsequently, the methodological background of the current study is outlined. Thirdly, in the results section, we discuss the central findings of our analysis of cybercrime cases as street crimes. Lastly, we discuss the (theoretical) implications of our results and propose some directions for future research at the intersection of street crime and cybercrime.

Economically motivated street crimes in a digitized world

Traditionally, the streets and street corners of urban environments are the home of economically motivated street crimes. Within these settings, scholars have identified a range of instrumental criminal activities, ranging from "amateur and playful" to professional, high end and high value criminal transactions (Ilan 2015: 89). In-depth accounts of street and gang cultures operating within local neighborhoods in the United States (for instance, Anderson 1999; Bourgois 1995) and in Europe (for instance, de Jong 2007; Densley 2013; Ilan 2015; Roks 2016; Sandberg and Pedersen 2011; van Hellemont 2015) have illustrated that the street economy offers a plethora of criminal opportunities for motivated street-oriented individuals. A central commonality in these studies is the

ways community characteristics shape illegitimate offending opportunities, with most research foregrounding the local drug trade as a means of generating income.

The majority of the abovementioned studies were conducted before the omnipresence of the Internet had transformed many aspects of social life in the urban environment. Technology, as Moule et al. (2014: 1419) argue, "is a values-neutral medium that provides new, and different opportunities for dangerous, deviant, and criminal behaviour, especially for individuals engaged in street crime." The Internet might also be a suitable environment to expand criminal activities, providing new opportunities for making money (Pyrooz, Decker, and Moule 2015: 491). However, in their research on gang and non-gang members in the United States, Pyrooz, Decker, and Moule (2015: 492) found gangs were engaging in mostly expressive rather than instrumental online activities. Building on this instrumental/expressive dichotomy from the research on gangs (Decker and Pyrooz 2013), Storrod and Densley (2017) seek to answer whether the use of social media by gangs in London is expressive, instrumental, or both. The findings from their social media context analysis of UK-based youth, however, suggest a convergence of expressive and instrumental online behaviors, illustrating that expressive activities can also achieve instrumental goals, and vice versa (Storrod and Densley 2017: 817).

Several studies have illustrated that street-oriented people make use of new and different technological opportunities for economic gain. For instance, in his ethnography of gangs in London, Densley (2013) describes how the gang members in his study exchanged illegal goods, services, and information via online auction sites, virtual gaming worlds, chatrooms, PayPal accounts, and synchronous conferencing protocols. Similarly, research on street-oriented youth in the Netherlands (Roks and van den Broek 2017) and the UK (Storrod and Densley 2017) documents how online communication technologies like BlackBerry Messenger and WhatsApp, and social media sites like Twitter, Facebook, and Instagram, are used to sell stolen property or narcotics. Social media in particular seems to provide new opportunities for both the purchase and sale of narcotics. In their recent exploration of the use of social media and encrypted messaging apps to supply and access drugs, Moyle et al. (2019: 102) describe how the use of "Emoji's" "provide the gateway to access advertisements for sales of a range of substances: a diamond or snowflake for cocaine, a capsule for MDMA, and a needle for heroin." The findings of Moyle et al. (2019: 108) indicate that "apps ranging from encrypted messaging services to social media platforms are fast becoming a viable option for accessing drugs."

In addition, there are also some examples of more advanced uses of technology in economic street crimes. Storrod and Densley (2017: 680), for instance, note that research indicates that some gangs use "the internet to commit cybercrimes such as hacking, phishing, fraud, money laundering and selling stolen goods." Furthermore, Densley (2013: 99) signals that gang members use "basic stenography to hide information within image and audio files and applications that allow users to send private messages that, like the film Mission Impossible, literally self-destruct in seconds." More recently, Storrod and Densley (2017) describe how real-time data were integrated into certain aspects of gangs' instrumental activities. Their research indicate an extreme form of "remote mothering" online, with gang members tracking the whereabouts of younger gang members "at all times via locations tags, GPS tracking, pictures and video calling," amongst other things to monitor their drug dealing (Storrod and Densley 2017: 688).

Current study

The overview of the emerging literature on street offending in a digitized world illustrates how technological advancements are, or could be, utilized to facilitate and enhance already existing street economic crimes. Pyrooz, Decker, and Moule (2015: 492) state that in their research neither the gang members nor their non-gang peers had "the technological competency to engage in complex forms of cybercrime." Moreover, as Ilan (2015: 89) notes, it "is extremely difficult to engage in economic street crime to any great level of dedication and success without appropriate street cultural

competencies and networks." However, research in the field of cybercrime indicate that not all street-oriented individuals or gang members need highly advanced technological skills to engage in cybercrime (see, for Leukfeldt 2017; Leukfeldt, Kleemans, and Stol 2017b). Therefore, in this article, we will look at cybercriminal activities from a perspective that goes beyond the cyber-elements. We will address three research questions. First of all, to what extent do the networks in the cases we studied commit criminal activities other than cybercrime? Secondly, what role do both online and offline interactions play in the origin and growth of the networks? Lastly, to what extent do these cases reveal elements of a street culture (Ilan 2015)?

Methods

For this study, we used data collected by the first author in the period 2013–2015 (see, for a detailed description Leukfeldt 2016). The data were gathered to gain insight into cybercriminal networks (cybercrime articles based on the data include Leukfeldt 2014; Leukfeldt and Kleemans 2019; Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c). However, during the analysis of the data, it was discovered that many of the cybercriminal networks were not actually that specialized in cybercrime at all. On the contrary, a number of networks seemed to be traditional criminal networks that also committed cybercrimes. Therefore, for this article, we concentrate on those networks that operate from the Netherlands, because we have unique insight into the modus operandi (including primary and secondary criminal activities) and origin and recruitment process of these networks. Our analysis, therefore, consists of 14 networks out of the original 18.

Fourteen Dutch criminal investigations into criminal networks that committed cybercrimes were analyzed to gain insight into the offline and local dimensions of these (criminal) activities. The criminal investigations into these networks lasted between six months and three years. The Dutch police – sometimes with the help of law enforcement agencies from other countries – carried out these investigations in the period 2004–2014.

The police investigations we analyzed are not publicly available. The research proposal had to be assessed by the Research and Documentation Center (WODC) of the Dutch Ministry of Security and Justice, which gives advice on the (scientific) quality of the research proposal and the research topic (e.g. added value regarding current research projects). Furthermore, the Public Prosecutor's Office ("College van PG's") must give permission for the scientific analysis of a police investigation. We only used investigations into criminal networks that had been completed by the police, that is, the investigation team had collected enough evidence for the public prosecutor to decide to prosecute the suspects. This means that we do not know if a judge eventually convicted the members of the criminal networks. Excluding cases where no ruling is yet available would mean that only a few cases would remain because it may take years before suspects are convicted (after appeal).

The police investigations contain a wealth of information because of the use of special investigative powers, such as wiretaps, IP taps, interrogations and analysis of seized computers. Some of these police files can consist of thousands of pages of relevant (and non-relevant) information. Therefore, an analytical framework was used to systematically gather relevant information. It took the first author of this study between two days and two weeks to analyze each police investigation (which meant filling in the analytical framework (see Annex 1), and the actual analysis was carried out based on the raw data, i.e. all the completed analytical frameworks). The framework was inspired by the analytical framework used in the Dutch Organized Crime Monitor, a long-running program researching the nature of organized crime in the Netherlands (see, for example, Kruisbergen et al. 2018). The analytical framework included the following topics (see Annex 1 for an overview of all relevant topics in the framework):

- General information about the case (including case number, date of the analysis and names of relevant respondents that were interviewed).

- Case information (e.g. investigation code name; relations with other criminal investigations; location, size, and composition of investigation team).
- Short overview of the investigation (e.g. what was the starting point for this criminal investigation; on which criminal offenses did the investigation focus; which investigative methods have been used?).
- Structure of the criminal network (e.g. total number of suspects; description of each of the suspects; the structure of the criminal network; the composition of the criminal network: changes within the composition of the criminal network).
- Origin of the criminal group and binding mechanisms (including how, when and where did the criminal cooperation start; do the suspects have a common background? (family, neighborhood, friends, occupation, place of origin, etc.).
- Modus operandi (e.g. the main criminal activities of the network; the secondary criminal activities of the network and individual offenders; the working area of the network).

In order to get as much relevant information per topic as possible, the file analysis was complemented by interviews with the Public Prosecution Service, police team leaders, and senior detectives (including financial and digital experts). Indeed, police files only include the information that is needed to prosecute the suspects. For example, information about ties between members who carry out secondary criminal activities might not always be included in the police files. However, the actors we interviewed could shed light on these topics. Each interview was carried out using an interview protocol. This interview protocol was in essence the analytical framework (see Annex 1).

Cases were selected using the snowball method. Unfortunately, there is no central registration system in the Netherlands that allows for a quick overview of all criminal investigations into specific criminal networks. The first author used his network within the Dutch police and other relevant parties, for example, public prosecutors, primarily cybercrime teams, fraud teams, and members of the Dutch Police Academy, to identify cybercriminal networks. Furthermore, an online database in which court documents are published was used and media analysis was done to find news reports about relevant cases. During the file analysis, law enforcement officers and public prosecutors involved in the criminal investigation were asked whether they knew any other relevant cases.

The networks in our analysis all committed cybercrimes. However, not all types of cybercrimes are included. As the original data collection focused on phishing and banking malware networks, only criminal networks that carried out these activities are included. Phishing is the process that aims to obtain users' personal information by criminals posing as a trusted authority through digital means, such as e-mail (see, for example, Lastdrager 2014 for a systematic overview of phishing definitions). In our files, the criminals used phishing to gain access to online bank accounts in order to steal money from these accounts. Usually, the criminals sent an e-mail that appeared to be from the victims' bank. The e-mail refers to an issue that has to be addressed as soon as possible. For example, a security procedure has to be finished in order to not be banned from the bank. Thereafter, the victim has to log on to the website of the bank (which is actually a fake website controlled by the criminals), or has to perform another action which results in giving the criminals access to the online bank account (the modus operandi will be described in depth later in this article). Criminals can also take control of online bank accounts through more technological means. They can use malicious software – also named malware – such as trojan horses or spyware to intercept credentials or manipulate entire online banking sessions.

Results

We start by describing the modus operandi of the networks, including the primary and secondary criminal activities. Next, we concentrate on the origin of the networks and their recruitment processes. Finally, we address the presence of street culture within these cybercriminal cases.

Modus operandi: an array of online and offline crimes

The 14 networks in our study are involved in financially motivated online crimes: they use phishing and malware to gain access to victims' online bank accounts to steal their money. This is no surprise, as these networks were selected based on this modus operandi (see the methods section for more details on the selection process). However, there are distinctive differences in the type of financially motivated online crimes these networks commit and their involvement in other types of crime. Based on their primary modus operandi, the 14 networks can be divided into two categories: networks that only commit online crimes (networks 2, 4, 10, 13, 15, 17) and networks that commit both online crimes and traditional offline crimes (networks 1, 3, 5, 8, 9, 12, 14, 16).

The networks in the first category mainly commit a particular form of online crime. Networks 2, 4, 10, and 17 are all involved in phishing, while network 15 uses malware to gain control over online bank accounts. Furthermore, the members of network 13 commit both malware attacks and phishing attacks on banking customers and are involved in online consumer fraud. The crime scrips of all phishing cases have major similarities. First, criminals try to obtain the login credentials for victims' online bank accounts. In the case of phishing, criminals send potential victims an e-mail that looks like an e-mail from their bank and try to persuade the victim to click on a link that leads to a fake website controlled by the criminals that looks exactly like the bank's official website. Once the victim logs onto the website, the criminals know their login credentials and are able to access that bank account whenever they want. The second step is to transfer money from the victim's account. In order to do this, a one-time security code is needed. All major Dutch banks use different methods to generate this one-time code, but criminals that use phishing in the Netherlands usually simply telephone the victims at this point of the crime script (for an in-depth description see, for example, Leukfeldt 2014). Money is transferred to the bank accounts of so-called money mules and cashed out as fast as possible. In some cases the criminals do not cash out directly, but rather buy goods with the stolen money.

However, the police information on network 2 also illustrates that members of these cybercriminal networks are involved in other criminal activities:

> Sometime last year, I think it was in June or July, I went to Amsterdam to meet friends at a bar. At that place, I met a guy who introduced himself as Jimmy. I don't know his real name. In the bar, I had a conversation with Jimmy. At one point I asked him how I could make money. Jimmy responded that it was easy. I had already told him that I lived in [smalltownintheNetherlands] and that I made money selling drugs. Sometime later, I went outside with Jimmy and some other guys. Jimmy said he could make us rich, really rich and in a very simple way. He said that he used bank cards and that the money was transferred to the accounts and had to be withdrawn. The owner of the account would then receive a percentage of the money that was withdrawn. (Network 2)

In this case, phishing could be seen as a diversification of the already existing criminal activities of some of the offenders in the network. However, no legal evidence of involvement in the drug trade could be found in this specific case.

In category 2, we see networks of offenders that are involved in phishing, but that also carry out a variety of other more traditional offline criminal activities. For example, the members of eight of the 14 networks had been active in the criminal underworld in some major Dutch cities and had carried out many types of criminal activities within their own regions (networks 1, 3, 5, 8, 9, 12, 14, 16). For instance, two of the core members of network 1 were arrested for smuggling drugs into the Netherlands during the investigations into the phishing activities. In addition, another key member of network 1 was also involved in what is known as "spear phishing," attacking one of the largest flower wholesale companies in the Netherlands. Other core members were involved in skimming or fraud concerning cell phone contracts. Furthermore, network 9 was classified by the Dutch law enforcement agencies as a criminal youth gang whose members, in addition to many types of traditional crimes such as street robberies and shoplifting, were involved in recruiting money mules and cashing out money stolen from online bank accounts. Moreover, offenders were involved in drug trafficking (networks 3, 9 and 16), human trafficking

(networks 3 and 12) and burglary and theft (networks 1, 5 and 8). Finally, we see offenders carrying out other types of fraud (with phone subscriptions or healthcare subsidies), as well as fencing and street robberies.

Origin and growth of the networks: offenders navigating online and offline spaces

In the origin and growth of the networks in these cases, we also clearly see how offenders navigate online and offline spaces. First, however, it is important to note that networks in the present study are comprised of three different layers with specific membership roles: core members, facilitators, and money mules (see also Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c). Core members initiate the network and its criminal activities and, in addition, direct other members and coordinate the criminal activities. Although the cases we studied do not always contain information about how the networks originated, most of the core members appear to have been actively involved in crime for some time and knew the other offenders from previous criminal endeavors. In other cases, the social ties of offenders could be traced back to the streets in the neighborhoods where they grew up or currently reside. In the layer below the core members, we find facilitators who provide specific services to the core members and usually work for multiple criminal networks. In the recruitment of facilitators, we can observe the importance of social contacts, despite the availability of phishing services and plug-and-play malware on the dark web.

Finally, the last layer in the networks is comprised of so-called money mules: individuals who cash out the money that is transferred to their bank accounts by core members or facilitators (for more detail, see Leukfeldt 2014). Money mules can be easily replaced, but they play a significant role in the phishing activities. After all, without the money mules core members cannot access the victims' stolen money. Money mules are often the first to be apprehended by the police because their bank accounts can be traced directly to the victims. Moreover, in the case of unusual or suspicious transactions, their accounts are blocked by the banks and are no longer useful for phishing activities. Therefore, networks need a constant flow of money mules to successfully complete their phishing activities.

The recruitment of money mules seems to take place both online and offline. First, we see how money mules are being recruited through offline social contacts. For instance, a money mule in network 3 declared that a classmate approached him to ask whether he wanted to make 800 euros by handing over his debit card and PIN number. Similarly, during interrogations money mules declare that they were approached at school or at a gym by friends of acquaintances, but also by strangers whilst hanging out on the streets in their local neighborhoods. After being approached, contact information is exchanged and potential mules are contacted through digital messenger services like Blackberry Ping or WhatsApp.

In addition to approaching potential mules on the physical street, the cases contain several examples of recruitment on the digital street (Lane 2019). For example, a money mule in network 5 stated: *"On the streets, I hear about a lot of opportunities to commit fraud. Even on Facebook you receive this kind of messages about earning some money."* A money mule in network 10 also referred to social media – in this case Twitter – as a platform to approach potential mules, in addition to the chat functions of mobile phones. These networked publics – referring to the ways (young) people's peer worlds are embedded in social media (Boyd 2014: 11–14) – have several distinct characteristics from traditional physical public spaces. Four affordances in particular tend to shape the mediated environments created by social media: digital content is more persistent, visible to a larger audience, easily spreadable, and searchable (Boyd 2014: 11). Therefore, recruitment on the digital street has the benefit of reaching a large audience of potential money mules in comparison to social ties on the physical streets.

However, these initial digital interactions result in physical encounters, as the following example of a money mule from network 3 illustrates:

> On BlackBerry ping I was asked for my debit card. I know Ray, the person who asked me for the card, from primary school, but we haven't been in the same class. I handed him my card and my PIN code at the diner just around the corner. He promised me € 9,000, but I did not receive anything. I did not ask him why he needed the card. He just told he would put money on it, but I don't know where that money came from. He told me that I would get my card back a day later. But he told me that the machine had swallowed my card. He stills asks me for cards, but I haven't given him other cards. (Network 3)

In sum, these examples illustrate that some of the recruitment processes have been digitized, with potential mules being targeted both on the physical and digital streets. However, these cases also point to the ongoing importance of offline interactions and encounters. Therefore, interpreting these networks only as cybercriminal obfuscates the vital importance of both the physical and digital streets for the recruitment of (potential) money mules.

Contours of a street culture?

Examples of activities and individuals that navigate online and offline spaces can be seen in both the modus operandi and the origin and growth of the networks in this study. In addition to the youth gang in network 9, we see individuals in different cases engaged in different economic street crimes, like drug dealing, street robberies, and burglaries. Relationships between offenders originated offline, whilst potential money mules are targeted via both the physical and digital street. Instead of classifying these activities as cybercrime, these findings could also indicate that street-oriented individuals in the Netherlands have adapted to the rise of technology. In fact, nine cases (1, 2, 3, 4, 5, 8, 9, 10, 12) contain empirical evidence that supports this claim, in particular, because information on core members, recruiters, and money mules seems to indicate the contours of a street culture.

"Sappie": Dutch street vernacular

First, the information in the police files shows the strong presence of language that is embedded in Dutch street culture. For example, the police file on network 9 contains a transcript of a wiretapped conversation between offenders, in which one of them says: *"Hurry up, the 'sani' will go down."* "*Sani*", Dutch street slang that originated from the street culture of Suriname, can be roughly translated as "thing" or "activity" (Snijders 2000: 138). Moreover, various offenders in the cases make use of the word *"swipen,"* a word used among street-oriented individuals in the Netherlands to refer to phishing. In the case of network 8, we find an even more prominent example that indicates that offenders are embedded in street culture: several offenders make use of the word *"sappie."* In this case *"sap"* should be read as the reverse of the Dutch word for card (*"pas"*) (see also Roks and van den Broek 2017: 43). This practice of "talking backwards" (Lefkowitz 1989), inspired by the *verlan* spoken on the streets of the banlieues in France (Slooter 2015: 49), is increasingly used by youth embedded in street culture in the Netherlands.

Most notably is the use of reversed words in Dutch rap music (SMIB 2017). The origin of this musical genre can be located on the streets and in the public spaces of inner-city neighborhoods in the United States (Rose 1994). In network 8, we see an example of the intertwinement between street culture and rap music:

> During the police interrogation, one of the suspects says he is a rapper who has gained some notoriety through his music in a specific neighborhood in the Netherlands. Although he acknowledges his tough appearance, he claims this is only a persona he portrays to the outside world. However, because of this imagery, he was often approached by people for "sappie", street slang for phishing activities. (Network 8)

Furthermore, the case on network 2 also contains information that illustrates how rap music played a part in the origin and growth of the network. During an interrogation, one of the prime suspects states: *"I got in touch with these guys through (rap) music. I saw [namesuspect] in Amsterdam for the first time. Back then, they were already working with cards*."

The lure of easy money

In addition to language, the cases show how offenders are motivated by the lure of making easy money. Although it could be said that monetary gains motivate economic offenders in general, the cases we studied contain numerous examples that indicate the presence of a street culture that informs the motives and neutralizations of the offenders and the money mules. Hallsworth (2013: 152–153) argues that street culture can be located in the deprived areas of the urban environment where obtaining money is a precarious endeavor. Whilst the cases we studied do not contain detailed information about the personal backgrounds of the offenders, we do see various examples of vulnerable people, in particular, youth from disadvantaged neighborhoods, succumbing to the lure of easy money as advertised by recruiters on the physical and digital street. In fact, during police interrogation many money mules admit they were enticed by the prospect of making money in a rather easy manner (see for more detail Leukfeldt and Kleemans 2019). This search for money is seen as one of the core imperatives that informs street culture (Hallsworth 2013:144; Ilan 2015).

Moreover, some of the core members and recruiters presented a lifestyle that younger generations look up to, like one of the offenders in network 2 explains during an interrogation:

> Not a normal car, a fancy car. It was a dark car, it was lowered. Sometimes it would be a Mercedes and sometimes a BMW. The clothes the guy was wearing were Gucci and they also frequented a club. They were in the secured VIP-area, and we were in the crowd. The two of them were often together. They both had golden teeth. One of them was wearing a Moncler. That's an expensive coat, it had a beautiful collar on it. I've always wanted a jacket like that. (Network 2)

Our cases contain more examples of young people looking up to the lifestyle and especially the conspicuous consumption of core members or recruiters, which seduces them to "believe that success in life is to be obtained by owning the right thing" (Hallsworth 2013: 153).

In addition to the lure of easy money, our cases indicate that involvement in phishing activities could be seen as less problematic as opposed to other (economic) street crimes like street robberies or involvement in the drug trade. In fact, one of the core members in network 2 proclaims, after explaining the phishing procedure to a potential co-offender, that "*it isn't illegal.*" Moreover, because of the frequency with which youths are confronted with opportunities to commit this type of fraud, with some claiming that everyone on the streets knows about these activities, we see evidence of a degree of normality amongst the offenders in the cases we studied.

Conclusion and discussion

In this article, we analyzed the criminal activities of 14 cybercriminal networks, with a specific focus on the offline and local dimensions of their cybercriminal activities. Firstly, we examined whether the networks in the 14 cases are also involved in criminal activities other than cybercrime. Our findings show that the offenders in the networks commit a wide array of both digital and more traditional (street) crimes. Rather than specializing in cybercrimes, eight of the 14 cases contain information that offenders engage in versatile, "cafeteria style offending" (Klein 1995: 132) both online and offline. Although our data does not permit quantitative statements, it is striking that quite a few networks are engaged in both traditional and cybercriminal activities. Moreover, the networks that seem to limit their activities to online crimes are not specialized and commit various cybercriminal offenses. Furthermore, based on the empirical data we studied, we cannot be sure that these networks only engage in cybercrime. Police investigations tend to focus on particular crimes, leaving the possibility open that these networks are involved in additional (offline) crimes. Conversely, our empirical material shows that a number of networks engage in both online and offline crime. Future research, therefore, should be directed at gaining more insight into the intersection(s) between (economic) street crimes and cybercrimes.

Secondly, we zoomed in on the origin and growth of the criminal networks, with specific attention to the role of offline social ties and interactions. In most cases, the origin and

development of the cybercriminal networks seem to follow the laws of both geographical and social proximity (Kleemans and van de Bunt 1999), with social ties between offenders originating (on the streets) of local neighborhoods or from previously shared criminal endeavors. Despite the existence of crypto markets on the dark web, where offenders can buy phishing services, plug-and-play malware, and money mule networks (see, for an overview, Leukfeldt 2017), our results find most core members of the criminal networks falling back on their offline social capital to establish relationships with other offenders. Although these findings mirror previous research on the origin of organized crime networks (Kleemans and de Poot 2008), the cases we studied seem to differ in some important respects. Our research illustrates that the Internet seems to provide a new and additional opportunity structure to recruit co-offenders, especially facilitators and money mules. Previous research has suggested that this can be done by hiring specialists for phishing activities through online contacts, for example, via the dark web, but also offline, in the offenders' immediate social environment (Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c). Our findings indicate that money mules are being targeted on both the physical and digital streets of the Netherlands and that only a few networks seem to be recruiting exclusively via offline social contacts. These results illustrate the ways (street) offenders adapt to the rise of technology, using their networked publics (Boyd 2014) to reach a larger audience of (potential) co-offenders and money mules.

Our analysis of both the criminal activities and the origin and development of the cybercriminal networks highlights the ongoing importance of the offline world. However, our results shed light on more than just the "hidden face of cybercrime" (Lusthaus and Varese 2017). Therefore, we also examined whether the 14 cybercriminal cases contained information that would indicate the presence of a street culture that informs the activities of the offenders. Based on their linguistic practices and motives and neutralizations, we see examples of how core members, recruiters, and money mules in different cases are embedded in Dutch street culture. According to Ross (2018: 11), street culture could be seen as both a cause and an effect of street crimes. Although our empirical data does not permit any causal statements of that nature, the contours of Dutch street culture in these cases on cybercriminal networks further questions the ";cyber"-label of these criminal activities and networks. In fact, based on our key findings, these cases could also be characterized as digital diversifications of traditional (economic) street crimes. These digital street crimes could, therefore, be seen as empirical examples of street offenders adapting to the rise of technology.

Despite the unique nature of the police investigations we studied, this research has several limitations. Firstly, although we could draw on rich data on criminal networks based on wiretaps, interrogations, and observations, the police files only provide information on networks and activities that are known to law enforcement agencies. Therefore, it is possible that this police focus contributes to a distorted picture of reality. Criminal networks outside of the scope of Dutch law enforcement agencies might have a different network structure and could be making use of online opportunities in a different manner. Furthermore, the number of cases we studied was limited to 14 criminal investigations. In addition, our selection was limited to cybercriminal networks that carried out phishing and malware attacks. Finally, we only studied networks that were active in the Netherlands. Future research should, therefore, also include criminal networks and activities that fall outside of the scope of this study. However, despite these limitations, our study illustrates criminal activities on the intersection between cybercrime and traditional street crime. Thus, moving forward it is necessary for researchers to study both the offline and online dimensions of street crimes. Notwithstanding this relevant insight, several theoretical and empirical questions remain and will arise as scholars focus their attention on the ways technology impacts the lives of street-oriented (young) people. Our digital era calls for research methodologies that are able to grasp the realities of street culture and street crimes not just on the physical or digital streets, but simultaneously on the ground, in the feeds, and in the networks (Lane 2019: 169–187).

Notes on contributors

Dr. E.R. (Rutger) Leukfeldt is senior researcher and cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Furthermore, Rutger is director of the Cybersecurity Research Group of the Hague University of Applied Sciences. Over the last decade, Rutger worked on a number of cybercrime studies for the Dutch government and private companies. Examples include studies into the modus operandi and characteristics of cybercriminals, a nation-wide cybercrime victim survey and a study into the organization of Dutch law enforcement agencies responsible for the fight against cybercrime. His PhD-thesis was about the origin and growth processes of cybercriminal networks. In 2015, Rutger received a Marie Curie Individual Fellowship (EU grant for promising researchers) to study the changing organization of organized crime due to the use of Information Technology. In 2017, Rutger received a Veni grant (Dutch grant for highly promising researchers) to carry out a study into the online and offline pathways into cybercriminal networks. Rutger is currently the chair of the Cybercrime Working Group of the European Society of Criminology (ESC) and member of the International Interdisciplinary Research Consortium on Cybercrime (IIRCC).

Dr. R.A. (Robert) Roks is assistant professor of Criminology at the Erasmus University of Rotterdam. He completed his doctorate at the Erasmus University of Rotterdam in March 2016. His PhD-thesis focused on the embeddedness of crime and identity. For this ethnographic study, he conducted three years of fieldwork (2011-2013) among members of the Rollin 200 Crips, a Dutch 'gang' that originated in the city of The Hague, the Netherlands in the late 1980s. After his PhD, he was involved as a researcher for the fifth sweep of the Dutch Organized Crime Monitor (DOCM). His research interests include street culture, street gangs, outlaw motorcycle gangs, and organized crime, with a preference for qualitative research methods and exploring alternative ways of collecting data (social media, digital communication, and (rap) music). Robby is a board member of the Centre for Information and Research on Organized Crime (CIROC) and on the editorial board of two Dutch scientific journals.

References

Anderson, Elijah. 1999. *Code of the Street. Decency, Violence, and the Moral Life of the Inner City*. New York: Norton.
Bourgois, Philippe. 1995. *In Search of Respect: Selling Crack in El Barrio*. Cambridge: Cambridge University Press.
Boyd, Danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.
de Jong, Jan Dirk. 2007. *Kapot Moeilijk: Een Etnografisch Onderzoek Naar Opvallend Delinquent Groepsgedrag Van 'Marokkaanse' Jongens*. Amsterdam: Aksant.
Decker, Scott H. and David C. Pyrooz. 2013. "Gangs: Another Form of Organized Crime?" Pp. 270–87 in *Oxford Handbook of Organized Crime*, edited by Letizia Paoli. New York: Oxford University Press,
Densley, James A. 2013. *How Gangs Work. An Ethnography of Youth Violence*. New York, NY: Palgrave Macmillan.
Hallsworth, Simon. 2013. *The Gang and Beyond: Interpreting Violent Street Worlds*. Basingstoke: Palgrave Macmillan.
Holt, Thomas J. and Adam M. Bossler. 2014. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35 (1):20–40.
Ilan, Jonathan. 2015. *Understanding Street Culture. Poverty, Crime, Youth and Cool*. London: Palgrave MacMillan.
Irwin-Rogers, Keir, James Densley, and Craig Pinkney. 2018. "Gang Violence and Social Media." Pp. 400–10 in *The Routledge International Handbook of Human Aggression*, edited by J.L. Ireland, P. Birch, and C.A. Ireland. London: Routledge
Kleemans, Edward R. and Christianne J. de Poot. 2008. "Criminal Careers in Organized Crime and Social Opportunity Structure." *European Journal of Criminology* 5 (1):69–98.
Kleemans, Edward R. and Henk G. van de Bunt. 1999. "The Social Embeddedness of Organized Crime." *Transnational Organized Crime* 5 (1):19–36.
Klein, Malcolm. 1995. *The American Street Gang*. New York: Oxford University Press.
Kruisbergen, Edwin W., E. Rutger Leukfeldt, Edward R. Kleemans, and Robby A. Roks. 2018. *Georganiseerde Criminaliteit En ICT. Rapportage in Het Kader Van De Vijfde Ronde Van De Monitor Georganiseerde Criminaliteit*. Den Haag: WODC.
Lane, Jeffrey. 2015. "The Digital Street: An Ethnographic Study of Networked Street Life in Harlem." *American Behavioral Scientist* 60 (1):43–58.
Lane, Jeffrey. 2019. *The Digital Street*. New York: Oxford University Press.
Lastdrager, Elmer E. 2014. "Achieving A Consensual Definition of Phishing Based on A Systematic Review of the Literature." *Crime Science* 3 (1):9.
Lauger, Timothy R. and James A. Densley. 2018. "Broadcasting Badness: Violence, Identity, and Performance in the Online Gang Rap Scene." *Justice Quarterly* 35 (5):816–41.
Lefkowitz, Natalie J. 1989. "Verlan: Talking Backwards in French." *The French Review* 63 (2):312–22.
Leukfeldt, E. Rutger. 2014. "Cybercrime and Social Ties." *Trends in Organized Crime* 17 (4):231–49.

Leukfeldt, E. Rutger., ed. 2017. *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven International Publishers.
Leukfeldt, E. Rutger and Edward R. Kleemans. 2019. "Cybercrime, Money Mules and Situational Crime Prevention." Pp. 75–89, in *Criminal Networks and Law Enforcement: Global Perspectives on Illicit Enterprise*, edited by S. Hufnagel and A. Moiseienko. London: Routledge.
Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017a. "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.
Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017b. "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.
Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017c. "Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis." *Crime, Law and Social Change*. doi:10.1007/s10611-016-9647-1.
Leukfeldt, E.R. 2016. Cybercriminal networks: Origin, growth and criminal capabilities. (Doctorate thesis) The Hague: Eleven International Publishers.
Lusthaus, Jonathan. 2018. *Industry of Anonymity. Inside the Business of Cybercrime*. Cambridge: Harvard University Press.
Lusthaus, Jonathan and Federico Varese. 2017. "Offline and Local: The Hidden Face of Cybercrime." *Policing: A Journal of Policy and Practice*. doi:10.1093/police/pax042.
Moule, Richard K., David C. Pyrooz, and Scott H. Decker. 2014. "Internet Adoption and Online Behaviour among American Street Gangs: Integrating Gangs and Organizational Theory." *British Journal of Criminology* 54 (6):1186–206.
Moyle, Leah, Andrew Childs, Ross Coomber, and Monica J. Barratt. 2019. "#drugsforsale: An Exploration of the Use of Social Media and Encrypted Messaging Apps to Supply and Access Drugs." *International Journal of Drug Policy* 63 (1):101–10.
Patton, Desmond U., David Pyrooz, Scott Decker, William R. Frey, and Patrick Leonard. 2019. "When Twitter Fingers Turn to Trigger Fingers: A Qualitative Study of Social Media-Related Gang Violence." *International Journal of Bullying Prevention*. Advance online publication. doi:10.1007/s42380-019-00014-w
Peterson, Jillian and James Densley. 2017. "Cyber Violence: What Do We Know and Where Do We Go from Here?" *Aggression and Violent Behavior* 34 (1):193–200.
Pyrooz, David C., Scott Decker, and Richard K. Moule. 2015. "Criminal and Routine Activities in Online Settings." *Justice Quarterly* 32 (3):471–99.
Roks, Robby A. 2016. *In De H200d. Een Eigentijdse Etnografie over De Inbedding Van Criminaliteit En Identiteit*. PhD dissertation, Department of Criminology, Erasmus University, Rotterdam.
Roks, Robby A. and Jeroen B.A. van den Broek. 2017. "#HOUHETSTRAAT: Straatcultuur Op Social Media?" *Tijdschrift over Cultuur En Criminaliteit* 7 (3):31–50.
Rose, Tricia. 1994. *Black Noise: Rap Music and Black Culture in Contemporary America*. Hanover, NH: Wesleyan University Press.
Ross, Jeffrey I. 2018. "Reframing Urban Street Culture: Towards a Dynamic and Heuristic Process Model." *City, Culture and Society* 15 (1):7–13.
Sandberg, Sveinung and Willy Pedersen. 2011. *Street Capital: Black Cannabis Dealers in a White Welfare State*. Bristol: Policy Press.
Slooter, Luuk A. 2015. *The Making of the Banlieue: An Ethnography of Space, Identity and Violence*. PhD dissertation, Paris, EHESS.
SMIB. 2017. *Smibanese Woordenboek*. Amsterdam: Smibanese University.
Snijders, Ronald. 2000. *Surinaams Van De Straat*. Amsterdam: Prometheus.
Storrod, Michelle L. and James A. Densley. 2017. "'Going Viral' and 'Going Country': The Expressive and Instrumental Activities of Street Gangs on Social Media." *Journal of Youth Studies* 20 (6):677–96.
Stuart, Forrest. 2019. "Code of the Tweet: Urban Gang Violence in the Social Media Age." *Social Problems*. Advance online publication. doi:10.1093/socpro/spz010
Urbanik, Marta-Marika and Kevin D. Haggerty. 2018. "'#it's Dangerous': The Online World of Drug Dealers, Rappers and the Street Code." *The British Journal of Criminology* 58 (6):1343–60.
van Hellemont, Elke. 2012. "Gangland Online. Performing the Real Imaginary World of Gangstas and Ghettos in Brussels." *European Journal of Crime, Criminal Law and Criminal Justice* 20 (2):165–80.
van Hellemont, Elke. 2015. "The Gang Game: The Myth and Seduction of Gangs." PhD dissertation, Koninklijke Universiteit van Leuven, Leuven.