THE HYBRIDIZATION OF STREET OFFENDING IN THE NETHERLANDS

Robert A. Roks, E. Rutger Leukfeldt and James A. Densley*

Based on the results of two research projects from the Netherlands, this paper explores how street-oriented persons adapt and use digital technologies by focussing on the changing commission of instrumental, economically motivated, street crime. Our findings show how social media are used by street offenders to facilitate or improve parts of the crime script of already existing criminal activities but also how street offenders are engaging in criminal activities not typically associated with the street, like phishing and fraud. Taken together, this paper documents how technology has permeated street life and contributed to the ‘hybridization’ of street offending in the Netherlands—i.e. offending that takes place in person and online, often at the same time.

Key Words: opportunity structure, street culture, street crime, gangs, cybercrime

Introduction

For street offenders, technology has the potential to provide ‘new, and different opportunities for dangerous, deviant, and criminal behaviour’ (Moule et al. 2013: 1419). In 1995, Natarajan et al. (1995: 141) explored the then relatively new phenomenon of mobile phones in drug dealing, concluding that the role of telephone communication, either via (cloned) mobile phones, beepers or pagers, is ‘barely mentioned in ethnographic research’. A few years later, at the turn of the century, Anderson (1999: 30) noticed how ‘the beeper and telephones have become more important’ as a consequence of law enforcement pressure ‘on local crack houses and open-air street sales’ forcing drug dealing into private spaces. Nowadays, mobile telephones come equipped with internet access, different applications and, in some cases, advanced encryption, all of which has the potential to benefit street offenders in their criminal endeavours. Therefore, Pyrooz et al. (2015: 473) argue that ‘it is important to understand how offenders adapt and use rising powerful digital technologies, and whether this parallels or diverges from street offending’.

Different studies to date have examined the integration of the internet and social media into street gang life (for a review, see Pyrooz and Moule 2019), finding that for street-oriented persons like gang members, activity in physical space and in virtual space are increasing intertwined, creating what Lane (2019) has called, ‘the digital street’. Gang membership is strongly associated with criminal offending (Pyrooz et al. 2016), but the extent to which the digital street influences street offending patterns

*Robert A. Roks, Department of Criminology, Erasmus School of Law, Erasmus University Rotterdam, Burgemeester Oudlaan 50, 3000 DR Rotterdam, The Netherlands; roks@law.eur.nl; E. Rutger Leukfeldt, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, The Netherlands; The Hague University of Applied Sciences, The Hague, The Netherlands; James A. Densley, School of Law Enforcement and Criminal Justice, Metropolitan State University, Saint Paul, MN, USA

© The Author(s) 2020. Published by Oxford University Press on behalf of the Centre for Crime and Justice Studies (ISTD). This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs licence (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial reproduction and distribution of the work, in any medium, provided the original work is not altered or transformed in any way, and that the work is properly cited. For commercial re-use, please contact journals.permissions@oup.com
remains an open question. Based on the results of two different research projects from the Netherlands (Leukfeldt 2016; Roks 2016), this paper explores how street-oriented persons adapt and use rising powerful digital technologies by focussing on the changing commission of instrumental, economically motivated, street crime. Specifically, instead of illustrating the current (digitized) street economy in the Netherlands, we focus on the ways technological developments since the early 2010s contribute to the ‘hybridization’ of street offending in the Netherlands—that is, offending that takes place in person and online, often at the same time.

The current study combines traditional urban ethnography with detailed analyses of digital artefacts, and in an effort to further bridge the physical and virtual divide, we integrate research on gangs and street crime with research on cybercrime. The paper advances the concept of hybridization to make sense of the ways in which criminal opportunity and circumstantial opportunity come together in the modern world, and how circumstantial opportunities rely on a certain hybridity between virtual and actual spaces. Our examination of the changing nature of street crime begins with insights from studies on street culture that indicate street offenders use technology not just for expressive means, but also instrumental purposes like money making. It continues with an exploration of related research on cybercrime. Next, we introduce our hybrid dataset produced from two mixed-methods studies. Findings indicate that for street offending today, both the digital street and the physical street play a pivotal role and offer new illegitimate opportunities: the hybrid nature of contemporary street crime spans both online and offline worlds. The discussion puts these findings in context and formulates several questions for future research.

Street crime and criminal opportunity in a digital world

Simon Hallsworth (2013: 152) notes how street culture is mostly found ‘in areas characterized by high indices of deprivation where local labour markets provide little by way of secure employment where the jobs on offer are of the precarious form’. In these circumstances, street-oriented individuals ‘seek to make money by mobilizing whatever entrepreneurial talent they possess in whatever activity will deliver it’ (Hallsworth 2013: 153). And, as Hallsworth (2013: 153) writes, ‘opportunities always exist’. The omnipresence of opportunities to make money on the street is illustrated by ethnographic accounts of street and gang cultures operating within local neighbourhoods in the United States (Sullivan 1989; Bourgois 1995; Wright and Decker 1997; Anderson 1999; Jacobs 1999; Venkatesh 2000) and in Europe (De Jong 2007; Sandberg and Pedersen 2011; Densley 2013; Harding 2014; McLean et al. 2019; McLean and Densley 2020; Van Hellemont 2015). These studies indicate that the street economy offers a plethora of criminal opportunities for motivated street offenders. Within these settings, scholars have identified a range of instrumental criminal activities, ranging from ‘amateur and playful’ crime, to professional, high risk, high reward, criminal transactions (Ilan 2015: 89).

A central theme in these studies is how community settings and characters shape illegitimate offending opportunities (Bursik and Grasmick 1993; Sampson et al. 1997). Sullivan (1989: 199) illustrates how (sections of) neighbourhoods function as ‘underground markets’ for illegal opportunities. However, 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’. The idea that crime results from variable access to illegitimate means and success-goals, or a differential opportunity structure, speaks to Cloward and Ohlin’s (1960) seminal work, *Delinquency and Opportunity*.

Cloward and Ohlin’s (1960) contribution to the study of gang culture lies in uncovering that when traditional and legitimate opportunity structures are blocked, people pursue success through structures that are considered non-traditional and illegitimate, like (gang) delinquency. From their viewpoint, this resolution depends upon the kind of social support for one or another type of illegitimate activity that is given at different points in the social structure (Cloward and Ohlin 1960: 151). Cloward and Ohlin (1960: 171) argued that criminal subcultures tended to manifest in neighbourhoods that featured a specific milieu characterized by ‘close bonds between different age-levels of offenders, and between criminal and conventional elements. As a consequence of these integrative relationships, a new opportunity structure emerges which provides alternative avenues to success-goals’.

In most of the abovementioned studies on street and gang cultures, offending is anchored in the ecology and economy of the street and physical spaces like the street corner are central to social life (for a review, see Valasik and Tita 2018); a tradition that dates back to the Chicago School (Park et al. 1925; Thrasher 1927; Shaw and McKay 1942; Whyte 1943). However, as Jeffrey Lane describes in *The Digital Street*, street life today is ‘decoupled from its geographic location to split along the physical and the digital street’ (Lane 2019: ix). In other words, everyday experiences of urban poverty—including the localized opportunities and risks associated with life ‘on road’ (Hallsworth and Silverstone 2009: 359)—are filtered through digital technology. Further studies document a digitization of the ‘street code’ (Anderson 1999), highlighting the changing dynamics of violent interactions in the digitized era, with an emphasis on the expressive performance of street culture, both in North America (Moule et al. 2013; 2014; Patton et al. 2017a; 2017b; 2019; Lauger and Densley 2018; Urbanik and Haggerty 2018; Lane 2019; Leverso and Hsiao 2020; Stuart 2020), and in Europe (Van Hellemont 2012, Densley 2013; Storrod and Densley 2017; Roks 2019).

Stuart (2020: 8) recently urged researchers to look beyond ‘quantitative disparities in access to technology’ in the analysis of urban poverty toward a focus on the qualitative differences in the uses and consequences of technology in part because recent data suggest that ‘poor black youth are more glued to their smartphones, tablets, and social media accounts than their more privileged peers’. Stuart’s (2020: 18) ethnography of drill rappers in Chicago found young black men coming of age in impoverished and violent neighbourhoods needing to adapt to now being ‘locked out of the underground job market once available for their fathers’. Instead of via the drug economy, they tried to generate income in the online attention economy because ‘micro-celebrity yields valuable resources for daily survival’ and could mean the difference ‘between going hungry and securing a hot meal’ (Stuart 2020: 9). By capitalizing on violent performances, often rooted or inspired by first-hand experiences growing up in poverty-stricken and gang-ridden neighbourhoods, in drill music and videos and accompanying content on social media, drill rappers used their tech-savviness to generate likes, views and streams and, eventually, make money (Stuart 2020).
Pyrooz et al. observed that, although the internet has reached the urban poor, ‘access alone is not translating into sophisticated technological know-how’ (Pyrooz et al. 2015: 472) and, for gangs especially, the internet was exploited ‘to further their collective identity rather than for instrumental means’ (Pyrooz et al. 2015: 493). Building on the instrumental/expressive dichotomy in gang research (Decker and Pyrooz 2013), Storrod and Densley (2017) found a convergence of expressive and instrumental online behaviours, illustrating that expressive activities like posting a rap video could help gangs achieve instrumental goals like selling drugs because the video positioned the gang in the marketplace as credible suppliers of illicit goods and services. Whittaker et al. (2020: 6–7) also found that there were ‘differential adaptations’ to social media among gangs, including gangs that occupied the same geographic spaces. The authors attributed this to a ‘generation gap’—newer gangs and younger gang members, especially those with tenuous ‘street capital’ (Harding 2014), who had more to gain and less to lose from expressive internet use, versus more durable gangs and more senior gang members, who had street capital in the bank and worried over-exposure on social media would jeopardize their instrumental criminal activities.

Still, there is emerging evidence that the internet is affording traditional street offenders like gang members with new opportunities to expand their criminal repertoire. An ethnography of gangs in London, England, found gang members using ‘basic stenography to hide information within image and audio files and applications that allow users to send private messages that, like Mission Impossible, literally self-destruct in seconds’ (Densley 2013: 99). The same study documented the exchange of illegal goods and services via PayPal and online auction sites and information pertinent to the street shared ‘via virtual gaming worlds, chat rooms, and synchronous conferencing protocols’ (Densley 2013: 99).

Another study of drug-selling gangs in Glasgow, Scotland, documents how ‘drug dealing via online apps and social media platforms has emerged as a highly lucrative new development’ (Densley et al. 2018: 118). First, for drug dealers, technology has facilitated the easy purchase of various drugs online, often in ‘small user-ready quantities’. Second, the internet made it possible to source drugs from ‘further afield than was possible in years past, but it also fed consumer demand for new illicit products’ (Densley et al. 2018: 118).

In general, recent studies point to a digitization of the drug economy (Bakken and Demant 2019). For instance, Søgaard (2019: 213) notes a transformation of retail-level drug distribution, resulting not just in a shift towards online cryptomarkets (Aldrigle and Décary-Hétu 2016) but also both drug users and sellers moving online to social media platforms like Facebook and Instagram and smartphone encryption apps like Wickr (Salinas 2018). In an 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 ‘Emojis’ ‘provide the gateway to access advertisements for sales of a range of substances: a diamond or snowflake for cocaine, a capsule for 3,4-methylenedioxymethylamphetamine (MDMA), and a needle for heroin’. The findings of Moyle et al. (2019: 108) indicate—in concordance with the findings of Densley et al. 2018—that apps and social media platforms are transforming and moving the drug economy online.

Surprisingly, however, the merging of offline and online situations is rarely reflected in cybercrime studies. For the past two decades, the burgeoning field of cybercrime
has vastly improved our knowledge and understanding of emerging crime trends and the influence of information technology (IT) on offenders and offending (Holt and Bossler 2020). Technological innovations have transformed or digitized existing crime types (‘cyber enabled crimes’) but have also fostered the emergence of new ‘cyber dependent’ crimes (McGuire and Dowling 2013). Gordon and Ford (2006: 15) suggest that cybercrime—an umbrella term referring to all types of crime in which IT plays a role—should be conceived as a continuum ‘ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people-related’.

Perhaps caused by the relative novelty of cybercrimes, a large body of cybercrime literature is conceptual rather than empirical, especially when it pertains to the overlap between offline and online offending (e.g. Peterson and Densley 2017; Lauger et al. 2020). Existing empirical studies tend to concentrate on the cyber aspect of the crime and limit their scope to the online world (on online cybercriminal meeting places see, e.g. Holt and Lampke 2009; Holt 2013; Hutchings and Holt 2015) or on the processes of gaining trust in an online criminal environment (Décary-Hétu and Dupont 2012; Holt et al. 2013; Lusthaus 2013; Dupont et al. 2016). However, research shows that even anonymous cybercrime has its roots in personal social networks (Lusthaus and Varese 2017). Cybercriminal activities could be distinguished between offenses where technology is both the instrument and the target and criminal activities in which IT is essential for the enactment of the offense but where technology is not the target. Therefore, on either side of the cybercrime continuum, we see criminal activities that are indicative of changing illegitimate opportunity structures.

The Current Study

Traditional research on street offending emphasizes the criminal opportunities associated with one’s immediate surroundings. Increasingly, research shows how gang members and street-oriented individuals adapt to opportunities provided by technology, albeit mostly in expressive ways for reputation building. Pyrooz et al. (2015: 493) predict more advanced manipulation of the internet once gang members ‘acquire the technological knowhow to exploit the instrumental opportunities available online’. Presently, less is understood about if and how street offenders use technology to make money (c.f. Storrod and Densley 2017) in part because research into instrumental crime in the digital age has become the purview of the field of cybercrime.

The extant literature indicates that technology is now integral to the lives of street-oriented individuals. To capture this reality, Lane (2015: 46) bridged urban ethnography with digital research approaches, concluding that ‘each have particular commitments in their respective fields that when combined can be mutually beneficial’. The current study follows this thinking, drawing to different data sources to bridge between the study of (economic) street crimes and cybercrime. It is driven by the question to what extent has technology changed the illegitimate opportunity structure of the street? We find that street offenders do not simply adapt to digital technologies, but rather a digitally mediated street life has changed the opportunity structure for street crime. There is a certain hybridity between virtual and actual spaces that has contributed to the hybridization of street offending in the Netherlands.
Method

The current research illustrates the hybridization of street offending by drawing on empirical data from two mixed-methods studies conducted in the Netherlands (Leukfeldt 2016; Roks 2016). The first (Study A) was a three-year ethnographic study of a small neighbourhood in The Hague that has housed the Dutch Crips gang since the late 1980s (for details, see Roks 2019). Ethical approval for this study was granted by the first author’s home institution and, for a detailed discussion of the ethics of researching people in person and online at the same time, see Urbanik et al. (2020). Between January 2011 and December 2013, the first author built a network of 150 informants consisting of (former) members of the Crips, community residents, young people hanging in and around the neighbourhood and a local Youth Centre, social workers and local police officials. Interviews, informal conversations and observations resulted in in-depth information about the lives and/or criminal careers of 60 research subjects. Additionally, the first author analysed the activities on public social media accounts on Facebook, Twitter and Instagram of 40 street-oriented young people he met and spoke to offline (for details, see Urbanik and Roks 2020). Data from these 40 individuals forms the base of the research in this article.

For the second study (Study B), the second author examined cybercriminal networks using data collected from 2013 to 2015 (Leukfeldt 2016; Leukfeldt et al. 2017a; 2017b; 2017c). After a formal request to the Dutch Public Prosecution Office, permission was granted to study criminal investigations into cybercriminal activities in the Netherlands. In the absence of a central registration, a snowball method led to selecting 18 cases on criminal networks involved in phishing and the use of banking malware in the Netherlands in the period 2004–14. Police investigation files generally contain a wealth of information because of the use of special investigative powers, such as wiretaps, network taps, interrogations and analysis of seized computers. Because of this wealth of information, some case files were thousands of pages long.

The analytical framework of the Dutch Organised Crime Monitor, employed by Dutch researchers for over three decades, was used to systematize the analytical process (see, e.g. Kleemans et al. 1998; 2002; Kleemans and De Poot 2008; Kruisbergen et al. 2012; 2018; 2019; Leukfeldt et al. 2019). The framework includes questions about the ties between members of the criminal group (e.g. composition, structure and hierarchy), processes of origin and growth (i.e. how, when and where the network started and how new members were recruited) and the network’s use of offline and online offender convergence settings. In addition to analysing police data, the second author interviewed police team leaders and senior detectives, including financial and digital experts, to gain insight into matters not covered in the police files (for details, see Leukfeldt 2016).

Although Studies A and B were not related, they took place in the same social and geographical context and the empirical findings in both studies overlap to provide a unique and complementary insight into the ongoing digitization of street offending. To facilitate the synthesis of the findings on the digitization of street offending, the first and second authors used a method of comparative analysis inspired by the ethnographic revisit described by Van Hellemont and Densley (2019). To that end, the first and second authors first independently selected raw materials from their respective studies that illustrated the use of technology by street-oriented individuals. For Study A, this meant over 50 social media posts and a dozen pages of excerpts from field notes.
For Study B, 30 pages of raw material from 18 cases were used. Using a secured digital workspace, the first and second authors exchanged the anonymized empirical data. After familiarization with the data, initial semantic coding was completed across the data set, focussed on what was explicitly said and/or what was written. After coding both their own and each other’s raw data using the initial thematic codes ‘criminal opportunities’, ‘use of technology’ and ‘online and offline crimes’, both researchers compared and discussed their initial coding. After reflecting and realigning their interpretation and use of the codes, the authors completed their analysis of the material, identifying latent themes—the underlying ideas and assumptions that shape and inform the semantic content of the data—and exploring the relationship between them. These themes were then reviewed by the research team to ensure consistency within each theme and across the whole data set (Braun and Clarke 2006).

Findings

Notwithstanding the important differences between the two original research studies—in terms of research questions, theoretical framework and methodological approach—and the evident limitations of our pragmatic comparison and analysis, both studies document a similar phenomenon, albeit from a different perspective: the hybridization of street offending in the Netherlands. The findings demonstrate how (digital) technology has affected the nature of street offending in the Netherlands by creating and expanding opportunities for crime.

In this section, we will document the hybridization of street offending in the Netherlands. Before illustrating the process of street crime going digital, we will begin by focussing on analogue street crime in a digital world. Next, we elaborate on the hybridization of street crimes by zooming in on the digitization of parts of both online and offline crimes. In building our argument, we will shift between the two empirical studies.

Analogue street crime in a digital world

During Study A, the majority of the older informants seemed to be engaged only in offline crimes. This was especially true for the members of the Dutch Rollin 200 Crips. Starting as a breakdance crew in the early 1980s, this group evolved from a youth group to a street gang in the 2000s (Roks and Densley 2020). At the start of the fieldwork of the first author in 2011, the Rollin 200 Crips consisted of 50 members, predominantly from Surinamese and Antillean descent. Some members had been part of the gang since the 1980s, whereas, over the years, new and younger members joined the gang, resulting in a mixture of adolescent youngsters and OGs (original gangsters). The group engaged in serious criminality, including violence and drug trafficking (marijuana and powder cocaine), and several members were incarcerated during the fieldwork for their role in stabbings, assaulting police officers, weapons charges and possession of illegal narcotics.

Most of the Crips would limit the use of their mobile phones to playing music (videos) and communicating with other gang members, mirroring the sentiment documented by Whittaker et al. (2020: 2) that openly using social media would
attract unwanted attention by law enforcement agencies. For youth growing up in ‘the h200d’, a reference to the local neighbourhood made popular by members of the Rollin 200 Crips (Roks 2019), older Crips members functioned as role models, but the mere presence of street-oriented elders in the local neighbourhood also provided youngsters with opportunities to make money. Older members would ask local youth for assistance not only on innocent tasks like buying groceries but also criminal endeavours like obtaining information about crime, brokering contacts between social networks, changing counterfeit currency or selling narcotics and counterfeit cigarettes.

Vice versa, local youth would approach members of the Crips to inquire about criminal opportunities. One day, the first author was hanging out with Rick, an older member of the Crips, on a small square behind the local Youth Centre. Vernon, an adolescent youngster who resided in the neighbourhood, passed by on a bicycle. Rick signalled Vernon to come over, resulting in the following interaction:

Vernon: Fafi [What’s up in Surinamese] Rick, do you have work?
Rick: No, it’s quiet, not much to do, only a few burglaries. Do you know how to break in?
Vernon: No Rick, I’m more into the click clack beng haha.
Rick (laughing): You better chill, or else you get a long sentence. If you come strapped, they give you six to seven. But Vernon, if I know about work or something, I will let you know (Excerpt from fieldwork notes, 9 July 2012).

Most of the informants of Study A would use similar depictions of ‘crime-as-work’ (Letkemann 1973; Sullivan 1989) for the ways they would make money on the street. Gang leader Raymond would even refer to the locality of ‘the h200d’ as his ‘office’ where he would meet criminal contacts from inside and outside the neighbourhood and discuss ongoing and future criminal activities, exemplifying what Felson (2006) described as an ‘offender convergence setting’. Days after the abovementioned interaction, Vernon and his friend Railey came up to Rick to disclose that the permanently closed blinds and the penetrating odour of weed coming from a house led them to conclude that there might be an active weed plantation in a nearby neighbourhood. Rick urged the youngster to further look into the matter to see if they could break in and take the crops.

When street crime goes digital

In Study A, youngsters from the local neighbourhood—like Vernon and Railey—were more active online than most members of the Crips. The first author became aware of this during his initial visits to the local youth centre that was frequented a couple times a week by a group of 50 young people aged between 12 and 20. Early in the fieldwork, it became apparent how much time the youth spent online, visiting social networking sites, such as Hyves (a formerly popular Dutch social media platform), Facebook and Twitter, on their personal smartphones or on the Youth Centre’s computers. The first author located most of the regular visitors of the Youth Centre on the internet. Through studying their open, public social media profiles, significant insights were garnered about how the youth chose to portray their day-to-day whereabouts and happenings, school and leisure activities (Urbanik and Roks 2020). They also posted images
of themselves with what appeared to be various firearms and large sums of money in attempts to bolster their street credibility.

By being present in the Youth Centre, the first author was able to triangulate these online images and profiles with information about the youngsters’ involvement in street robberies, burglaries and thefts of bicycles and scooters—classic street crime. A youth worker then disclosed that the youth were talking more and more about looking for ATM cards to progress into more elaborate cybercrimes. Later, during informal conversations on the streets, the topic of ATM card fraud came up. In late August 2011, the first author was talking to Simon—a local youngster who would frequent the Youth Centre—about his aspirations to put in work for the Crips, specifically by selling weed on the streets. Simon had had some run-ins with police and quickly summarized his criminal resume: ‘yeah, for threatening someone, for carrying a weapon and for the fraud shit’.

In August 2013, 18-year-old Reynaldo, one of the younger members of the Rollin 200 Crips, explained how ‘the fraud shit’ worked. Reynaldo was hanging out with Önder, someone who grew up in the neighbourhood and could be classified as a peripheral member of the Crips. The first author overheard them talking about ‘spa’ and ‘nip’. These words are examples of the practice of ‘talking backwards’ (Lefkowitz 1989) and can be traced to the verlan spoken on the streets of the banlieues in France (Slooter 2015: 49). ‘Spa’ or ‘sap(pie)’ refer to the Dutch word for ATM card (‘pas’), whereas ‘nip’ or ‘nippen’ are derived from the Dutch word ‘pinnen’, meaning to withdraw money from the bank. As Reynaldo and Önder were discussing their experiences with this type of crime, the first author decided to ask ‘how the “spa” thing works’:

Reynaldo says that he is not involved in these scams, but he is also quick to mention that he made over 2500 euros with Emile, so he knows how it works. Önder chimes in to say that he was presented with an opportunity to make some easy money, but that it is not something he engages in normally. Reynaldo starts explaining, noting that you need to bring your ATM card and that money will be transferred to your account. He says that Emile has different women working for him, or for his nephew, but Reynaldo is not quite sure. These women try to get access to back accounts by calling people, asking for codes to access bank accounts. Then, according to Reynaldo, money is transferred to different accounts and withdrawn. However, Reynaldo claims that you should not use your own ATM card or bank account, because this might result in a ban from that specific bank for several years. Önder says: ‘well, but you can still open an account at other banks’. (Excerpt from fieldwork notes, 14 August 2013)

This excerpt illustrates how street-oriented individuals had created a hybrid of street crime and cybercrime to make money.

Study B provides a more detailed insight in the process of phishing described by Reynaldo. Analysis of the modus operandi of phishing across 14 criminal networks showed that ATM cards were used for cash withdrawals after other criminal actors had successfully transferred money from bank accounts either by posing as a trusted authority on the phone—like the example mentioned by Reynaldo—or using digital means like emails purporting to be from the bank to induce individuals to reveal personal information, such as passwords and credit card numbers. In some cases, such emails directed the victim to log on to a fake banking website that was made to look real. Control of online bank accounts was also taken in more sophisticated ways by using malware to intercept credentials and manipulate entire online banking sessions.
The hybridization of street offending in the Netherlands

In our respective studies, the clearest examples of the hybridization of street offending in the Netherlands can be found in Study B on cybercriminal networks. The starting point of all 14 networks in this study were financially motivated online crimes: the main suspects in the police files used phishing attacks and malicious software (malware) to target victims, access their online bank accounts and steal their money. However, a more thorough analysis of these cases shows that the offenders in these networks were not exclusively cybercriminals. For example, the police file on Network 3, focussed primarily on the phishing activities of six main subjects and 16 so-called ‘money mules’ (i.e. someone who moves illegally acquired funds at the direction of another person), showed offenders engaged in crimes beyond phishing. During a police interrogation, one of the money mules declared that she was asked by one of the main subjects to partake in changing counterfeit 100 Euro bills by buying cheap goods at different locations and collecting the change as ‘laundered’ cash. The police also found various narcotics during a raid on the houses of two of the main subjects: in total almost 5 g of cocaine and over 1,250 MDMA pills.

Similarly, in the police documentation on Network 9 we see how offenders engage in both online and offline crimes. In fact, the police investigation commenced with a focus on the offline crimes of the subjects in Network 9, who were classified by Dutch law enforcement agencies as a youth gang. According to local police, members of Network 9 were responsible for not only residential and commercial burglaries but also street robberies, fencing and drug dealing. During the investigation into these street crimes, the police gradually noticed that different subjects were also active as money mules or recruiting money mules. Regarding the latter, the suspects in Network 9 mostly targeted vulnerable youngsters from disadvantaged neighbourhoods by luring them with the prospect of earning easy money. We see a similar dynamic in the police files on Network 12:

My nephew [the main subject in Network 12] came up to me with a nice offer. I could make money. Enough money anyway. If I started a company for him, I could make money. He would not explain to me why. Also, I had to take out phone plans and give the phones to him. He would then sell the phones and put the money in the company’s account. (Network 12)

Network 12 was primarily involved in phishing, posing as a legitimate institution to lure individuals into providing sensitive data, such as personally identifiable information, banking and credit card details and passwords. However, police records show the gang also targeted vulnerable individuals, like drug addicts and people who were in debt, on the street. They took out mobile phone plans so that the gang could sell any phone bundled with the plans. Therefore, although the cases in the second study were all labelled as cybercrimes by the Dutch police, we see that 8 of the 14 cases contain information about offenders engaging in crimes both online and on the street.

In addition to both studies shedding light on street offenders in the Netherlands engaging in both online and offline crimes, we can make out another way that technology has permeated street life: internet and social media in particular are used by street offenders to facilitate or improve parts of the crime script of already existing criminal activities. Moreover, this is the case for both the online and offline crimes discussed in the previous sections. Some of the members of the Crips in the first study...
were selling various narcotics on the streets and occasionally also counterfeit cigarettes that they would sell below market prices. Instead of selling the knockoff cigarettes in bulk, younger members of the Crips would roam the streets of The Hague and frequent bars and clubs to sell the counterfeit cigarettes, often combined with weed or cocaine. However, some would also make use of technology to sell their products as indicated by the following message sent by gang member Tyrell:

Lil 200 M † NHC 20X10 Gang:
If yall need some green Holla @ me main eastside Up!! Bitch nigga Down
Lil 200 M † NHC 20X10 Gang:
I have tabaka 3 euros Holla @ me main
Lil 200 M † NHC 20X10 Gang:
Green H and malboro 35 euro for carton 3.50 for pack So Holla’
(Tyrell communication via Blackberry ping, 18 July 2012)

Using the broadcast functionality of the chat service BlackBerry Ping, Tyrell and several other younger gang members would inform their contact list about the prices of counterfeit ‘tabaka’, a word used in Dutch street slang to refer to cigarettes, and ‘green’ (marihuana). In the second study, we see a very similar example: one of the main suspects in Network 3 used broadcast on BlackBerry Ping to sell goods, as indicated by a money mule during an interrogation: ‘He [main suspect] sometimes sells BlackBerry phones. He sends a broadcast about BlackBerry’s for sale. I don’t know how he gets the BlackBerry’s though’.

The reach of BlackBerry Ping was limited to the known contacts that street offenders had stored in their phones. Similar messages sent via other social media platforms, like Facebook, however, had the potential to reach a larger audience because users could like, share or repurpose content. The younger informants in Study A would use social media in a similar way as the broadcasts on BlackBerry, amongst other things to advertise drugs (see Figure 1) but also other goods like the following post by Sylvester illustrates: ‘samsung galaxy s4 for sale new new 300.- send me a message’. (August 2013). In addition to phones, iPads (see Figure 2) and televisions were also sold on social media, with photographs of the products still in their original packaging. These messages would often include the Dutch hashtag #sneldenken, which translates to #thinkfast. More than a marketing strategy, this funhashtag, when used to sell new and old products, or in combination with below market prices, hinted at the use of social media to fence stolen property because the temporality of these online ‘deals’ saw posts disappearing from the informant’s timelines within hours.

The abovementioned examples illustrate how street-oriented individuals use digital technology to facilitate parts of the crime script of already existing criminal activities. By taking their business to social media platforms, informants were able to reach a larger audience, thus increasing their potential to make money. The case files in Study B further illustrate how potential money mules were recruited using the chat function on mobile phones with messages inquiring about people who were interested in making money or more specific questions like ‘What kind of card do you have?’ or asking about the colours ‘orange’ or ‘green’—a reference to the colours of the ATM cards from popular banks in the Netherlands. In these messages, money mules were promised large sums of money, sometimes 5,000 or 10,000 Euros or a 30 to 35 per cent cut of all profits if they handed over their ATM cards. The recruitment of money mules
Fig. 1. Advertising drugs on Instagram.
would also take place on social media as indicated by a money mule in the police documentation on Network 5:

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 referenced social media—in this case, Twitter—as a platform to approach potential mules. During Study A, the first author similarly came across messages on social media aimed at money mules, oftentimes in the form of cryptic messages like the following posts by Wesley, David and Emile:

‘Are you green or orange sappie’ (Wesley—February 2012).
‘Green 18+&Inta needed with copy of ID.. Lets make some money’ (David—February 2013).
‘Tomorrow lets #justjust make money. Just bring your spas everything will be alright xD’ (Emile—May 2013).

From 2012 onwards, the words ‘sap’ or ‘sappie’ and ‘nip’ were common parlance on social media and in Dutch street rap music, often accompanied by references to the colours ‘green’ or ‘orange’.

However, Study B indicates that the process of recruiting money mules did not solely play out on the ‘digital street’. For instance, police data showed that money mules were approached not only at school or at a gym by friends or acquaintances but also by strangers whilst hanging out on the streets in their local neighbourhoods. Only after being approached in person and contact information was exchanged were potential mules contacted through digital messenger services like Blackberry Ping or WhatsApp. The data thus indicate that, while part of gangs’ recruitment of money mules has gone digital, the process is still anchored in ties to the physical street. Offline interactions and encounters remain important even in a socially mediated crime environment (Leukfeldt 2014). Interpreting these networks only as cybercriminal runs the risk of overlooking the vital importance of both the online and the offline world for the recruitment of (potential) money mules.

Discussion

The current study used data from two studies—an ethnography of the Dutch Crips conducted online and offline and an analysis of cybercriminal networks known to police—to highlight the hybridization of street offending in the Netherlands. First, the data show a digital diversification of traditional (economic) street crimes. Street offenders used smart phones and social media to market stolen goods, sell drugs, recruit money mules and communicate with co-offenders, thereby utilizing digital tools and technologies to enhance traditional street crimes. Second, the data demonstrate how street offenders also were engaged in criminal activities not typically associated with the street like phishing and fraud, which suggests that street-oriented persons and groups were adapting to the new digital economy of crime. At the same time, cybercriminals, long assumed to be criminal specialists operating in spaces remote from the street, maintained ties to physical spaces and engaged in analogue crimes more typically associated with street criminals like drug selling and counterfeit money and goods. The findings suggest that the hybridization of street offending arises out of both digital connections and criminal opportunities that present themselves as a result of technological advancements.

Consistent with Pyrooz et al. (2015), therefore, we find that the internet is changing the ‘criminal and routine activities’ of street offenders, especially their instrumental activities, namely economically motivated street crime. Much like how, a few
decades ago, pagers and payphones opened new doors for drug dealers (Decker and Van Winkle 1996; Anderson 1999), the internet has become a venue for street offenders to expand their repertoire for making money illegally. Illegitimate opportunities are, in contrast to the classic work of Cloward and Ohlin (1960), no longer dependent exclusively on neighbourhood milieus or direct social surroundings; but, as Storrod and Densley (2017) also found, the neighbourhood still matters. Offline street networks and cultures remain crucial to understanding motivations, networks and operational tactics even for crimes that are committed through electronic means. Street culture is patterning the modes in which cybercrime is discussed and understood within the street milieu and, for this reason, notions of criminal opportunity going forward must account for where online situations create opportunity but also where a lack of ‘real world’ acquaintance might block it. As Lane (2019) argued, technology reconfigures face-to-face interactions and vice versa.

The methodology of the current study speaks to the ‘value of comparisons in street gang research’ (Klein 2005). By merging and reanalysing two unique data sets, the current study illustrated the ways street offenders adapt to the rise of technology using their networked publics (Boyd 2014) to reach larger audience of (potential) co-offenders and money mules. Although elements of the modus operandi of phishing might be characterized as more complex and technical, requiring specialized cybercriminals, the data show that aspects of this criminal activity are within the reach for street-oriented individuals otherwise lacking specialist skills. For cybercriminals, the findings show how opportunities may affect the structure of cybercriminal networks but that opportunities also have an impact on who becomes part of the network and, overall, the nature of the specific cybercriminal activities. The majority of the networks in the second case study still relied on real-world social ties and some fully utilized the digital advantages provided by technology.

This is a unique contribution to the literature because, in general, most studies on street crime discount online offending, and studies of cybercrime tend to focus on the role and function of technology, excluding the human factor in the commission of crime (Leukfeldt 2017). Our findings instead highlight a digital diversification of traditional economic street crimes. No mention was made of highly encrypted communication, artificial intelligence, algorithms, big data, etc., which suggests that street criminals are no experts in cybercrime. However, the data provide empirical examples of street offenders adapting to the rise of technology while keeping important offline interactions and encounters in focus. Therefore, interpreting groups and networks as either ‘street’ or ‘cyber’ criminals obfuscates the vital importance of both the physical and digital streets for the recruitment of offenders and their activities—this obviously has implications for law enforcement and other professionals engaged in crime prevention and intervention.

Owing to the hybridization of street offending documented here, researchers are encouraged to study both the offline and online dimensions of street crimes for they are intertwined. To address one of the limitations of the current retrospective approach, however, future studies should attempt to do this simultaneously, mixing street ethnography with analyses of official online network data. Several theoretical and empirical questions remain and will rise as scholars focus their attention on the ways technology impact the lives of street offenders. Future research, therefore, should be directed at gaining more insight into the intersection(s) of economically motivated street crimes
and cybercrimes and examining how the internet shapes both street and cybercrime alike. The results should yield important implications for crime prevention and intervention in the digital age.

Funding

This work was partly supported by the Netherlands Organisation for Scientific Research under the program ‘Conflict and Security’ (grant no. 432-08-089 to R.A.R.)

References


Moule, R. K., Pyrooz, D. C. and Decker, S. H. (2013), ‘From “What the f@#% is a Facebook” to “who doesn’t use Facebook?”: The Role of Criminal Lifestyles in the Adoption of the Use of the Internet’, Social Science Research, 42: 1411–21.


Roks, R. A. (2016), *'In de h200d. Een Eigentijdse Etnografie Over de Inbedding van Criminaliteit Enidentiteit'* , PhD dissertation, Department of Criminology, Erasmus University.


