Computers in Human Behavior 126 (2022) 106979

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals

Eric Rutger Leukfeldt[a,b,*], Thomas J. Holt[c]

[a] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan, 1077, Amsterdam, the Netherlands
[b] Centre of Expertise, The Hague University of Applied Sciences, The Hague, the Netherlands
[c] Michigan State University, USA

ARTICLE INFO

Keywords:
Cybercrime
Phishing
Malware
Organized crime
Criminal network
Cafeteria-style offending

ABSTRACT

Criminologists have frequently debated whether offenders are specialists, in that they consistently perform either one offense or similar offenses, or versatile by performing any crime based on opportunities and situational provocations. Such foundational research has yet to be developed regarding cybercrimes, or offenses enabled by computer technology and the Internet. This study address this issue using a sample of 37 offender networks. The results show variations in the offending behaviors of those involved in cybercrime. Almost half of the offender networks in this sample appeared to be cybercrime specialists, in that they only performed certain forms of cybercrime. The other half performed various types of crimes on and offline. The relative equity in specialization relative to versatility, particularly in both on and offline activities, suggests that there may be limited value in treating cybercriminals as a distinct offender group. Furthermore, this study calls to question what factors influence an offender's pathway into cybercrime, whether as a specialized or versatile offender. The actors involved in cybercrime networks, whether as specialists or generalists, were enmeshed into broader online offender networks who may have helped recognize and act on opportunities to engage in phishing, malware, and other economic offenses.

1. Introduction

Criminologists have frequently debated whether offenders are specialists, in that they consistently perform either one offense or similar offenses, or versatile by performing any crime based on opportunities and situational provocations (Britt, 1994, pp. 173–191; DeLisi, 2003; Moffitt, 1993; Piquero, Farrington, & Blumstein, 2007; Wolfgang, Figlio, & Sellin, 1972; Youngs & Canter, 2012). The issue of offense specialization or versatility is often examined in the context of developmental theories of crime (e.g. Moffitt, Caspi, Rutter, & Silva, 2001: Laub & Sampson, 1993) as a way to assess the development and progression of a criminal career. Contradictory evidence is presented by researchers who support the general theory of crime (Gottfredson & Hirschi, 1990) or rational choice frameworks (Cornish and Clarke, 2014; Guerette, Stenius, & McGloin, 2005), who argue the absence of specialization is a result of individuals acting on opportunities when available.

Evidence suggests that street criminals are largely versatile (Britt, 1994, pp. 173–191; DeLisi & Piquero, 2011; Jacobs & Wright, 1999; Kempf, 1987), leading to the notion of "cafeteria-style offending" whereby individuals seize upon criminal opportunities presented within specific situations or on the basis of offender networks (Klein, 1995). For instance, qualitative and quantitative research has found evidence that individuals who engage in burglary do not engage in burglary only, but sell drugs, perform robberies, steal cars, and act on whatever criminal opportunities may emerge (Cromwell, Olson, & D'AunnWesterAvary, 1991; Jacobs, 1999; Jacobs & Wright, 1999; Piquero et al., 2007; Wright & Decker, 1994, 1997). The fact that many of these offenses could be clustered into an offense type, such as theft, leading to some confusion over whether this should be viewed as a sort of specialization or should be viewed as versatility (DeLisi, 2003; McGloin, Sullivan, & Piquero, 2009; Williams & Arnold, 2002; Youngs & Canter, 2012; Youngs, Ioannou, & Eagles, 2016).

The paradox of specialization has yet to be satisfactorily resolved (Youngs et al., 2016), though the broader insights from this literature regarding the nature of street crimes are substantial. Individuals engaged in street crimes frequently offend with others, though partnerships may be short-lived and driven by situational utility rather than unique specialized roles to facilitate offending (Klein, 1995; Wright &

[*] Corresponding author. Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan, 1077, Amsterdam, the Netherlands.
E-mail address: Rleukfeldt@nscr.nl (E.R. Leukfeldt).

https://doi.org/10.1016/j.chb.2021.106979
Received 17 February 2021; Received in revised form 15 July 2021; Accepted 8 August 2021
Available online 10 August 2021

Decker, 1994, 1997). Co-offending networks may also be limited by the fact that individuals may prey upon their peers as suitable targets should the opportunity arise (Cornish & Clarke, 2014; Jacobs, 1999). The spoils of criminality are used largely to continue a party lifestyle based around drugs or alcohol. Money made from criminality may also be used to keep up appearances in the context of street life and values, and rarely goes toward paying bills or essentials (Jacobs & Wright, 1999; Klein, 1995; Wright & Decker, 1997).

Such foundational research has yet to be developed regarding cybercrimes, or offenses enabled by computer technology and the Internet (Holt & Bossler, 2015). Much of the extant research on cybercrime has focused on so-called cyber-enabled crimes, or activities that are made easier by the use of the Internet and online communications platforms, including harassment, stalking, and online fraud schemes (Holt & Bossler, 2015; Leukfeldt & Yar, 2016; McGuire & Dowling, 2013, p. 75). These studies largely focus on prevalence and theoretical predictors of offending, particularly involvement in interpersonal offenses and participation in digital piracy (Holt & Bossler, 2015; Maimon & Louderback, 2019). Less research explores so-called cyber-dependent crimes, or offenses that only exist as a function of and directly target information technology, particularly computers, networks and digital data (Leukfeldt & Yar, 2016; McGuire & Dowling, 2013, p. 75). These offenses primarily involve some form of computer hacking or the use of malicious software, and cause substantial economic harm to businesses and consumers alike (see Holt & Bossler, 2015; Maimon & Louderback, 2019).

There is less research exploring whether individuals involved in cyber-dependent crimes are versatile or inclined toward specialization (Holt & Bossler, 2015; Leukfeldt, Kleemans, & Stol, 2017b). These offenses require a degree of specialized knowledge related to computers and network protocols in order to be effective (Holt, 2007; Steinmetz, 2015). The same is true for related forms of financially motivated cyber-enabled crimes like phishing, as the offender must often maintain an online infrastructure of sites and malware (Holt, 2013; Leukfeldt, Kleemans, & Stol, 2017a).

At the same time, the emergence of markets that sell malware, sensitive data, and hacking tools have made it far easier for anyone to engage in sophisticated forms of cyberattacks and fraud (Franklin, Perrig, Paxson, & Savag, 2007; Holt, 2013; Hutchings & Clayton, 2016; Leukfeldt et al., 2017). Additionally, offenders may utilize so-called money mules who can cash checks or make wire transfers via Western Union to obtain physical currency from cybercrime schemes like phishing and carding (Hutchings & Holt, 2015; Leukfeldt, 2016; Roks, Leukfeldt, & Densley, 2020). The degree of technical knowledge needed to complete these activities may be small, or involve the use of recruited actors who unwittingly participate in the offenses in order to complete some of these crimes (Hutchings & Holt, 2015; Leukfeldt et al., 2017b).

These issues require research assessing the degree to which individuals involved in economic cybercrimes simply act on opportunities presented to them while in the process of engaging in other real world offenses, or if there is some degree of specialization involved. Specifically do individuals engage in cybercrimes only, real world offenses only, or both offenses depending on their level of knowledge? In addition, there is little empirical evidence as to the ways that cybercriminals utilize any profits earned from their offending, regardless of offender versatility. This study attempted to address these questions through a qualitative analysis of 37 criminal investigations carried out by law enforcement agencies in the Netherlands, Germany, United Kingdom and United Sates. The implications of this analysis for our understanding of the degree of offender versatility in on and off-line spaces were explored in detail.

2. Cybercrime offending versatility and specialization

Cybercrimes are similar to traditional real world offenses in that they take multiple forms with expressive and/or instrumental value to the offender. Acts such as online harassment and cyberbullying may provide the offender with a sense of power similar to what is observed in real world violence (Holt & Bossler, 2015; Patchin & Hinduja, 2013). Cyber-enabled fraud schemes such as phishing enable individuals to acquire personal information which could be used for financial gain (James, 2005; Leukfeldt, 2016; Wall, 2007). Additionally, the offenses themselves have commonalities that may contribute to confusion over the nature of specialization or versatility observed in real world crime research (Kempf, 1987; Youngs, 2011). For instance, an individual may use computer hacking techniques to gain access to a computer network in order to steal sensitive files or materials that could be used for fraud or sold to others (Jordan & Taylor, 1998; Schell & Dodge, 2002). The same effect could be achieved through the use of malicious software, though not all individuals who hack utilize these tools (Holt, 2013). Thus, these offense types may be clustered together, but are not strictly the same, which may create confusion when attempting to measure involvement in cybercrimes generally (Youngs et al., 2016).

The body of empirical research on cybercrimes has placed generally limited emphasis on understanding the nature of specialization or versatility. Most quantitative assessments focus on the prevalence of offense types across college populations with a focus on simplistic forms of offending, that may produce limited economic gains (Holt & Bossler, 2015; Maimon & Louderback, 2019). Evidence suggests that between 30 and 40 percent of college student samples engage in piracy (e.g. Holt, Burruss, & Bossler, 2010), though less than 20 percent report engaging in acts of basic computer hacking (e.g. Holt et al., 2010; Marcum et al., 2014; Rogers, Smoak, & Liu, 2006). Less than 10 percent of student samples appear to engage in more serious offenses that may be used to generate funds, such as the creation or distribution of malicious software or forms of electronic fraud (Holt & Bossler, 2015; Rogers et al., 2006).

Though prior research has generally eschewed measurement of offender versatility, evidence from qualitative studies of serious economic offenders provides some insight into the ways they operate. Individuals engaged in phishing, malware, and complex hacking operations tend to offend with a limited number of co-conspirators, though they are enmeshed in larger online social networks that may facilitate access to information and techniques to offend (Dupont, Côté, Boutin, & Fernandez, 2017; Leukfeldt, Kleemans, & Stol, 2017; Leukfeldt & Roks, 2020; Roks et al., 2020). The participants appear to have some division of labor that justifies their co-offending, such as knowledge of certain programming languages or connections to local communities who can serve as money mules (Dupont et al., 2017; Holt, 2013; Leukfeldt & Holt, 2020; Roks et al., 2020).

These studies also find that there is potential for cybercriminal versatility, since some offender groups engaged in offenses that cut across both physical and virtual spaces (e.g. Leukfeldt et al., 2017b; Roks et al., 2020). Individuals who obtain credit or debit card data through phishing and data breaches regularly work with others to move funds from the hijacked accounts so that it can be converted into cash (Leukfeldt, 2016; 2017a). This may take the form of cashout teams who can use illegally acquired debit card information at physical ATMs in order to withdraw funds (Hutchings & Holt, 2015). Some may also utilize money mules who may be recruited through online advertisements or through local community connections, including immigrant communities who can be exploited for their labor (Leukfeldt, 2016; Leukfeldt et al., 2017b).

It is unknown how much technical skill these service providers need in order to facilitate the offense, as well as whether they engage in cashing related crimes only, or offend whenever opportunities appear on or offline. The growth of cybercrime-as-service operations, where individuals pay others to use existing malware and hacking infrastructure to engage in attacks, may reduce the need for such expertise (e.g. Dupont et al., 2017; Hutchings & Clayton, 2016). Instead, individuals may be able to engage in different forms of cybercrime at will, so long as they have sufficient financial resources to pay for services. The costs involved may present a barrier to entry, as well as the need for basic technical skills to troubleshoot in the event the tool or infrastructure is not functioning properly (Hyslip & Holt, 2019).

These gaps in the literature require greater examination in order to understand the nature of versatility and specialization of criminality, and cybercrime in particular (Dupont et al., 2017; Leukfeldt et al., 2017a; Roks et al., 2020). Prior criminological research provides some insights into these dynamics, though further research is needed with diverse samples of active offender populations to understand how their behaviors take shape and evolve over time (e.g. Leukfeldt, 2016). Furthermore, research is needed that explores the degree of overlap in offline and online offending across serious cybercriminal communities and assess any variations in their practices (Roks et al., 2020). There is also a need for exploration of the ways that members of cybercriminals networks spend their criminal earnings relative to their versatility. Such insights can improve our knowledge of whether networks mirror what is known about street criminals who engage in "cafeteria-style offending" (Jacobs, 1999; Jacobs & Wright, 1999; Klein, 1995). Specifically, some evidence suggests profits derived from versatile street offending is small and short-lived, being spent in part on maintaining a party lifestyle around drug and alcohol use, and to a lesser extent on basic necessities such as food and shelter (Jacobs & Wright, 1999; Wright & Decker, 1994, 1997).

The current study specifically explores to what extent cybercriminal networks can be labelled as specialists or versatile offenders and if they fit the 'cafeteria-style offending' label. In order to do so, this study will attempt to address these issues using a study of 37 offender networks developed from criminal investigations carried out by law enforcement agencies in the Netherlands, Germany, United Kingdom and United Sates.

3. Data and methods

This study utilized data collected from 37 separate criminal investigations into criminal networks active in committing cyber-dependent crimes involving malware, or the financially-motivated cyber-enabled crimes phishing and fraud (Leukfeldt & Yar, 2016; McGuire & Dowling, 2013, p. 75). Other forms of cyber-enabled crime were excluded from the selection of cases, as the goal of the data collection was to gain more insight into financially motivated cybercrimes aimed at attacking customers of financial institutions (see, for example, Leukfeldt et al., 2017a; 2017b; 2017). Therefore, only the cybercrimes 'phishing', 'banking malware' and 'credit card fraud' were selected.[1]

The unit of analysis for this study are the networks of actors know to have engaged in four forms of economic cybercrime. A network in this case is defined as the suspects associated with a known criminal event, inclusive of those who performed the primary offenses such as the implementation of malicious software or creation and management of phishing schemes. In addition, the ancillary suspects who facilitated the offense, such as money mules, were included. Participants within a network had to have some tie to one another, whether through direct communication and contacts, or connection through a recruiter.

The focus on networks is distinct from traditional research on offender versatility, which typically explores individual-level behaviors (Piquero et al., 2007; Wolfgang et al., 1972), even in the context of gang membership (e.g. Adams & Pizarro, 2014; Melde & Esbensen, 2013; Wiesner, Yoerger, & Capaldi, 2018). Such research is possible due to the prevalence of traditional street offending behaviors reported by the general public. Serious economic cybercrimes, like phishing, are far less common and are difficult to identify via general population studies (Holt & Bossler, 2015; Weulen Kranenbarg et al., 2019). Thus, sampling on known networks of offenders provides access to a convenient, yet purposive population of offenders. Furthermore, evidence from both academic research and law enforcement investigations demonstrates that computer hacking and related offenses are largely a group activity, involving social ties between multiple actors (e.g. Dupont et al., 2017; Hutchings & Holt, 2015; Leukfeldt et al., 2017a). Situating individuals within their broader offender network is essential to better identify the distinct factors that shape their activities, and assess their overall versatility.

Criminal cases in various countries were reconstructed: the Netherlands, Germany, United Kingdom (UK) and United States (US). The methodology used varied on the basis of the location of the investigation, though all research materials involved qualitative data. First, the research team utilized police files for information related to 18 cybercriminal networks operating in the Netherlands. These data provided distinct evidence of the activities of the offenders involved in the networks derived from wire and IP taps, overt and covert police observations, and house searches. This data was not publicly available, and required permission from the Public Prosecution Service, as well as external assessment from the Dutch Ministry of Security and Justice's Research and Documentation Centre (WODC) on the qualities and outcomes of the proposed research.

Upon approval, the researchers were required to analyse data from police investigations in the physical buildings of the Public Prosecution Service and relevant police departments. The researchers could then review all materials and take notes on their own devices, though all electronic files had to be stored on encrypted hard drives. All offender-related materials had to be anonymized to reduce the likelihood of identification, which led to the use of pseudonyms for their role in the offenses. Additional interviews were conducted with members of the Public Prosecution Service, police team leaders, and senior detectives to augment the police files. There was particular emphasis on developing information from investigators on the offender networks and practices beyond the evidentiary focus of the official records. Clarifying questions were asked regarding ties between members, the economic activities of offenders, and their practices while they were actively offending. These 18 cases reflect all phishing and malware attacks against financial institutions investigated by Dutch police at that time.

Data for 21 additional cases were developed from three countries: nine in the UK, nine in the US, and three in Germany. For these cases, the researchers were unable to obtain direct access to police files. Instead, cybercriminal networks were reconstructed solely based on interviews with case officers and/or Public Prosecutors involved in the criminal cases. Official court documents about the cases were also analyzed to triangulate the data acquired via interviews. It should be noted that the German, UK, and US cases did not provide as much substantive detail as those produced from Dutch data. This may be a function of the nature of the case data available to the researcher, rather than any differences in the legal definitions regarding these types of cybercrimes, investigative strategies and law enforcement priorities. Thus, these cases provide additional value to understand the underlying offending practices and economic activities of offenders.

In these countries, case officers were interviewed in order to gain more insight into direct ties, origin and growth, use of forums, and criminal capabilities of criminal networks. Contacts with law enforcement agencies in the different countries were made using existing contacts within the Dutch police (especially the Dutch High Tech Crime Unit) and the Dutch Police Academy. It was difficult for the researchers to obtain overviews of the completed criminal investigations into cybercriminal networks. As a result, the cases from Germany, the UK and US can be seen a convenience sample meant to extend the data beyond a Dutch context. Leads to relevant cases were provided by the Dutch National High Tech Crime Unit through a media analysis carried out by

[1] Phishing is the process of retrieving personal information using deception through impersonation (Lastdrager, 2014). Malware is the infection of a device – in this case one that is used for online banking – with malicious software, including viruses, worms, Trojan horses and spyware, for the purposes of carrying out the harmful intentions of an attacker (Moser, Kruegel, & Kirda, 2007). Credit card fraud is the act of fraudulently using a payment card.

the researchers and based on information from the NCA, BKA, USSS and FBI. These factors may result in an overrepresentation of high-profile investigations and offender populations in the data.

A snowball sampling method was used to generate 22 cases covering offenses occurring between 2003 and 2014. Interviews with case agents were conducted between March 2014 and November 2015. First contact was made with cybercrime teams at the national level: in the UK the NCA (National Crime Agency), in the US the USSS (United States Secret Service) and FBI (Federal Bureau of Investigation), and in Germany the BKA (Bundeskriminalamt). After a first meeting with the team leader, follow-up appointments were scheduled with case officers who had been involved in relevant criminal investigations. An agreement was drafted with the UK NCA concerning data collection and the use of data.

Kleemans (2014) provides an overview of the strengths and weaknesses of using police investigations for scientific research based on three decades of experience with the Organized Crime Monitor in the Netherlands. The immediate benefits lie in the ability to generate solid empirical data on a wide cross-section of criminal cases. Closed police files of criminal groups are the main sources of these cases. Each investigation on which the police files are based often spans a period of several years. Furthermore, Leukfeldt and Kleemans (2021) describe the added value of reconstructing cases based on interviews with case officers, which can be triangulated with official court document and open source information.

To assess the extent to which offender networks were specialized or generalists, the primary and secondary modus operandi of the offenders in each network were analyzed. It should be noted that this analysis focused on the broader activities of the individuals nested within their offender networks, rather than the offenders' specific activities as individuals. Prior studies have examined the social organization of cybercriminal networks and the specialization of actor roles within the context of cybercrime (i.e. Leukfeldt & Holt, 2020). Instead, this study focused on the primary criminal activities of the networks that were the main focus of the criminal investigation.

In the initial selection of cases, only financially motivated cybercrimes aimed at attacking customers of financial institutions were included, and the primary modus operandi of the network in the case had to involve 'phishing', 'banking malware' or 'credit card fraud' (see the definition of these crimes in footnote 1). Individuals who engaged in only one of these offense types with no secondary forms of offending were considered specialists. Those who not only performed one offense, but also other forms of crime on or off-line were considered generalists or versatile offenders. The sampling framework used meant that the primary crime types of the actor would involve some form of economic cybercrime. The secondary activities of those in the network were, however, variable and captured on the basis of the crimes noted by police investigators.

In addition, the researchers noted any profits that offenders in the network may have generated from their primary or secondary criminal activities. This information was not present in all investigation files and interviews due to inconsistencies in victim reporting, whether by individuals or financial institutions. In some cases, estimated profits were provided by co-conspirators who were interviewed by law enforcement. Any information provided by investigators or suspects as to the ways that criminal gains were used to support individual lifestyles were also analyzed.

4. Findings

Examining the primary and secondary criminal activities of the offenders across these 37 networks, demonstrated three categories of offenders: cybercrime specialists, cybercrime versatile, and traditional offline crime and cybercrime versatile. In fact, 18 of the 37 networks in this data set can be labelled as specialist networks. These networks performed phishing, malware, or another specific form of cybercriminal activity only. There was no evidence within the data that members of these networks were involved in other types of crime in off-line environments.

In total, 19 networks can be considered versatile, though that versatility can be segmented into online only activities and those which cut across both virtual and real environments. Four of the networks were generalists in cybercrimes, while 15 were engaged in both cybercrimes and traditional offline crimes. Examples of the versatile cybercrime category include a network that used both phishing and malware to execute attacks, and a network that used banking malware to take over online bank accounts, as well as steal credit card credentials. Examples of the versatile cyber and online offenders include a phishing network whose members are also active in burglaries and drug trafficking, and a network that used credit card credentials to commit fraud with additional ties to traditional organised crime. Below, cases in all three categories are described in depth. Case descriptions included the primary modus operandi, secondary modus operandi and how the criminal earnings were spent. Quotes from the data are provided where possible. An overview of all the cases can be found in Tables 1–3.

4.1. *Specialists networks*

The core members from 18 of the 37 networks could be classified as specialist networks, as there was no evidence within the data that members were involved in other types of criminal activity on or offline. The participants' goal appeared to be economic gain through the theft of personal data, inclusive of online bank accounts or credit card numbers, using various methods. It should be noted that although these 18 networks are labelled as specialists, the individual members of these networks usually had their own specific role within the network (e.g. malware writer, developer of phishing kits, money mule recruiter or casher – see Table 1). As all of these roles were needed to carry out the primary modus operandi of the group, these groups were labelled as specialists. Table 1 shows that six networks specialized in phishing attacks to obtain user credentials, four used banking malware attacks, and three involved hacking databases containing credit card credentials. Only one network was identified where the offenders simply bought financial or personal credentials online for use in fraud.

Unfortunately, there was generally little evidence in the data regarding the ways that specialist offender networks spent their criminal earnings. There was some information available in networks 2, 10 and 20 regarding how any funds acquired were dived amongst the criminals and spent. The offenders in network 2 were able to steal approximately 500,000 euros, based on an assessment of all reported victim losses. These funds were acquired through a cash out process, whereby money was moved from victim accounts to those of money mules who would in turn transfer those funds to the primary offenders. One member in the network was directly linked to 67,000 Euros in diverted funds from mule accounts to his own. The mules associated with this network who were interviewed by police reported that the main members used their profits to finance an expensive lifestyle, wearing designer clothes, and spending money when going out buying drinks for large parties at clubs. One of the mules described his lifestyle succinctly during an interrogation, stating:

> The clothes of this guy were from Gucci, they also frequented a club. They were in the secured VIP-area, we were in the crowd … One was wearing a Moncler [brand name coat]. That's an expensive coat. I've always wanted to have such a coat. Both had golden teeth.

Additionally, the main network of offenders appeared to avoid sharing any of their profits with the mules who facilitated their fraudulent schemes. One mule who was arrested by Dutch police stated their recruiter said they would receive a portion of the total transfer, though they would have to negotiate the final amount. The main network and their recruiters would often lie to mules to avoid payment, as in one case where a mule stated:

Table 1
Overview of specialist networks.

No.	Primary criminal activity	Secondary criminal activity	Roles within the network	Spending of criminal earnings
2	Phishing	None	Caller, transferring money, money mule recruiter, cashing, money mules	Lifestyle
4	Phishing	None	Casher, money mule recruiter, money mules	Lifestyle
6	Malware	None	Coordinator, developer phishing website, money mule recruiter Europe, money mule recruiter Russia, translator, spammer, casher, money mules	Unknown
10	Phishing	None	Caller, transferring money, cashing, postal employee, bank employee, money mule recruiter, money mules	Lifestyle
15	Phishing	None	Coordinator, malware writer, malware adapter, cashing, money mule recruiter, money mules	Unknown
17	Phishing	None	Spamming, caller, cashing, money mule recruiter, money mules	Unknown
18	Malware	None	Coordinator, falsifier identity documents, cashing, money mule recruiter, money mules	Unknown
20	Phishing	None	Coordinator, coder, money mule recruiter coordinator, money mule recruiter, money mules	Lifestyle
24	Hacking	None	Coordinator, hacker, coder, forum administrator, money mule recruiter, money mules	Investments
26	Malware	None	Coordinator, money mule recruiter, money mules	Unknown
28	Hacking	None	Coordinator, hacker, money launderer, money mules, end users forum	Unknown
31	Hacking	None	Hacker, wholesaler, developer hacking tools, end users forum	Unknown
32	Hacking	None	Coordinator, hacker, carder, casher, vendor on forum, end users forum	Unknown
33	Hacking	None	Coordinator, seller, franchiser, money launderer, end users forums	Unknown
34	Hacking	None	Hacker, vendor on forum, exchanger, end user forum	Unknown
36	Buying logins	None	Coordinator, fencer, credit card supplier, money launderer, driver, shopper	Unknown
38	Malware	None	Coordinator, transferor, coder, malware writer, coordinator money mules, recruiter money mules, money mules	Unknown
39	Malware	None	Phishers, falsifying identity documents, money mule recruiters, money mules	Unknown

Table 2
Overview of versatile cybercrime networks.

No.	Primary criminal activity	Secondary criminal activity	Roles within the network	Spending of criminal earnings
11	Malware	Credit card credentials; extortion of bank; skimming	Coordinator, malware writer, telecom provider, caller, money mule recruiter, money mules	Lifestyle
13	Malware	phishing web shops and online consumer fraud	Obtain logins, spamming, malware writer, postal employee, money mule recruiter, money mules	Unknown
21	Malware	Botnet rental	Coder, end user on forum	Unknown
22	Phishing	Buying stolen credit card credentials	Coordinator, data provider (forum), caller, money mule recruiter, money mules	Unknown

[Main member 1] had told me that the transaction had failed and that the card was blocked. [so no money was paid to the money mules]. However, [the recruiter] approached me with his bank statement at one point. It stated that 2500 euros had been transferred along with the description ‘Driving school owner’. I then went to [Main suspect 1] and showed the statement of [the recruiter] … I told him to give the boys money and me too. [Main member 1] started to justify everything, he had excuses. For example, I would get double the next time. He had excuses every time.

The main actors in Network 10 were similarly effective at acquiring money through phishing, though the amounts obtained from any phishing scheme were variable. For instance, the group were linked to an estimated 1.4 million Euro in phishing victim losses reported by financial institutions. The targeted banks were able to stop approximately half of all of those fraudulent transactions, leading to a yield of approximately 700,000 Euros total for the offenders. Further details were revealed by a money mule recruiter involved with the scheme who was interrogated by police. They indicated that a yield of 1000 Euros from an account would typically generate 600 Euros to the core members of the network. The remaining 400 would be split with 75 % going to the mule and 25 % to their recruiter.

Despite the funds generated by phishing, the main offenders appeared to engage in relatively simple lifestyles. One of the members lived in an older, ramshackle apartment and maintained a legitimate job as a receptionist at a large construction company. The size of the network may have minimized the overall profits available, and some of the members reported engaging in spending sprees for clothing, as well as paying for expensive dinners and drugs.

By contrast, the members of network 20 also spent most of their money on an expensive lifestyle. This group was based in the UK and Eastern Europe and was involved in phishing attacks in various European countries. The police respondents stated in their reports:

> “(…) “E”[a member of the network] lived the life. Even his underpants were dry cleaned.

And I am not joking either. So he had, you know, travelled first class on the trains. He spends a lot of money in central London nightclubs, where even if you want to sit on a table, you have to be spending a thousand pounds. So he lived everything. And he would transfer cash back to Africa. “C” and “D” lived in extremely well-furnished premises in Romania. So they used it to maintain a lifestyle. (…) They were just blowing their money. Because for them the percentages were smaller. So you know if they have got 400 or 600 pounds, for them it was just of two weeks having a good time and that was it. There was nothing to invest, because it didn’t get high enough – only the opportunity to have a

Table 3
Overview of versatile cybercrime and traditional offline crime networks.

No.	Primary criminal activity	Secondary criminal activity	Roles within the network	Spending of criminal earnings
1	Phishing	Skimming, burglary, drug trafficking, fraud with phone subscriptions	Coordinator, caller, casher, bank employee, post worker, developer phishing website, falsifier identity documents, money mule recruiter, money mules	Lifestyle + investments
3	Phishing	Malware, drugs dealing, money laundering	Casher, money mule recruiter, money mules	Lifestyle + investments
5	Phishing	Burglaries, street robberies, fencing stolen jewelry	Casher, money mule recruiter, money mules	Investments
8	Phishing	Burglary	Coordinator, caller, transferring money, spammer, casher, money mule recruiter, money mules	Lifestyle
9	Phishing	Theft, burglary, drugs, robbing, drug dealing, assault	Bank employee, casher, money mule recruiter, money mules, falsifier identity documents	Lifestyle
12	Phishing	Fraud and human trafficking	Obtain logins, falsifier identity documents, cashing, money mule recruiter, money mules	Unknown
14	Phishing	Offline banking fraud	Bank employee, caller, transferring money, falsifier identity documents, cashing, money mule recruiter, money mules	Unknown
16	Phishing	Malware, drug dealing	Falsifier identity documents, cashing, money mule recruiter, money mules	Unknown
19	Malware	Offline fraud, burglary, robbing	Coordinator, malware developer, bank employee	Lifestyle
23	Phishing	Drug dealing	Coordinator, postal employee, caller, money mule recruiter, money mules	Lifestyle
25	Malware	Armed robbery, extortion, fraud, boiler room fraud	Hackers, bank employee	Unknown
27	Malware	Fraud, organized crime	Coordinator, transferor, coders, money mule recruiter, money mules	Unknown
30	Phishing	Credit card theft + traditional organized crime	Coordinator, e-mail harvester, developer phishing websites, translator, card writer, money mule recruiter, money mules	Unknown
35	Buying logins	Offline fraud	Coordinator, seller logins, exchanger, money mule recruiter, money mules	Unknown
37	Malware	Credit card theft + traditional organized crime	Coordinator, hacker, coder, exchanger, money mule	Unknown

certain lifestyle. And maybe that attract the mules … lots of money. [They became] elevated persons within their social network.

Such activities differ from what is known about the practices of most street criminals whose profits do not enable such lavish lifestyles (Jacobs & Wright, 1999; Wright & Decker, 1994) and reinforce the substantial earning potential of cybercrime generally.

4.2. Versatile offenders: all-rounder cybercrime versus all-rounders cybercrime and offline crime

As noted earlier, 19 networks contained generalist offenders, segmented on the basis of whether they performed various forms of cybercrime (n = 4; 21 %) or engaged in both cybercrimes and traditional offline crimes (n = 15; 79 %; see Table 2). The primary criminal activities of three of the general cybercrime networks involved the use of malware, though one also engaged in the purchase of stolen financial credentials via phishing. The actors involved in malware used their skills as programmers to create various forms of malicious code, though they also performed types of online fraud and theft, such as phishing, buying credit card credentials and skimming bank cards. Three of these networks also engaged in recruiting money mules for phishing and cash out operations as an extension of their online fraud activities.

One of the networks that carried out various cybercrimes, but no traditional offline crimes was Network 11. The primary actors involved with this network were three individuals operating out of the Netherlands, Germany and Turkey respectively. This network was identified as a result of a criminal investigation that began from victim reports in the Netherlands. The primary core actor would log into bank accounts acquired through malware that captured user credentials and one-time security codes. Once he gained access to the user accounts, he would then perform electronic funds transfers to accounts he and his co-conspirators controlled. The offender network succeeded based on their collaborative efforts, as evidence demonstrated that the Dutch participant did not understand how the malware functioned, and depended on others to acquire credentials. In fact, he regularly posted in Internet Relay Chat asking questions and actively soliciting others, stating: “Looking for help to exploit … Willin to trade with nice things) also looking for UK and TR LOGS .. paying egold and wu now contact me."

Member 1’s efforts with banking malware led to losses of approximately 35,000 Euros, emphasizing the lucrative nature of this form of cybercrime. He also regularly received credit card details from the third core member within the network, who apparently obtained the information from accomplices working within a financial institution. He then used the information to make purchases in both physical and online stores, eventually leading to approximately 73,000 EU in fraudulent charges.

The participants reportedly recognized that the money they obtained was easily spent, requiring them to continuously engage in fraud to keep profits coming in. Evidence from the police files noted that during wire tapped conversations, Member 1 had discussions with an accomplice regarding the funds earned from their offending, which was captured in police reporting:

Both [Member 1 and accomplice] indicate that they want to stop when they have received a nice amount, but that until now the money they earned was always spent quickly and that they needed to make money again. It is a kind of addiction, [Member 1] says. There is talk of buying hotels in Turkey in order to be able to live off their rental, but this seems to remain a dream.

In this respect, the network mirrors traditional street criminals who must engage in offenses in order to maintain a basic standard of living (Jacobs & Wright, 1999; Wright & Decker, 1997).

The larger proportion of networks (n = 15; 79 %) included offenders involved in both cybercrime and traditional offline crimes such as burglaries, street robberies or selling drugs (see Table 3). For instance, Network 9 included members of a criminal network who were involved in both cybercrimes and traditional offline forms of crime. The investigation actually began by Dutch police as a function of their offline activities, most notably burglary, as well as drug trafficking, robbery, and violence.

Police investigators essentially discovered their role in phishing by coincidence eight months into their initial investigation while monitoring a wire tapped phone conversation. The participants indicated that they had an appointment in the city center of The Hauge to “swipe,” or cash out money fraudulently obtained from bank accounts. The police file of the call noted one individual say: “I heard ‘V’ said this man was waiting. I heard ‘V’ say to the man: “Come quickly, that ‘sani’ will be on in a minute”. [Sani is slang for “the thing/case will continue].” Police in The Hague observed individuals physically handing stacks of bank cards between themselves while near ATMs. They then withdrew money from the machines at which time police arrested seven individuals in the process of cashing out accounts.

Network 3 was another example of a network in which the members performed cybercrimes as well as traditional offline crimes. Several of its members had direct family ties, and knew one another from living in the same neighbourhood or attending the same schools. The network was engaged in phishing and consisted of eight members with different roles depending on their abilities, such as cashing out accounts from ATMs, the recruitment of money mules, and money laundering. Subgroups from this network were also involved in different criminal activities, such as the sale of MDMA pills.

The network was identified by police in Amsterdam because of its focus on prolific offenders within a given place. Similar to Network 9, the group’s cybercrime activities were identified based on activity in physical space. Specifically, a group of youths were loitering by a parked car and began to move on foot when they saw the police approaching. The officers searched these youths and the vehicle which no one claimed to own. The car smelled of marijuana and had an envelope filled with bank cards in the glove compartment.

Police seized the vehicle since no one claimed to own it, though that evening an individual arrived at the police station with their girlfriend. The individual claimed the car was a rental vehicle he had picked out, though it was in her name. A search of the individual’s name revealed he was one of the top 600 individuals of interest in the area, due to an ongoing investigation related to a phishing and money mule scheme. He and two others were observed at an ATM attempting to obtain cash from a money mule account. When police searched his phone while he was in the station, a photo was found containing bank transfer information. It was though that he was responsible for losses to three victims totalling over 150,000 EU.

The actor’s involvement in offline criminal activity was reinforced by a money mule who worked for him, stating while being interrogated by police:

A classmate asked if I wanted to earn money quickly. He said: “You have to give me your bank card and security code.” He would get 800 euros for it. The money mule knew that whoever he gave the pass to was doing bad things. “He had already robbed a school. And later also a house. He offered stolen things to people. He also sells weed at school.

Another mule stated that: “[member 1] is involved in criminal offenses and his friends are not sweethearts. He sometimes asked me if I wanted to exchange counterfeit money for him. I had to buy something small with a counterfeit banknote, so that I could get real change back.”

Examining the police data suggested that members of Network 3 spent their criminal profits quickly, though the information was not thorough on what kinds of items or activities. Individuals interviewed by police noted the network members generally spent their money renting expensive cars, buying clothes and partying. In addition, police searches of one of the network member’s homes revealed thousands of euros worth of clothing was found in the homes of the members. A money mule also noted one of the member’s activities:

The guy takes her [a girlfriend] out to dinner several times and gives her expensive clothes. Jacket of 500 euros, shoes of 250 euros. He also sometimes gives money to buy something for her son. When the core member hears about the money mule’s worries about money, he indicates that he knows a way to make money quickly.

Again, this reinforces that the offenders are likely to utilize their profits to engage in a party lifestyle similar to street criminals (Jacobs & Wright, 1999; Wright & Decker, 1997). The amount of money offenders can earn is, however, far more than what is typically derived from robbery, burglary, or other traditional forms of street crime.

5. Discussion and conclusions

Though research on cybercrime has expanded dramatically over the last two decades (Holt & Bossler, 2015; Leukfeldt, 2016), there are still myriad questions related to offending behaviors that must be explored. Specifically, there is generally little research addressing the extent to which cybercriminals are generalists who perform various crimes on and offline, or specialists who engage in only one offense type (Leukfeldt et al., 2017b; Roks et al., 2020; Weulen Kranenbarg et al., 2019). Criminologists examining traditional offenses have often debated this question, though evidence suggests street criminals are largely versatile (Britt, 1994, pp. 173–191; DeLisi & Piquero, 2011; Kempf, 1987; Klein, 1995). Offenders appear to act on situational opportunities, leading to what some refer to as “cafeteria-style offending” (Jacobs, 1999; Jacobs & Wright, 1999; Klein, 1995). The profits derived from offending are often small and short-lived, being spent in part on maintaining a party lifestyle around drug and alcohol use, and to a lesser extent on basic necessities such as food and shelter (Jacobs & Wright, 1999; Wright & Decker, 1994, 1997).

Limited evidence has considered the nature of specialization or versatility among those engaged in cybercrime, or the manner in which their criminal earnings are used (Leukfeldt et al., 2017; Roks et al., 2020; Weulen Kranenbarg et al., 2019). This study attempted to address this issue using a sample of 37 offender networks developed from police files and interviews in The Netherlands, Germany, the UK, and US. This study demonstrated variations in the offending behaviors of those involved in cybercrime. Almost half (48 %) of the offender networks in this sample appeared to be cybercrime specialists, in that they only performed certain forms of cybercrime. The other half performed various types of crimes on and offline. Only four networks (10.8 %) included versatile cybercriminals who performed multiple types of cybercrime. The relative equity in specialization relative to versatility, particularly in both on and offline activities, suggests that there may be limited value in treating financially motivated cybercriminals as a distinct offender group (Holt & Bossler, 2015; Weulen Kranenbarg et al., 2019).

This study also calls to question what factors influence an offender’s pathway into cybercrime, whether as a specialized or versatile offender. The actors involved in cybercrime networks, whether as specialists or generalists, were enmeshed into broader online offender networks who may have helped recognize and act on opportunities to engage in phishing, malware, and other economic offenses (see also Dupont et al., 2017; Leukfeldt et al., 2017a). Opportunities to engage in cybercrime among those who engaged in traditional offenses appeared to arise out of similar social ties, though they appeared to be more driven by relationships in physical spaces (Weulen Kranenbarg et al., 2019).

Since the data for this study did not focus on the broader origins of offender’s behavior, it is difficult to disentangle the factors that propelled individuals into versatile or specialized offending trajectories. It also is unclear why some criminal networks that have the opportunity to commit cybercrimes do not stop committing traditional offline crimes. Offline offending would have a greater risk of arrest or detection compared to online offending behaviors, though it is unclear if it is a function of offender interests or other factors (for example, Collier, Clayton, Hutchings, & Thomas, 2020). Future research is needed to identify the foreground and situational factors that affect cybercriminal criminal careers over the life course, and develop strategic interventions to reduce their likelihood of persistent offending (Brewer et al., 2019; Holt & Bossler, 2015; Leukfeldt et al., 2017b).

In addition, this study provided partial support for the notion that offenders appeared to spend their earnings from cybercrime on living an extravagant party oriented lifestyle. Regardless of whether the network contained specialists or versatile offenders, evidence from police indicated they spent their money on traditional trappings, including nice clothes, cars, and nightlife. These practices are in keeping with what is known about the general expenditures of street criminals, on maintaining a basic lifestyle while also keeping up a so-called party lifestyle of drug and alcohol use (Jacobs, 1999; Jacobs & Wright, 1999; Klein, 1995; Wright & Decker, 1997).

A key difference lies in the fact that cybercrime may generate far more income for offenders compared to physical crimes like burglary and robbery (e.g. Holt & Bossler, 2015; Newman & Clarke, 2003). Individuals who perform street crimes are only able to target a small number of victims at a time, and are dependent on their target having cash or valuables on hand that can be readily monetized (Cornish & Clarke, 2014; Wright & Decker, 1994, 1997). Thus, cybercrime appears to engender far more discretionary funds that can be spent on extravagant lifestyle activities (Holt, Smirnova, & Chua, 2016; Leukfeldt et al., 2017b).

The limited evidence of offender spending habits and earnings in this analysis is a function of the police data used. Law enforcement investigations typically focus more developing evidence to connect the suspects to specific criminal activities and victim complaints. The lifestyle and habits of offenders are less relevant compared to proof of involvement in phishing or malware schemes. Future research is needed specifically addressing this issue through interviews with offenders, victims, and police investigators to triangulate any claims of criminal earning potential. Additionally, structured interviews with offenders would be critical to better understand the ways in which their lifestyle choices were facilitated by cybercrime activities. In turn, we may better understand the similarities between the behaviour patterns of both offline and online offenders (Holt & Bossler, 2015; Leukfeldt, 2016).

There were additional limitations within this study that reduce its generalizability. First, this data focused on offenders whose activities were identified by police. They may not be reflective of active offenders who are able to operate without being detected by law enforcement. Further research is needed utilizing open source data from forums, markets, and other online sources to assess the versatility of active cybercriminals that may not be captured in official data (Holt & Bossler, 2015). Additionally, this sample contained offenders who were investigated by major European and North American police agencies. Their behaviors and spending patterns may not be reflective of cybercriminals in other parts of the world, particularly Asian nations and the global south broadly (Brewer et al., 2019; Newman & Clarke, 2003). Future research developing samples of offenders from these nations is vital to improve our understanding of the nature of cybercriminality and its association to traditional offending as a whole.

Credit statement

Eric Rutger Leukfeldt: Conceptualization, Methodology, Data collection, Writing- Original draft preparation. Thomas Holt: Conceptualization, Writing- Original draft preparation, Writing- Reviewing and Editing.

References

Adams, J. J., & Pizarro, J. M. (2014). Patterns of specialization and escalation in the criminal careers of gang and non-gang homicide offenders. *Criminal Justice and Behavior, 41*(2), 237–255.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. New York: Springer.

Britt, C. L. (1994). *Versatility. The generality of deviance*.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2020). *Cybercrime is (often) boring: Maintaining the infrastructure of cybercrime economies*.

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*.

Cromwell, P. F., Olson, J. N., & D'Aunn Wester Avary. (1991). *Breaking and entering: An ethnographic analysis of burglary* (Vol. 8). Newbury Park, CA: Sage.

DeLisi, M. (2003). Criminal careers behind bars. *Behavioral Sciences & the Law, 21*(5), 653–669.

DeLisi, M., & Piquero, A. R. (2011). New frontiers in criminal careers research, 2000–2011: A state-of-the-art review. *Journal of Criminal Justice, 39*(4), 289–301.

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

Franklin, J., Perrig, A., Paxson, V., & Savag, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM conference on computer and communications security* (pp. 375–388). New York: ACM.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Guerette, R. T., Stenius, V. M., & McGloin, J. M. (2005). Understanding offense specialization and versatility: A reapplication of the rational choice perspective. *Journal of Criminal Justice, 33*(1), 77–87.

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

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*(2), 31–61.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*(4), 353–367.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior, 37*(10), 1163–1178.

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

Hyslip, T. S., & Holt, T. J. (2019). Assessing the capacity of DRDoS-for-hire services in cybercrime markets. *Deviant Behavior, 40*(12), 1609–1625.

Jacobs, B. A. (1999). *Dealing crack: The social world of streetcorner selling*. UPNE.

Jacobs, B. A., & Wright, R. (1999). Stick-up, street culture, and offender motivation. *Criminology, 37*(1), 149–174.

James, L. (2005). *Phishing exposed*. New York: Elsevier.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.

Kempf, K. L. (1987). Specialization and the criminal career. *Criminology, 25*(2), 399–420.

Kleemans, E. R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson, & E. Cockbain (Eds.), *Applied police research: Challenges and opportunities. Crime science series. Cullompton: Willan*.

Klein, M. W. (1995). *The American street gang*. New York: Oxford University Press.

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

Laub, J. H., & Sampson, R. J. (1993). Turning points in the life course: Why change matters to the study of crime. *Criminology, 31*(3), 301–325.

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

Leukfeldt, E. R., & Holt, T. J. (2020). Examining the social organization practices of cybercriminals in The Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology, 64*(5), 522–538.

Leukfeldt, E. R., & Kleemans, E. R. (2021). Breaking the walls of silence: Analyzing criminal investigations to better understand cybercrime. In A. Lavorgna, & T. J. Holt (Eds.), *Researching cybercrimes: Methodologies, ethics, and critical approaches"*. Cham: Palgrave Macmillan (in press).

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

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704–722.

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

Leukfeldt, E. R., & Roks, R. (2020). Cybercrimes on the streets of The Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*. https://doi.org/10.1080/01639625.2020.1755587

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime. A theoretical and empirical analysis. *Deviant Behavior*. https://doi.org/10.1080/01639625.2015.1012409

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*, 191–216.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior, 35*(7), 581–591.

McGloin, J. M., Sullivan, C. J., & Piquero, A. R. (2009). Aggregating to versatility? Transitions among offender types in the short term. *British Journal of Criminology, 49* (2), 243–264.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence. Summary of key findings and implications*. Home Office Research report.

Melde, C., & Esbensen, F. A. (2013). Gangs and violence: Disentangling the impact of gang membership on the level and nature of offending. *Journal of Quantitative Criminology, 29*(2), 143–166.

Moffitt, T. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review, 100*(4), 674.

Moffitt, T. E., Caspi, A., Rutter, M., & Silva, P. A. (2001). *Sex differences in antisocial behaviour: Conduct disorder, delinquency, and violence in the dunedin longitudinal study*. Cambridge university press.

Moser, A., Kruegel, C., & Kirda, E. (2007). Limits of static analysis for malware detection. In *Twenty-third annual computer security applications conference (ACSAC 2007)* (pp. 421–430). IEEE.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery*. London: Routledge.

Patchin, J. W., & Hinduja, S. (2013). Cyberbullying among adolescents: Implications for empirical research. *Journal of Adolescent Health, 53*(4), 431–432.

Piquero, A. R., Farrington, D. P., & Blumstein, A. (2007). *Key issues in criminal career research: New analyses of the cambridge Study in delinquent development*. Cambridge University Press.

Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*(3), 245–268.

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2020). The digitized opportunity structure of street offending. *British Journal of Criminology, 61*(4), 926–945. https://doi.org/10.1093/bjc/azaa091

Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Greenwood Publishing Group Inc.

Steinmetz, K. F. (2015). Craft (y) nessAn ethnographic study of hacking. *The British Journal of Criminology, 55*(1), 125–145.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). New York: Polity.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40–55.

Wiesner, M., Yoerger, K., & Capaldi, D. M. (2018). Patterns and correlates of offender versatility and specialization across a 23-year span for at-risk young men. *Victims and Offenders, 13*(1), 28–47.

Williams, R. K., & Arnold, B. L. (2002). Offense specialization among serious habitual juvenile offenders in a Canadian city during the early stages of criminal careers. *International Criminal Justice Review, 12*(1), 1–21.

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). *Delinquency in a birth cohort*. Chicago, IL: University of Chicago.

Wright, R. T., & Decker, S. H. (1994). *Burglars on the job: Streetlife and residential break-ins*. UPNE.

Wright, R. T., & Decker, S. H. (1997). *Armed robbers in action: Stickups and street culture*.

Youngs, D., Ioannou, M., & Eagles, J. (2016). Expressive and instrumental offending reconciling the paradox of specialisation and versatility. *International Journal of Offender Therapy and Comparative Criminology, 60*(4), 397–422.

Youngs, D. E., & Canter, D. V. (2012). When is an Offender not a Criminal: A Comparison of the self report offending of convicted and non convicted respondents. *Psychology, Crime & Law*.