Trends in Organized Crime
https://doi.org/10.1007/s12117-022-09476-9

Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions

Jonathan Lusthaus[1] · Edward Kleemans[5] · Rutger Leukfeldt[3] · Michael Levi[2] · Thomas Holt[4]

Accepted: 26 November 2022

Abstract
This article examines the network structure, criminal cooperation, and external interactions of cybercriminal networks. Its contribution is empirical and inductive. The core of this study involved carrying out 10 case analyses on closed cybercrime investigations – all with financial motivations on the part of the offenders - in the UK and beyond. Each analysis involved investigator interview and access to unpublished law enforcement files. The comparison of these cases resulted in a wide range of findings on these cybercriminal networks, including: a common division between the scam/attack components and the money components; the presence of offline/local elements; a broad, and sometimes blurred, spectrum of cybercriminal behaviour and organisation. An overarching theme across the cases that we observe is that cybercriminal business models are relatively stable.

✉ Jonathan Lusthaus
jonathan.lusthaus@sociology.ox.ac.uk

Edward Kleemans
e.r.kleemans@vu.nl

Rutger Leukfeldt
rleukfeldt@nscr.nl

Michael Levi
levi@cardiff.ac.uk

Thomas Holt
holtt@msu.edu

[1] University of Oxford, Oxford, UK

[2] Cardiff University, Cardiff, UK

[3] NSCR, The Hague University of Applied Sciences, Amsterdam, Netherlands

[4] Michigan State University, Michigan, United States

[5] Vrije Universiteit Amsterdam, Amsterdam, Netherlands

Published online: 03 February 2023

Introduction

Over the last two decades, researchers have considered the ways in which cybercriminal networks organize, how they operate, and the ways they interact with their environments. This is a complex set of questions to address, as cybercriminals hide their illegal activities in various ways, both technologically and socially. Researchers have engaged with a variety of methodological approaches, including studies centred on interviewing offenders and/or investigators (Hutchings and Clayton, 2016; Lusthaus, 2012, 2018); victim surveys (Williams et al., 2019); the use of data from cybercriminal marketplaces and forums by way of both qualitative and quantitative analysis (Decary-Hetu & Dupont, 2012; Dupont et al., 2017; Dupont and Lusthaus, 2021; Holt, 2013; Holt and Dupont, 2019); and employing machine learning and other data science techniques to engage with even larger amounts of data from these cybercriminal settings (Pastrana et al. 2018).

Each of these approaches provides insights into offender practices on- and off-line. There is, however, also benefit in using data from law enforcement investigations to better understand the structural and social dynamics behind criminal networks. Wiretaps and other police data have been used to study Russian mafia groups (Varese, 2001), Nigerian human traffickers (Campana, 2016), and a considerable number of criminal networks within the Netherlands (e.g., Kleemans & van de Bunt, 1999; Kleemans & de Poot, 2008; Roks et al., 2021; Leukfeldt et al., 2017a). Building on this tradition, some initial work has engaged with police data on cybercriminal cases, particularly in the Netherlands (Leukfeldt et al., 2017b; Leukfeldt et al., 2019). As Leukfeldt and Kleemans (2021) argue, in-depth police investigations can be a very useful extra tool for cybercrime researchers: "these investigations provide a unique insight into cybercriminal networks and their members because of the use of intrusive investigation methods, such as wiretaps, IP taps, observations, undercover policing, and house searches" (Leukfeldt & Kleemans, 2021, p. 128).

Compared with the organized crime literature, only a relatively small number of cybercriminal cases have been studied through the use of law enforcement data, and there is much scope to expand this endeavour. This article adds to the literature by analysing 10 cybercriminal networks that were active in the UK and beyond. As the project funder was a UK government department, this helped facilitate initial introductions and conversations with law enforcement representatives in order to gain access to closed police files, which provided valuable detail not present in the public domain. This also allowed wider access to investigators for interview. The focus of this data collection was to study the business models of cybercriminal groups, with the goal of illustrating different group structures. This helps move the discussion of cybercriminal organisations from generalities to a richer micro-level understanding.

The key aim of this paper is to provide an overview of the cases that have been collected and to use this rich dataset to provide insights on cybercriminal networks, adding to what is already known in the literature. As such, our contribution is empirical and inductive. This article is organized as follows. First, we provide a review of the existing literature on cybercriminal networks, and highlight key points that have already been developed. Second, we summarise the data and methods that we employed. Third, we outline the key details of the ten cybercrime cases that comprise this project. Fourth, we provide the main findings, before proceeding to the final discussion section.

Cybercriminal networks: a brief review

It is important to briefly review existing knowledge on cybercriminal networks, to assess what can be confirmed, challenged or expanded by these new case studies. We organize this review around the three key themes that emerge from the literature: Network Structure: Criminal Cooperation; and External Interactions. We later use these same three topics to analyse the 10 cases we collected, to determine what insights can be added through this data.

Network structure

The online environment of the Internet is well suited to supporting decentralized, criminal networks, which are somewhat flat and loose in their structure. Numerous studies indicate that cybercriminals use online meeting places, like forums and marketplaces, to meet co-offenders that can provide a variety of illicit goods and services (for example, Decary-Hétu & Dupont, 2012; Decary-Hétu et al., 2012; Dupont et al., 2016; Holt & Lampke, 2010; Holt, 2013; Holt & Smirnova, 2014; Lu et al., 2010; Lusthaus, 2012; Motoyama et al., 2013; Peretti, 2008; Soudijn and Monsma, 2012; Yip et al. 2012). Some offenders operate largely within these online networks, where they are known only by nicknames. Some scholars argue that with a range of goods/services on offer within large online marketplaces and elsewhere, it may be easier to locate partners than in offline settings (Dupont et al., 2016; Franklin et al. 2007; Holt et al., 2015; Holt and Lampke, 2010; Holt and Smirnova, 2014; Leukfeldt, 2014; Lusthaus, 2012; Soudijn & Zegers, 2012; Wehinger 2011; Yip et al., 2013). It also may be easier to replace partners that are lost to arrest or other elements. With that said, there is also evidence of cybercriminals seeking to work with the same partners across long periods of time, which perhaps offers some greater degree of certainty and mitigates (though not eliminates) much of the risk of covert agents or police informants (Bulanova-Hristova et al., 2016; Holt, 2013; Leukfeldt et al., 2017b/d; Lusthaus 2018). These competing drivers need not be mutually exclusive, in that cybercriminals may find co-offenders in open settings and then proceed to work with them for as long as possible.

Despite a significant part of the literature focussing on online network structures, some scholars have identified other cybercriminal networks, which are not decentralised, loose, and (primarily) online. Some of these networks more closely resemble conventional criminal networks (Bulanova-Hristova et al., 2016; Kruisbergen et al., 2018; Leukfeldt et al., 2017a/b/d; Leukfeldt et al., 2019; Lusthaus et al., 2022; Odinot et al., 2017; Werner & Korsell, 2016). For instance, some networks consist of offenders who are known to each other in person and, in some cases, may have known each other for long periods of time (Lusthaus 2018; Nguyen and Luong, 2021).

Some of these networks are more hierarchical and stable than the looser online networks. All the networks studied by Leukfeldt et al. (2017a/b/d) have clear levels of authority, most notably core members who coordinate the network, and those they recruit to provide particular cybercriminal services for the criminal enterprise (which can occur through online meeting places). A portion of the core groups within cybercriminal networks may even include dense structures which might be considered criminal "firms" (Lusthaus 2018, p.66; Lusthaus et al., 2022). Some of this density may be due to relatively low police efforts against cybercrimes in certain countries.

Criminal cooperation

If the focus is on online networks, there are a number of barriers to cooperation facing cybercriminals, including difficulties in accurately determining identity and limits to enforcement of agreements, especially in the use of physical violence (Lusthaus 2018; Dupont and Lusthaus, 2021). Existing research has uncovered some ways that cybercriminals address these challenges in online networks. For instance, for closed forums, potential members are vetted in various ways, such as being vouched for by existing members or by providing evidence, such as stolen credit card data, to demonstrate that they are active in cybercrime (Ablon et al. 2014; Dupont et al., 2017; Holt et al., 2015; Lusthaus, 2012; Soudijn & Zegers, 2012; Yip et al., 2013). Many forums have a review system, where members who have purchased data, tools or services, assess the vendor by means of a written review or a score on a rating scale (Ablon et al. 2014; Chu et al. 2010; Décary-Hétu & Dupont, 2012; Dupont et al., 2016; Herley and Florencio 2009; Holt, 2013; Holt & Smirnova, 2014; Holt et al., 2015; Lusthaus, 2012; Soudijn & Zegers, 2012; Wehinger 2011; Yip et al., 2013). Finally, Dupont and Lusthaus (2021) examine the arbitration system within the Darkode marketplace, which provides an avenue for enforcement in a digital setting.

But the mere presence of these components does not mean that they foster successful cooperation. For instance, review systems do not always work well (Décary-Hétu & Dupont, 2012; Dupont et al., 2016; Holt et al., 2015). An analysis of Darkode by Dupont et al. (2017) indicates that numerous users gained access to this 'exclusive' marketplace, despite not having the requisite technical skillset. There may be a desire to balance the need for new blood with the demand for exclusivity. The same is true for arbitration systems, which provide some value but are limited in many ways (Dupont & Lusthaus, 2021; Holt, 2013; Holt et al., 2015).

Given that online cooperation is sub-optimal, it is not surprising that some cybercriminals explore offline modes of cooperation, as well. As noted, studies show that cybercriminals draw on both online and/or offline social networks (Bulanova-Hristova et al., 2016; Leukfeldt, 2014; Leukfeldt et al., 2017a/c/d; 2019; Lusthaus 2018; Lusthaus et al., 2022; Odinot et al., 2017). In offline networks, friends, family and long-term acquaintances might co-offend together, in a similar way to conventional crime. A related aspect is that cooperation is not only offline, but also local in many respects. Leukfeldt et al. (2017b/d) show that phishing and malware attacks on payment transactions are locally embedded. As Lusthaus and Varese (2017, p. 1) argue: "The economic and social dynamics of different settings are likely to influence who gets involved in cybercrime, what types of cybercrime they carry out and the way they are organized".

External interactions

It is important to distinguish between "underworld" elements of a network and other "upperworld" components, which are external to the cybercriminal economy. There are those from legitimate industries and organisations, such as bank employees, that knowingly aid cybercriminal networks in some way. Some term these "recruited facilitators" (see, for example, Leukfeldt et al., 2017a-d). This also links with the concept of corruption and the role that public sector employees may play within cybercrime. High levels of corruption are seen across a number of jurisdictions, including Nigeria, Southeast Asia and the former Soviet Union (Lusthaus 2018), which sees "corrupt state agents act as protectors of cybercriminals by neglecting to arrest the relevant offenders, tipping them off about upcoming operations against them, and even intervening after arrests have been made" (Lusthaus 2018; p.181). There may be political considerations driving aspects of this behaviour, as well.

There are also external interactions with legitimate components that may unknowingly support cybercriminal operations. Along with using bulletproof hosting, cybercriminals also abuse legitimate hosting services to gain access to, for instance, servers (Hutchings & Clayton, 2016; Odinot et al., 2017; Bijlenga & Kleemans, 2018). Other legitimate services which are abused, include: online advertising to carry out malware infections; ecommerce sites where cybercriminals use stolen funds to purchase goods/services; financial infrastructure such as virtual currencies and cryptocurrencies (Odinot et al., 2017; Leukfeldt et al., 2017a/b/c/d). There are also numerous IT tools which are "neutral" but can be deployed for criminal purposes. Access to tools may be legally available or purchased illicitly online. Other tools might be created or modified by individuals or companies without a clear idea of the eventual criminal purpose (Bijlenga and Kleemans, 2018). More broadly, lawyers and other professionals might enable financial crimes in various ways (Levi, 2022).

Data and methods

The core of this study involved carrying out 10 case debriefs on closed cybercrime investigations in the UK and beyond. These were chosen based on a number of key characteristics. Two critical factors were that the cases selected involved financial motivations on the part of the offenders, and had at least partly gone through the judicial system with clear information on the offenders and their operations available. Initial case collection began in late 2019. Each case analysis was built on an interview with one or more investigators, access to police/legal files, and also the incorporation of any relevant/reliable public source or other information. While law enforcement terminology refers to "operations" or, more informally, "jobs", these case analyses are focussed on criminal networks engaged with a specific enterprise.

The approach that was adopted was strongly influenced by the Dutch Organized Crime Monitor, which has been operating in the Netherlands over a number of decades (for more information, see Kleemans 2015). But some variations were made to this project to account for both the nature of cybercrime and also the specificity of collecting this data in the UK context, where there is not as strong a tradition for data sharing by law enforcement for academic purposes. To aid us in these efforts, we conducted workshops with experienced stakeholders in Amsterdam, London and Pittsburgh, as well as a number of other ad hoc discussions in the UK and beyond.

Legal files were obtained for all 10 chosen cases. Depending on the case in question, these included: prosecutor's opening notes, MG5s (case summaries for prosecution), MG3s (reports for charging), jury bundles and assorted other documents of relevance. Each case analysis drew on different types of documents, depending on which contained the richest information. In some instances, particular documents did not exist. For instance, if an offender pleaded guilty before court proceedings took place, there is unlikely to be an opening note or jury bundle unless it was a last-minute plea. In other cases, certain documents couldn't always be located. Finally, there were stylistic choices made by officers and prosecutors, which dictated, for example, whether an opening note and MG5 were similar or vastly different, or whether an MG3 was likely to contain more useful detail than a "bare bones" MG5.

Each case analysis began with an interview of at least one key investigator involved in the case. Discussions took place with the relevant points of contact, and the most suitable participant(s) was identified based on knowledge, availability and interest. The investigator interviews served two purposes. First, it provided a good introduction to, and overview, of the case. Second, investigators would identify which files/documents would be most useful in the case, and either provide access to them, or advise how to find them.

Data analysis took place using a checklist, which was standard across all cases (see Appendix). The checklist was adapted for use on cybercrime cases from those templates previously used for the Dutch Organised Crime Monitor. It surveys the core elements of how each business model works, while also adding new components that address how common or unusual this model is and how the model might change over time. This gave some comparative and predictive power to a project that was built on analysis of a small number of closed cases.

There was a balance between complying with privacy regulations and ethical considerations, while also producing case studies with as much information as possible. The data was scrubbed of identifying or sensitive information by the Principal Investigator, and sorted under the various checklist headings. Given the UK context, and that this was the first time this data collection has been conducted, strict emphasis was placed on removing identifiers to the cases and individuals within them. As a result, certain elements of the original Dutch checklist regarding offenders and their identifying information had to be removed.

Case selection

Case selection was based on some key principles:

1. Only financially motivated and serious offences, which involve substantial sums of money being sought (even if some individual victim losses may be small).

2. A connection to major/common cybercrime case "types"[1] the research team identified.
3. Cases where at least some offenders have been prosecuted.

We also saw value in strategic sampling criteria, including:

4. A preference for (larger) groups, though we also allowed for lone offenders if the offence was very serious and well linked to the broader underground economy.
5. We also had a preference for cases with international links (and the possible extra data layers therein), though we include more local cases too.

Cases were excluded if:

a) They were primarily centred on insiders rather than "professional" cybercriminals.
b) The criminal activity was largely tied to competition between otherwise legitimate businesses.
c) Child sexual offences were present within the case (this was both for subject matter reasons, along with raising complex questions around ethics and risk).

By reviewing resources like the Cambridge Computer Crime Database, along with media articles, and by relying on existing knowledge, we developed a list of possible cases that met these criteria. The original intention was to present these possible cases to the relevant agencies, along with allowing for the possibility that they would suggest some of their own examples.

The final selection was weighted evenly in this regard, with five cases suggested by law enforcement participants, four by the PI, and one that was suggested by both sides. While these cases also reflected a good cross-section of different types of cybercrime operations, there was not one case for each "type" that had been conceptualised in advance. Suitable cases could not be identified or accessed for all categories, and there were also attempts to include some similar matched cases, which would allow points of comparison. In the opposite direction, some single cases met multiple categories.

While the Dutch Organised Crime Monitor model involves substantially more cases for a wider range of criminal activity, our approach saw 10 cases as the ideal number for the length/resources of this project. Stakeholders in the UK expressed a strong preference for richness of detail within case studies. While some comparative power might be lost, the core interest was in the precise micro-level mechanics of how certain cybercriminal groups function. This figure was appropriate for practical reasons as well: a smaller number of cases allowed a deeper engagement with the ad hoc UK data collection process that was required. As a result, even though the sample

[1] (1) A malware developer group; (2) A group that exploits malware (e.g. ransomware); (3) An online auction fraud group; (4) A business email compromise group; (5) A phishing scheme group; (6) A money mule network (connected to cybercrime); (7) A money laundering group (connected to cybercrime); (8) A leading cybercriminal marketplace (and particularly the group behind running the forum); (9) A group running an online cybercrime shop; (10) A cybercrime case involving a traditional organised crime group (e.g. a mafia or a drug gang).

was designed to reflect a cross-section of cybercriminal activity, the cases should not be viewed as representative of all UK cases. In fact, some of the cases were chosen due to their significance, size or focus, and were not typical of many investigations (even if they might be typical of other cybercriminal networks which have not been prosecuted).

Case summaries

This section provides a short summary of each case that was analysed for this project, with a particular emphasis on the nature of their business models. Cases are identified by letters A-J, and are listed in the order in which the data was collected. In the next section, this summary is followed by a comparative analysis across the cases and the three key themes: network structure; criminal cooperation; external interactions.

Case A

This case centred on a data breach of a large company. A vulnerability was discovered by a hacker and published online in forums. This led to the company being targeted by a group of hackers, including the original finder of the vulnerability. Initially, a nation state actor was suspected. But once it was established no state was involved, the case was passed down to the cybercrime unit that completed the investigation. This took years before resolution, involving up to 10 attackers, not all of whom were prosecuted. The business model involved was extortion. Seemingly acting alone, one of the offenders contacted the company threatening to leak their compromised data, unless a bitcoin payment was made. There was also evidence that this offender separately had attempted to extort a large number of other companies around the world. Despite the apparent seriousness of the offences, the criminal network itself was relatively low-level and unprofessional, especially when compared to the other cases within this study.

Case B

This case concerned a criminal network that was engaged with a banking Trojan. This is a specific type of malware that targets online bank accounts, and which is distributed in various forms that on their face appear legitimate. For instance, they may rely on people to click on a link that has been included in an email. There are five key components of this business model: (1) Code and manage the malware; (2) Infect computers with malware; (3) Obtain bank account passwords and other security information; (4) Transfer funds out of these accounts and into mule accounts; (5) Return the proceeds net of intermediary costs back to the fraud organisers. In this investigation, the malware itself originated in the former Soviet Union, but many of the targets were bank accounts in the UK and elsewhere. The money mule group at the centre of this case was based in the UK, but some of the offenders were also Russian speakers with Eastern European backgrounds.

Case C

This multi-year investigation began with a credential stuffing[2] attack against an online company. It focussed on a vendor, who was very active on a number of dark web marketplaces. He made many sales of personal financial information like credit card details, banking information, online accounts and cannabis. It is estimated that the receipts from these sales were worth over £50,000 at the time. This offender used multiple means to obtain the data and accounts he was selling, including phishing sites, emails, smishing (text phishing) and credential stuffing. While he was the primary offender and operated relatively independently, he also drew on a loose online network of associates, along with his own family members who assisted with "cashing out".

Case D

This was also a banking Trojan operation, but the investigation into this criminal network predated Case B by around half a decade. The operations of these networks were also roughly half a decade apart. In Case D, the structure of the banking Trojan network was strikingly similar to the one that followed in Case B. Part of the network was responsible for coding the malware and compromising bank accounts; the other part of the network was responsible for the money side of the business. Both elements were predominantly Eastern European, with those in charge of the money components either resident or sometime resident in the UK.

Case E

This case was focussed on online auction fraud. This scam involves two key components: (1) the manipulation of the buyers online so they will transfer funds into a bank account the criminals control; (2) the opening of bank accounts in victim countries so they can receive the funds and the setting up of a system for returning the profits to the scam organisers. This case provided a rare detailed analysis of the business model of a Romanian group, based in the UK, which was involved in this type of fraud. The members of the criminal network in this case employed an approach that has been widely used both before them, and after them. In simple terms, this involved the online sale of products (such as cars), but which do not actually exist, to unwitting victims. The advertised products listed by the vendor were purchased by the consumer, but never delivered. The group in this case made use of sites like eBay and Gumtree to post "bogus" ads. They also leveraged payment procedures masquerading as PayPal, to socially engineer victims into transferring funds into bank accounts controlled by the criminal network. These accounts were opened using false ID documents.

[2] Credential stuffing involves "firing" long lists of usernames/passwords at a website, hoping to get a positive response for certain combinations. This is not only useful for that website, but also for other sites or accounts, as people often reuse passwords.

Case F

This case concerned another coordinated group of offenders from Romania. It was one of a series of contemporaneous cases in multiple jurisdictions involving the same organisers and the same business model of using malware to compromise ATMs. They targeted a particular type of ATM machine with known vulnerabilities: each used the same key to physically open the back of the unit; the machines then could be rebooted from an external device such as a CD, which contained the malware. Once the malware was deployed, the group could instruct the ATM to release all the funds held inside it. By targeting over 50 ATMs around the UK alone, in one short window, they stole over £1 million.

Case G

This case concerned a Remote Access Trojan (RAT), which can be used to access a victim's computer and browse files, take screenshots, access computer cameras, and/or log keystrokes to steal passwords. This RAT was used in almost 100 countries by multiple offenders against countless victims. The core of this investigation centred on the malware developer, who was based overseas, along with a number of UK offenders who made use of this RAT to commit a wide range of offences. The investigation began after a cyberattack on a school network, in which the RAT was discovered on one of the offender's computers. It became clear that the RAT had been used for numerous attacks, and was being marketed on a well-known publicly accessible hacker forum, as well as through a website. The RAT had an online network of users who provided customer support for its buyers.

Case H

The core business model of this case was centred on extortion through ransomware. This case involved leading Russian speaking cybercriminals, who were based overseas. A key part of this operation was to infect users with the ransomware so that this extortion could take place. The UK based offender at the heart of this investigation played an important role for this group in spreading the malware though (semi-) legitimate online advertising companies – a process known as malvertising. This offender's focus was renting ad space on pornography sites from brokers. When a user clicked on one of the ads in question, instead of being directed to the new site/content, they would be infected with ransomware, and be told to pay a "fine" to unlock their computer. A money laundering network was also required to deal with these proceeds.

Case I

This case was investigated by a cybercrime unit, tasked with major hi-tech crimes. It involved advance fee fraud, also known as 419 scams, which have many forms all involving the payment of "fees" to unlock a larger amount of money that has been promised. The specific form it took in this case was a lottery scam. The offenders sent out forged paper letters to victims, who were primarily based in the United States notifying them of a lottery win. The letter requested an administrative fee of a few hundred dollars. The letter was followed by emails and phone calls. If this initial payment was made, the fraudsters would make follow up payment requests. Nigerian offenders have a traditional association with this form of fraud (s. 419 of the Nigerian Criminal Code), and the offenders in this case were Nigerian, but based in the UK. There was also evidence of certain group members using computer forums and marketplaces to engage with more technical offenders.

Case J

This was a business email compromise investigation (BEC). These scams involve impersonating business professionals to dupe victim companies into paying invoices into accounts controlled by the offenders. The offenders in this case were also Nigerians based in the UK. The network was split between two components: (1) the fraudsters who duped the victims; (2) the money mule network which received the transfers from the victims and then redistributed the proceeds among the offenders. The second component was similar to money mule networks observed in some of the other cases. The first component required a phishing operation to gain access to email accounts and passwords. Business accounts were then selected from these lists to carry out the BEC scam.

Empirical results

Network structure

There was a range of network structures present across these 10 cases. Given the selection criteria, there was an inbuilt bias towards cases that involved multiple offenders. But there were still investigations that were focused on one or a relatively small number of offenders, even if a broader network of actors was involved (e.g. Case A, C, G, H). The cases could be broadly categorised into those which had looser more open networks, characterised by relatively weak ties, and those with tighter more closed networks, with some strong ties and clusters present.

Case A was a good example of a loose network of at least 10 members. Most of the offenders were hackers under the age of 18, and they engaged in chat groups on, for example, Skype. They were collaborative in nature, without a formal hierarchy, and were experimenting with hacking. They might come together for specific hacks, such as the data breach within this case. Only one member of this network seemed to be strongly focussed on financial gain and directly engaged in the extortion, as well as attempting to sell data, which increased the seriousness of the overall network's activities, and increased the exposure of its members to prosecution. This individual was relatively peripheral to the core of the network, who were focussed on recreational hacking and breaches, rather than blackmail. He was also quite unsuccessful in his commercial efforts.

Another loose network was observed in Case G. The author of the RAT was making considerable sums of money by selling the tool, and was strongly central to the network. But most others in the network were not monetarily profiting from the tool. Below the author, sat almost 20 people who offered buyers customer support across different time-zones and languages; these individuals did not appear to profit directly from the business. They may instead have provided this service to increase their reputation within the hacking forum, or to build a closer relationship with the author.

In all the other cases, most of the offenders sought profit and the networks were often more closed, or at least had some closed groupings within them. The networks were characterised by much more professional, and often older, offenders. But what is important to note is that the cases did not centre entirely around one single group which was completely self-sufficient. Many of the cases often included several individuals and groups linked together. Some of these connections were short-lived and transactional, but others were much longer-term partnerships. Such partnerships often appeared between the organisers of each cybercrime scheme and their cashing out providers, which operated as distinct but allied groups.

Cases B and D both involved banking Trojans, and some elite cybercriminals. But together with the more technical individuals who were part of a relatively closed group, each worked with a money mule network based in the UK. A similar organiser/cashing out division characterised many of the other cases too. This was regardless of whether they involved Russian speaking cybercriminals (Case B and D), Romanian fraudsters (Case E), or Nigerian scammers (Case I and J). Meanwhile, for Case H, the key subject of the investigation outsourced some of his money laundering needs, but the financial structure of the broader network was not clear. For Case C, the key offender was effectively a "sole trader", who drew on others as freelancers where needed, and handled much of his sales in bitcoin. He didn't require an extensive cashing out operation beyond members of his own family and a small number of contacts. Finally, Case F offered an unusual situation in that the "cyber-attack" was carried out in person against each ATM, which meant that the intrusion and the removal of funds happened at the same time and place, and was carried out by the same actors.

Criminal Cooperation

Criminal cooperation differed greatly between the lower-level forms of cybercrime found in Case A and G, and the more serious forms of offending observed in the other cases. In these former cases, cooperation occurred largely online. Because the offender in Case C was primarily a vendor on Dark Web markets, many of his interactions were online, with the exception of the family members he had included in his criminal activities. In Case H, there were suggestions that the Russian speaking components of the network may have had strong offline ties, including one cluster that effectively took the form of a technology firm within an office setting. But the main UK based offender only dealt with his overseas partners through virtual means.

While not all network elements were known, across Cases B, D, E, F, H, I, J there were significant offline components. The Nigerian offenders in Cases I and J were in regular social contact with one another, even though many of them conducted their scams somewhat autonomously. Some of the Romanian offenders in Cases E and F

Table 1 Profits/Victim Losses within Cases

Case	Profits/Victim Losses (£)	Source
A	0	Investigator Interview
B	Over 2 million	Investigator Interview
C	Over 50,000/ Almost 1 million	Case Files/ Investigator Interview
D	Over 2 million	Investigator Interview
E	Almost 3 million	Investigator Interview & Case Files
F	Over 1 million	Investigator Interview & Case Files
G	100,000s	Case Files
H	100,000s	Case Files
I	Unclear	N/A
J	Over 500,000	Case Files

had to operate in physical proximity to each other as they dealt with the proceeds of the crimes. This was also the case for the cash out groups in Cases B and D, even if less is known about the nature of ties for the organisers in Eastern Europe.

There was also an important national/regional dimension in certain investigations. Cases B and D both largely concerned Eastern European offenders. Cases E and F involved Romanian offenders, while Cases I and J were almost entirely characterised by Nigerian offenders. In Case H, an investigator was surprised that a British offender with no language, cultural or national ties to Eastern Europe had made his way so far into a leading cybercrime network from that region. This was rare when compared to other investigations he had been involved in. All of these elements suggest that national/regional ties may play an important role in increasing trust (and perhaps enforceability) within these networks.

There were different internal regulatory and enforcement mechanisms used by the offenders to manage relationships across the cases. Payment played an important role in cooperation and getting partners to comply (with the exception of Cases A and G). This was often also tied to monitoring, so that if a partner was not providing what they were meant to, payment might be withheld. In Case J, an investigator suggested that there was considerable evidence in the case due to the network meticulously keeping track of frauds and money movements through screenshots, which could serve as proof to collaborators that a particular action had been executed. This is likely because they did not trust each other. But it illustrates the paradox facing many of these cybercriminals: recording criminal acts may aid in cooperation, but then also evidentially exposes offenders to prosecution.

The amounts of money involved varied widely between the cases. In Case A, no real money was involved, as the extortion and data sale attempts failed. At the other extreme, in cases involving professional overseas cybercriminals, millions of pounds/dollars were being handled by the respective criminal networks (e.g., Cases B, D, E, F, H, I, J), even if it was more difficult to determine the precise division of profits in certain instances. Table 1 summarises some of the profits/victim losses involved, though it should be noted that different investigations calculate these figures in different ways. They also reflect the profits/victim losses linked to particular offenders or particular parts of a broader network that were being prosecuted in the UK, and for a period of criminal activity which was the subject of investigation. As some of these criminal networks operated over long periods of time, had operations and targets in multiple countries, as well as a variety of cells carrying out criminal activity somewhat autonomously, these figures do not capture the complete story.

The cases with offline elements had stronger enforcement mechanisms available to the cybercriminals involved. In Case A, there was little data on serious disputes or how they were resolved. In Case C, the central offender was known to make threats online, but there was no evidence he ever attacked anyone either virtually or physically. The same applied to Case H. But in Case J, the leader of the money muling network was a convicted criminal, with a previous background in the gang scene. There was never clear evidence of violence during the investigation, but there were strong suggestions of coercive control based on this individual's reputation and actions. There were also suggestions of physical threats and coercion in, for example, Case E.

External interactions

The involvement of non-criminal elements within these cases varied widely, but followed a similar pattern, in that the more professional and serious cybercriminal networks relied on these elements more. In an example like Case A, there was limited evidence of companies, government officials or insiders being involved. In Case C, the key offender required server space and domain registration, which he sourced from major technology companies. While there was no suggestion of direct corruption on the part of these companies, their policies allowed relatively long periods of time before phishing sites were taken down, even when payment for hosting costs was made with stolen credit cards.

In other cases, suspicions of corruption were much stronger. In Case I, one offender received aid from a lawyer in Nigeria, who fraudulently managed the proceeds of crime in a property transaction. There were also questions around UK bank branches which were used for cashing out. But it appeared to be more weaknesses in systems rather than there being clear evidence of insiders. A similar configuration was observed in Case J, where both a lawyer and accountant in the UK were supporting fringe aspects of the criminal activity. In this case, an investigator also suspected there may have been corrupt employees working inside banks, but did not have firm evidence to support this belief and the investigation process was too complex to engage with this line of inquiry.

Most cases did not provide enough detail on foreign jurisdictions to determine if corrupt law enforcement agents or government officials were protecting overseas members of some of these criminal networks. Cases D and E were the exception. In Case E, there was no presented evidence that the group had assistance from insiders or others within banks or other legitimate organisations. The investigator interview revealed that this was a line of inquiry within the law enforcement investigation, but no suspects were found within the bank branches who were being bribed or otherwise compromised. It is more likely that the broader network had external assistance within Romania on the cyber facet of the operation. During their collaboration with UK authorities, Romanian law enforcement had indicated the possibility that the criminal network had infiltrated the Romanian police, and that there may be corrup-

Table 2 Summary of Cases

Case	Presence of Tight Cluster(s)	Presence of Secondary (non-financial) Motivation	Presence of Offline/Local Dimension	Presence of Foreign Offenders Based in UK	Indicators of Corruption
A (Breach)	No	Yes	No	No	No
B (Malware)	Yes	No	Yes	Yes	No
C (Vendor)	No	No	Yes	No	No
D (Malware)	Yes	No	Yes	Yes	Yes
E (Auction Fraud)	Yes	No	Yes	Yes	Yes
F (ATM)	Yes	No	Yes	Yes	No
G (RAT)	No	Yes	No	No	No
H (Ransomware)	Yes	No	No	No	No
I (AFF)	Yes	No	Yes	Yes	Yes
J (BEC)	Yes	No	No	Yes	Yes

tion at a high level of the investigation (which is in line with some existing research on Romanian cybercrime: Lusthaus & Varese, 2017). It is possible that some of the value of the UK investigation was to provide an independent source of investigation on the criminal network.

For Case D, considerable time was spent looking into leads in the former Soviet Union, including engagement with authorities in the region and travel there by UK officers. This gave further insights into the context of the offenders based there, and specifically the role of law enforcement and others with political influence. But much of this information had to be reconstructed through investigator interviews. There were a number of malware group members who were suggested to have connections to senior political figures, in more than one country. In one instance, there was evidence that a group member was in the social circle of a leading politician's son. In another, one of the group may have been exchanging work for the government in return for protection for his criminal activities. Aside from formal protective arrangements, there were occasions where law enforcement agents preyed on the group. The theft of one of the cash shipments was an example. But there was also an example of a shakedown of at least one member of the malware group, where money was stolen on site and then no arrests made.

Summary of case features

Table 2 summarises the key features of each case analysis. It is important to note that this can only capture the information uncovered by the investigations, and not the complete cybercriminal networks.

As a visual summary, we attempted to capture as many of these cases as possible within two sociograms. These are very similar to each other, indicating that the overall structure of many groups studied in this project may be quite similar. The two figures account for the larger and more professional cybercriminal networks, in relation to both fraud (Fig. 1) and malware (Fig. 2).

Cases E, I and J fall within the fraud structure of Fig. 1, while Cases B, D and H fall under the malware structure of Fig. 2. We can see from these figures that the money

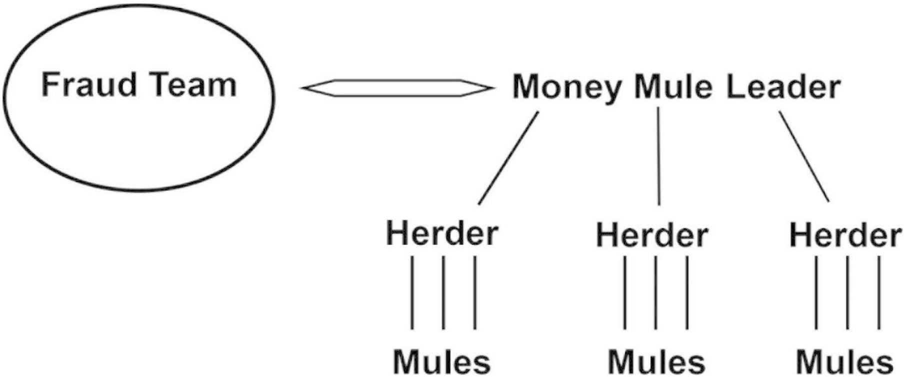

Fig. 1 Fraud Networks

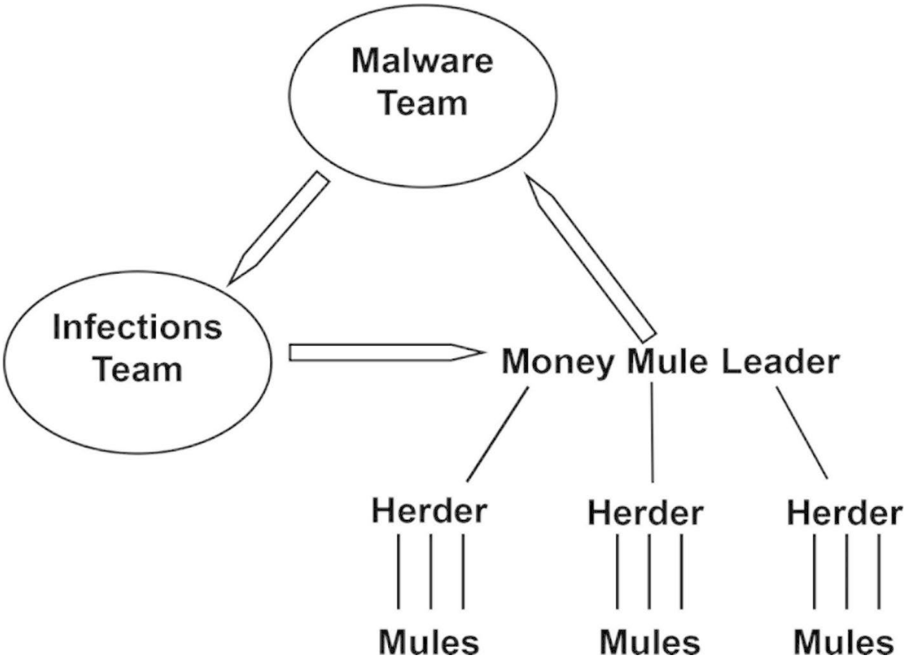

Fig. 2 Malware Networks

mule structure is hierarchical and consistent across different forms of cybercrime. Across the two figures, the fraud teams and infections teams play similar roles, in that they are directly responsible for squeezing the money out of the victims and directing it to the money mule team. It is the technical component of the malware cases which introduces the major difference between these networks. This is the presence of an additional team, which is responsible for creating and managing the malware.

An overarching theme across the cases is that we observe that cybercriminal business models are relatively stable. While the technology may change rapidly, the human and organisational structures behind the cybercrime schemes remain more entrenched. Most cases within this project showed relatively stable business models that persisted for a number of years. There was a common evolution in particular tactics used, but the overall modus operandi and group structures were surprisingly constant. This was certainly true for Cases B, D and E. Such stability was also observed in some of the other cases. For instance, in Case G several similar RATs had existed before this case, and they continued to exist after this case. Each time one RAT developer was taken out, buyers simply moved to the next one. There was some evolution in the code, with new developers adapting elements from past RATs, but the business model remained largely unchanged. Meanwhile, in Case J, there were constant adaptations to match changes in bank payment thresholds and other practical details. BEC scammers now also have to get around security innovations like double authentication for account payment changes. But the core of the business model continues very successfully. Case C indicated that the virtual marketplace scene is subject to some disruptions and evolutions, but in some sense it is cyclical: larger marketplaces may fall out of fashion after major law enforcement operations, but then they may return again at another point in the future.

Discussion and conclusion

Based on unique data from cybercrime investigations in the UK, this article explores how cybercriminal networks are organized, how cybercriminals operate, and how they interact with their environment. There were a number of key findings resulting from the comparison of these cases, which build on the findings of prior researchers, whether using police data or other sources.

First, in many cases there was a clear division between the components of the network that organised the scam or attack, and those that were responsible for engaging directly with the proceeds and returning them back to the organisers (Lusthaus 2018; Lusthaus et al., 2022). The presence of cashing out groups in the UK and other Western countries is likely to be relatively common, while the organisers may be in overseas locations. There also seemed to be clear similarities in the ways these cashing out groups were organised regardless of which business model they were used in. This suggests a potential, if it is not already occurring, that these groups may serve different cybercrime operations, rather than being tied only to one business model.

Second, the division between overseas organisers and the UK-based money component presents a major challenge for police and their ability to penetrate these cybercriminal networks in a meaningful way. The money component is susceptible to traditional policing methods, with key arrests made against not only mules, but also senior mule leaders. But the overseas organising component, for both fraud and malware cases, is much harder to target with traditional law enforcement methods. This is because the offenders reside in foreign countries, which presents the well-known challenges of international cooperation and also local corruption potentially shielding these individuals. Some cases provided a little hope for conventional policing against mid-tier players, in that some (Nigerian) fraudsters and a (British) ransomware infections expert were present in the UK, and vulnerable to arrest, even if other more senior elements of these cybercriminal networks were overseas.

Third, a number of the cases had clear and important offline elements, and were not solely online organisations (see also Leukfeldt, 2014; Leukfeldt et al., 2017b; Leukfeldt and Roks, 2021; Odinot et al., 2017; Lusthaus 2018). The evidence from these cases reinforces the notion that cybercrime groups are locally embedded, which is in line with prior research (Leukfeldt et al., 2017b/d; Leukfeldt et al., 2019; Lusthaus and Varese, 2017). Such a finding contradicts a conventionally held view that cybercrime is carried out almost entirely in cyberspace, and provides a clear avenue for investigators: even if only part of a network is local to a nation, as with the UK in these cases, there are still options for arresting this local element and disrupting the broader network in some way. But in certain cases, other elements, including some higher-level organisers, were also present in the UK and vulnerable to arrest.

Fourth, a number of the cases involved offenders from the same language, national or regional background, for instance Russian speaking, Romanian or Nigerian. This included both instances of pre-existing relationships, as well as contacts made through diaspora communities and their meeting places. These elements may have aided with trust building and cooperation. This affirms prior research from the Netherlands that social networks are very important within cybercrime (Leukfeldt et al., 2017b/d; Leukfeldt, 2014). While one can focus on online opportunities for networking, such as rating and review systems on criminal marketplaces and forums, traditional trust building mechanisms remain important for cybercriminal networks. From a policing perspective, there is inherent value in recognizing the offline connections between offenders, as they can produce investigative leads that may generate arrests.

Fifth, forums and marketplaces played an important role in some cases, but not in others. Some of this related to the point above. Many offenders coordinated through a range of in person and virtual communication strategies (such as texting and calls), in much the same way as many non-cybercrime offenders engage with each other. In cases with a strong offline dimension, any use of marketplaces was often for making connections or seeking expertise that was not held within the network (Leukfeldt et al., 2017b/d; Bijlenga & Kleemans, 2018). As a result, they may facilitate a fusion of otherwise distinct individuals/groups into part of the same broader cybercriminal network. In those cases where the digital element was more central from the beginning, offenders largely worked together online. But the core function of forums and marketplaces were more about trade and networking. Once these connections were made, offenders often moved to other communication platforms to carry out their business/collaboration together, which were much more private (such as messaging services).

Sixth, cybercriminal networks varied widely across the cases, with a spectrum from looser more open networks at one pole, to tighter more closed networks (or at least clusters within networks) at the other. While some networks concentrated key functions within certain individuals and groups, it was a common theme that individual cyber offenders, or even groups, struggle to operate in complete isolation, even if some connections are short-lived. This supports some findings from existing knowledge in the field (Lusthaus 2018; Lusthaus et al., 2022). There was no one-size fits all structure, and the sample is not representative of all UK cases, but two common types of cybercriminal network were observed: (1) cyber-fraud networks;

(2) malware networks. Both of these networks incorporated components responsible for social engineering and money muling. The malware networks had an additional component responsible for the creation and management of the malware itself.

Seventh, these cases indicate that the boundary between cyber-dependent crimes and cyber-enabled crimes is blurred. There are clear similarities between cases in each category, such as the presence of social engineering and money muling components. Tied to this, it is also clear that supposed cyber-dependent cases, like those centred on malware, actually involve a number of less technical components that are central to the success of the business model. For this reason, within profit-driven cybercrime, pure cyber-dependent crimes may rarely exist. This is because targeting a computer or system alone will not lead to any profit, without a number of additional elements, such as manipulating users into infecting their machines, and having a network of partners to receive, cash out, and/or launder the proceeds. It should not be overlooked that many present-day malware schemes are actually forms of (cyber-enabled) banking fraud or extortion. But, conversely, it must be remembered that some cyber-enabled crimes might look like conventional fraud, but have the use of computers, the internet and/or other technology at the core of their business model, and particularly with regard to the engagement with victims.

Before concluding, some study limitations have to be addressed. First, we took strong steps to ensure that a range of different types of financially-motivated cybercrime cases were included in this project. At the same time, 10 cases should not be viewed as representative of cybercrime or offender behaviors as a whole. Second, the small number of cases also limited the amount of comparison possible between different cybercriminal networks employing the same business model. Third, these cases speak to the UK context, and to the threats that are being targeted against this country. They do not provide as much information on attacks/scams being carried out elsewhere. Fourth, only cases investigated by UK law enforcement can be included in this research, which means that certain kinds of cybercrime might be occurring within the UK but are not being tracked and/or prosecuted there (though they may be elsewhere). Finally, because we intentionally sampled for more serious/international cases so we could better understand these types of cybercrime, there is natural in-built bias tilting the selection of cases in this direction.

There is enormous scope for future waves of data collection on closed cybercrime cases in the UK and beyond. By expanding this approach, some of the limitations noted here would be addressed and our knowledge of cybercriminal networks and their business models would continue to be enhanced. By better understanding a range of cybercriminal cases, this endeavour could lead to focussed policy recommendations for disrupting these networks and addressing this threat through a range of approaches.

Appendix – Case Analysis Checklist

Case information

1. Project code for case:
2. Start year and end year of the investigation:

Short overview of the investigation

3. What was the starting point for this criminal investigation?
4. On which criminal offences did the investigation focus?
5. Did the investigation focus on certain parts of the network? Why?
6. Were suspects prosecuted/convicted/sentenced?
7. Primary investigation methods used:
8. Did the investigation approach change during the case's evolution?

Modus operandi of the criminal network

9. Type of cybercrime(s) carried out:
10. Describe the period/duration of the criminal activities:
11. Describe the main criminal activities of the network:
12. Describe secondary criminal activities of the network:
13. Describe the working area and targets of the network, and whether this changed over time:
14. Give an indication of the scope and nature of the material and immaterial damage:
15. Did the suspects shield themselves against investigations?
16. Did the suspects react/adapt to law enforcement interventions?

Victims

17. Who became victim of the criminal network?
18. How did they fall victim?

Structure of the criminal network

19. Total number of suspects:
20. Describe the composition and structure of the criminal network:
21. Is the network hierarchical/tightly ordered, flat/loose or somewhere in between?
22. Respectively describe the roles of the leaders (if any), members and peripheral facilitators:

23. Describe changes within the composition of the criminal network over time:
24. Was there violence or internal conflicts within the network at any point?
25. How were new members recruited?

Origin and binding mechanisms

26. Was this an online or offline network (or both)?
27. How, when and where did the criminal cooperation start?
28. Do the suspects have a common social background (family, neighborhood, school etc.)?
29. Are there religious or ethnic ties within (parts) of the network?
30. How much trust was there within this network?
31. What bound members of the criminal network together?
32. How was the network governed/controlled?

Contacts with others (online or offline)

33. Was there contact with other criminal groups or individual offenders, considered to be outside the network?
34. Was there any (knowing or unknowing) involvement of legitimate businesses and/or non-offenders?
35. Was there involvement of government officials in any jurisdiction?
36. Did any "insiders" within companies and/or other organisations assist the criminal network?

Volume, distribution and use of illegally obtained profit

37. What is the volume of the illegally obtained benefits?
38. Describe the distribution of the criminal benefits within the criminal group:
39. Describe how and where the offenders spent the criminal benefits (e.g. for personal enjoyment or reinvestment into the criminal enterprise – and in which countries):
40. Does the cybercriminal group possess its own assets?

Money transactions and money laundering

41. Which types of payment systems are used within the criminal network?
42. Describe methods used by the criminal group to launder money:
43. Describe to what extent digitization plays a role (e.g. cryptocurrencies):

Forward-looking analysis

44. Have similar MOs been observed in later cases? If so, what are the similarities (and differences) within these cybercriminal networks?
45. What is a prediction of the future of this MO and the criminal networks involved?
46. Have any important lessons been learned from this case?

Acknowledgements This project was funded by the Home Office through a grant from the National Cyber Security Programme ("Case by Case: Building a Database on Cybercriminal Business Models"). We are grateful for the advice, knowledge and support provided by UK civil servants including Samantha Dowling, Abe Sweiry, Carolyn Budd, and Robert Clarke, along with a number of others. This project would not have been possible without the interview participants, who were generous with both their time and knowledge, along with those who facilitated access to the case files that were used. Finally, Professor Federico Varese offered valuable insights and input across the project as a whole, while Jack Warburton provided exemplary research assistance in the preparation of this article.

Declarations

Compliance with ethical standards There are no potential conflicts of interests. The research involved human participants as interview subjects. Informed consent was obtained in all cases. Ethics approval was given by the University of Oxford, CUREC Ref. SOC_R2_001_C1A_19_25.

References

Ablon L, Libicki MC, Golay AA (2014) Markets for cybercrime tools and stolen data. Hackers' Bazaar. RAND: www.rand.org

Bijlenga N, Kleemans ER (2018) Criminals seeking ICT-expertise: an exploratory study of dutch cases. Eur J Criminal Policy Res. https://doi.org/10.1007/s10610-017-9356-z

Bulanova-Hristova G, Kasper K, Odinot G, Verhoeven M, Pool R, de Poot C, Werner W, Korsell L (eds) (2016) Cyber-OC - scope and manifestations in selected EU member states. Bundeskriminalamt, Wiesbaden

Campana P (2016) The structure of human trafficking: lifting the Bonnet on a nigerian transnational network. Br J Criminol 56(1):68–86

Chu B, Holt TJ, Ahn GJ (2010) Examining the creation, distribution, and function of malware on-line. Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018. Available at https://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf

Décary-Hétu D, Dupont B (2012) The social network of hackers. Global Crime 13(3):160–175

Décary-Hétu D, Morselli C, Leman-Langlois S (2012) Welcome to the scene: a study of social organization and recognition among warez hackers. J Res Crime Delinquency 49(3):359–382

Dupont B, Côté AM, Savine C, Hétu D, D (2016) The ecology of trust among hackers. Global Crime 17(2):129–151

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. Am Behav Sci 61(11):1219–1243. https://doi.org/10.1177/0002764217734263

Dupont B, Lusthaus J (2021) Countering distrust in Illicit Online Networks: the dispute resolution strategies of cybercriminals. Social Sci Comput Rev. https://doi.org/10.1177/0894439321994623

Franklin J, Paxson V, Perrig A, Savage S (2007) *An inquiry into the nature and cause of the wealth of internet miscreants*. Paper presented at *CCS07*, October 29–November 2, 2007 in Alexandria

Herley C, Florencio F (2009) Nobody sells gold for the price of silver: Dis-honesty, uncertainty and the underground economy. Redmond: Microsoft. Microsoft TechReport nr. MSR-TR-2009-34

Holt JT, Lampke E (2010) Exploring stolen data markets online: products and market forces. Criminal Justice Studies 23(1):33–50

Holt TJ (2013) Exploring the social organisation and structure of stolen data markets. Global Crime 14(2–3):155–174

Holt TJ, Smirnova O (2014) Examining the structure, organization, and processes of the international market for stolen data. U.S. Department of Justice, Washington, DC

Holt TJ, Smirnova O, Chua YT, Copes H (2015) Examining the risk reduction strategies of actors in online criminal markets. Global Crime 16(2):81–103

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

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. International journal of offender therapy and comparative criminology, 63(8), 1127–1147.

Kleemans, ER, Van de Bunt, HG (1999) The Social Embeddedness of Organized Crime. Transnational Organized Crime 5(1): 19–36.

Kleemans ER (2015) Organized crime research: challenging assumptions and informing policy. In: Cockbain E, Knutsson J (eds) Applied Police Research. Challenges and Opportunities. Crime Science Series. Routledge

Kleemans, ER, De Poot, CJ (2008) Criminal Careers and Social Opportunity Structure. European Journal of Criminology 5(1): 69–98.

Kruisbergen EW, Leukfeldt ER, Kleemans ER, Roks RA (2018) Georganiseerde criminaliteit en ICT Nederland. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit [Organized crime and IT. Report based on the fifth round of the Organized Crime Monitor]. WODC, Den Haag. English summary available at https://english.wodc.nl/

Levi, M. (2022) Lawyers as money laundering enablers? An evolving and contentious relationship. Global Crime 23(2): 126–147.

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

Leukfeldt ER, Kleemans ER, Stol WP (2017a) A typology of cybercriminal networks: from low tech locals to high tech specialists. Crime Law and Social Change. https://doi.org/10.1007/s10611-016-9646-2

Leukfeldt ER, Kleemans ER, Stol WP (2017b) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. Br J Criminol. https://doi.org/10.1093/bjc/azw009

Leukfeldt R, Kleemans E, Stol W (2017c) The Use of Online Crime Markets by Cybercriminal Networks: a View from within. Am Behav Sci 61(11):1387–1402. https://doi.org/10.1177/0002764217734267

Leukfeldt ER, Stol WPH, Kleemans ER (2017d) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. Crime Law and Social Change 67(1):39–53. https://doi.org/10.1007/s10611-016-9663-1

Leukfeldt ER, Kleemans ER, Kruisbergen EW, Roks R (2019) Criminal networks in a digitized world: on the Nexus of borderless opportunities and local embeddedness. Trends in Organized Crime. https://doi.org/10.1007/s12117-019-09366-7

Leukfeldt ER, Kleemans ER (2021) Breaking the walls of silence: analyzing criminal investigations to improve our understanding of cybercrime. In: Lavorgna A, Holt TJ (eds) Researching cybercrimes. Palgrave Macmillan, Cham, pp 127–144. https://doi.org/10.1007/978-3-030-74837-1_7

Leukfeldt ER, Roks RA (2021) Cybercrimes on the Streets of the Netherlands? An exploration of the intersection of Cybercrimes and Street crimes. Deviant Behav 42(11):1458–1469. DOI: https://doi.org/10.1080/01639625.2020.1755587

Lu Y, Luo X, Polgar M, Cao Y (2010) Social network analysis of a criminal hacker community. J Comput Inform Syst 51(2):31–41

Lusthaus J (2012) Trust in the world of cybercrime. Global Crime 13(2):71–94

Lusthaus J (2018) Industry of anonymity: Inside the business of cybercrime. Cambridge, Massachusetts

Lusthaus J, Varese F (2017) Offline and local; the hidden face of cybercrime. Policing: A Journal of Policy and Practice. https://doi.org/10.1093/police/pax042

Lusthaus J, van Oss J, Amann P (2022) The Gozi group: a criminal firm in cyberspace? Eur J Criminol. https://doi.org/10.1177/14773708221077615

Nguyen T, Luong HT (2021) The structure of cybercrime networks: transnational computer fraud in Vietnam. J Crime Justice 44(4):419–440

Odinot G, Verhoeven MA, Pool RLD, De Poot CJ (2017) Organised cyber-crime in the Netherlands: empirical findings and implications for law enforcement. WODC, Den Haag. Cahier 2017-1

Pastrana S, Thomas DR, Hutchings A, Clayton R (2018) CrimeBB: Enabling cybercrime research on underground forums at scale. Proceedings of the Web Conference 2018 (WWW 2018), Lyon, France, 1845–1854

Peretti KK (2008) Data breaches: what the underground world of 'carding' reveals. Santa Clara Computer and High-technology Law Journal 25(2):345–414

Roks RA, Leukfeldt E, Rutger, Densley JA (2021) The hybridization of street offending in the Netherlands. Br J Criminol 61(4):926–945

Soudijn MRJ, Monsma E (2012) Virtuele ontmoetingsuimtes voor cybercrimi-nelen. Tijdschrift voor Criminologie 54(4):349–360

Soudijn MRJ, Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. Trends in Organized Crime 15(2–3):111–129

Varese F (2001) The russian Mafia: private protection in a new market economy. Oxford University Press, Oxford

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

Werner Y, Korsell L (2016) Cyber-OC in Sweden. In: Bulanova-Hristova G, Kasper K, Odinot G, Verhoeven M, Pool R, de Poot C, Werner W, Korsell L (eds) Cyber-OC: scope and manifestations in selected EU member states. Bundeskriminalamt, Wiesbaden, pp 101–164

Williams, M.L., Levi, M., Burnap, P., & Gundur, R.V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. Deviant Behaviour, 40(9), 1119–1131.

Yip M, Shadbolt N, Webber C (2012) Structural analysis of online criminal social networks. In IEEE international conference on intelligence and security informatics (ISI)(pp. 60–65). Arlington: IEEE

Yip M, Webber C, Shadbolt N (2013) Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Polic Soc 23(4):516–539

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.