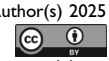
Special Issue: The Human Factor in Cybercrime

European Journal of Criminology

The evolution of Nigerian cybercrime: Two case studies of UK-based offender networks

European Journal of Criminology
1–21


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14773708251329695
journals.sagepub.com/home/euc

Jonathan Lusthaus
University of Oxford, UK

Thomas J. Holt
Michigan State University, USA

Michael Levi
Cardiff University, UK

Edward Kleemans
Vrije Universiteit Amsterdam, the Netherlands

Eric Rutger Leukfeldt
NSCR, the Netherlands; Leiden University, the Netherlands; The Hague University of Applied Sciences, the Netherlands

Abstract

Thus far, the literature on cybercrime has focussed on 'cyber-dependent', rather than 'cyber-enabled' crime. This has meant the emphasis has been on online settings, technical offences, and Western cybercriminals. This paper seeks to partially address these gaps through focussed qualitative case study analyses of two Nigerian offender networks based in Europe, which were both engaged in cyber-enabled fraud and had a strong offline component. We seek to answer two key research questions: (1) How have Nigerian cybercriminal networks evolved over time? (2) How do Nigerian cybercriminal networks operate abroad, particularly within a European context? Our findings include that, over time, Nigerian offenders have adopted several cybercriminal business models, and that these operations are increasingly sophisticated and engaging with some more technical components of cybercrime.

Corresponding author:
Jonathan Lusthaus, Department of Sociology, University of Oxford, 42-43 Park End Street, Oxford OX1 2JD, UK.
Email: jonathan.lusthaus@sociology.ox.ac.uk

Notably, these offenders were mobile, which suggests that cybercrime networks can be transnational through migration and the formation of new offline/local hubs across the world, rather than through virtual means alone.

Keywords
Cybercrime, cyber-dependent crime, cyber-enabled crime, evolution and innovation, Nigeria

Introduction

Research on financially motivated cybercrimes has grown substantially over the last two decades, covering hacking, malware, fraud, and phishing offences (for a recent review, see Holt, 2023). But the bulk of this literature addresses online relationships between offenders, particularly regarding virtual marketplaces where these offenders can network and trade (Dupont and Lusthaus, 2021; Hutchings and Holt, 2015; Holt and Lampke, 2010; Motoyama et al., 2011). Additionally, many studies frequently focus on hacking, malware and other technical forms of cybercrime. These offences are commonly known as 'cyber-dependent crimes', in that they ostensibly cannot be carried out without computers and the Internet (Maimon and Louderback, 2019). The bulk of data for these studies also focus on Western nations.

Despite its advances, the cybercrime research field retains key gaps. First, the role that offline and local networks can play within cybercriminal organisations remains underexplored (Leukfeldt, 2014; Leukfeldt et al., 2017a; Lusthaus and Varese, 2021). Second, 'cyber-enabled crimes' like fraud are given less attention than more technical offences like hacking or malware. Third, more cybercrime research is required on non-Western offenders (Lusthaus, 2018). Finally, scholars also need to explore how some cybercrime offenders may not be rooted in place but may move across borders.

This paper seeks to partially address these gaps through a focussed qualitative case study analysis of Nigerian cybercriminals living in Europe. Nigeria has long been associated with Internet fraud, and most famously 'Advance Fee Fraud' (AFF) email scams (Holt and Graves, 2007). While there have been high-profile warnings about the scale and impact of these threats (Igwe, 2021; Tiwari, 2022), Nigerian cybercriminals have not received the same degree of attention from academic researchers. Only a small amount of research has addressed offender networks, such as 'yahooboys', residing within Nigeria (Adeniran, 2008; Tade and Aliyu, 2011). There has been limited mention of the operation of these fraudsters outside Nigeria. To expand our understanding of Nigerian cybercriminal organisation and business practices, this study utilised a qualitative case study analysis of two historical offender networks that were based primarily within the UK. This was coupled with a comparative analysis of additional cases of more recent Nigerian cybercriminal networks operating around the globe that were dismantled by, or in collaboration with, the US law enforcement. We seek to answer two key research questions: (1) How have Nigerian cybercriminal networks evolved over time? (2) How do Nigerian cybercriminal networks operate abroad, particularly within a European context? This article, and the questions it engages with, have relevance to

European Criminology as it involves the study of diaspora cybercriminal groups within Europe, and the ways in which European citizens and businesses may become victims of these offenders.

This article proceeds as follows. First, it reviews the existing literature on both core cybercrime concepts and Nigerian offenders. Second, it outlines the data and methods employed. Third, it provides its core contribution, with two sections, respectively, covering a detailed case study of a Nigerian cyber fraud network, and the following section outlining additional cases for comparative purposes. Fourth, it presents the key findings and discussion.

Conceptual background: Cyber-dependent vs. cyber-enabled crime

Many scholars apply broad definitions, which conceptualise cybercrime not as a subclass of crimes, but rather as a variety of illicit activity in cyberspace. But, crucially, cybercrime continues to be sub-categorised in line with earlier debates about whether it is simply 'old wine in new bottles' or something quite novel (Wall, 1998: 201–202; Grabosky, 2001: 243). The UK Home Office published an influential report in 2013 that defined cybercrime as 'an umbrella term used to describe two distinct but closely related criminal activities: cyber-dependent and cyber-enabled crimes' (McGuire and Dowling, 2013: 5). These two terms are understood, respectively, as follows: (1) 'offences that can only be committed by using a computer, computer networks, or other form of ICT' (e.g., malware and hacking); (2) 'traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT' (e.g., fraud and theft).

The division between cyber-enabled and cyber-dependent crimes has been widely applied and continues to be central to cybercrime scholarship. But the focus of cybercrime scholars has been on cyber-dependent crime, which Wall (2007) calls 'true' cybercrime. As such, the bulk of the cybercrime literature has been on more technical offenders, like hackers and malware coders (Maimon and Louderback, 2019). The study of offender networks has also focussed on the types of forums where hackers congregate, with the literature emphasising that offenders are immersed in a loosely affiliated series of online social networks which provide access to information and resources that facilitate engagement in cybercrime generally (Dupont et al., 2017; Holt et al., 2016; Hutchings and Clayton, 2016; Leukfeldt and Holt, 2019). This focus may be tied to data availability, in that many of these kinds of forums are relatively public and open. But the idea of more technical, or more sophisticated, offences and offenders may have created an implicit bias that, on the other hand, cyber-enabled crimes may be less worthy of study.

Despite the wide application of this conceptualisation, there are some suggestions within the literature that there is not always a hard barrier between cyber-dependent and cyber-enabled crimes. One well-known example of this relates to credit/debit data breaches, and other similar operations, which require both online attacks and a network of offline offenders to 'cash out', by making ATM cash withdrawals, buying expensive items, and/or carrying out money transfers (Hutchings and Holt, 2015;

Leukfeldt et al., 2017b; Roks et al., 2021). Porcedda and Wall (2021: 169) advocate for a 'cascade' model of cybercrime, whereby 'upstream data-based cyber-dependent cybercrime can result in further cyber-enabled and cyber-assisted cybercrimes'. This means that, in practice, the theoretical division between cyber-dependent and cyber-enabled crime is porous, as both technical and non-technical offenders work together in many cybercriminal endeavours. Lusthaus (2018: 8) argues that it would be 'unusual for one of these technical crimes not to be linked to some broader motivation and a more traditional crime type, be it theft, fraud, extortion, harassment, vandalism, or espionage'. The significance of the offline dimension of cybercrime also challenges the pre-eminence that is often afforded to more technical conceptions of cybercrime, suggesting these offenders are embedded within local contexts and, sometimes, more conventional networks of criminality (Leukfeldt, 2014; 2017b; Lusthaus and Varese, 2021).

By surveying recent empirical findings, stronger support is found for the conception of cybercrime as a modern manifestation of pre-existing forms of crime, rather than something entirely novel. We use this study of Nigerian cybercrime to evaluate this proposition in a focussed way, by adding an important empirical component to the sparse literature on cyber-enabled crime.

Nigerian cyber-enabled fraud

For decades, Nigerians have been engaged in a range of online fraud schemes. This has led researchers to explore the practices of offender networks, such as 'yahoo-boys' residing in Nigeria (Adeniran, 2008; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011). These offenders have become so well known that their brand almost obscures the existence of cybercrime offenders from other West African nations. Studies of Nigerian fraud illustrate individuals are frequently motivated to engage in cybercrime as a means of making money to support themselves and, to a lesser extent, their families (Adeniran, 2008; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011). These offenders appear to engage in a variety of economic offences, whether involving phishing or various forms of email and computer-based fraud, and some schemes are aided by insiders within financial institutions and other agencies (Tade and Aliyu, 2011). The degree of corruption present in the Nigerian government and police agencies also plays a role in cybercrime offending, as individuals can find ways to avoid arrest or minimise formal sanctions (Ajibike, 2019; Lazarus, 2025; Tade, 2013).

Cybercrime is an enticing business path when faced with limited employment prospects (Monsurat, 2020; Thisse and Zenou, 2000). Researchers report that young Nigerians engage in cybercrime as a way to earn more than their peers in legitimate employment, and some engage in an overt party lifestyle (Adeniran, 2008; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011). In fact, there is some evidence that individuals come to engage in cybercrime because of their peers' displays of wealth and accounts of fraud schemes (Babatunde and Olanrewaju, 2015; Ojedokun and Ilori, 2023). Individuals frequently shared information on the process of offending and the tools required to perform certain types of cybercrime through direct/offline personal ties to friends or neighbours (Babatunde and Olanrewaju, 2015; Ojedokun and Ilori, 2023;

Tade and Aliyu, 2011). At the same time, individuals use cybercrime forums and other loose online networks to purchase, for instance, tools, stolen data, and spam lists (Ojedokun and Ilori, 2023; Tade and Aliyu, 2011).

Most of the academic literature up to this point has addressed Nigerian cybercrime within Nigeria. But given high levels of migration from Nigeria to Europe, the USA and elsewhere, including educated youths escaping restricted employment avenues at home, some individuals with a capacity for cybercrime may move overseas to expand their networks and opportunities to offend (Adhikari et al., 2021). There is tremendous space to examine how these Nigerian offenders may operate abroad. This study attempts to explore the ways that Nigerian offender networks have evolved over time and operate within the UK.

Data and methods

This paper is centred on two case studies of closed cybercrime investigations anchored in the UK. These cases were selected, in part, as the relevant prosecutions had been completed. They form part of a larger project on profit-driven cybercrime, involving the analysis of 10 closed cases (see Lusthaus et al., 2024). The key data for each case included an interview with at least one investigator and analysis of police and legal files, along with relevant and reliable open-source material. In large part, we followed the protocols established by the Dutch Organized Crime Monitor (see Kleemans, 2015). Although, some modications were made because: our study focussed on cybercrime rather than organised crime; we accessed data from the UK context, which does not have a widespread culture of law enforcement data sharing. We obtained the legal/police files from UK law enforcement, which included prosecutor's opening notes, MG5s (case summaries for court), and other documents. Data coding and analysis took place using a checklist covering a range of topics concerning the nature/organisation of criminal networks, which was adapted from the Dutch Organised Crime Monitor for use on cybercrime cases (see Lusthaus et al., 2024). Based on access and ethics protocols, the presentation of each case was anonymised.

This paper examines two UK investigations of Nigerian cybercriminals predominantly based in the UK, exploring the methods and organisational hierarchies of these offenders by using qualitative methods. The 10 cases that formed the overall project were chosen according to key selection criteria (Lusthaus et al., 2024), but specific effort was made to ensure that two cases involving Nigerian offenders were included. These cases offer something new to the literature in that they include Nigerian offender networks with significant components resident in the UK, along with other elements based in Nigeria. As noted, the current body of research on Nigerian cybercriminals is largely focused on offender populations living within Nigeria. Less is known about their mobility, and the methods and tactics used by Nigerian nationals to engage in cybercrimes when living abroad in Europe and elsewhere.

In order to increase validity outside Europe, we also gathered data on a number of investigations carried out by the US Department of Justice, which publishes some information on these cases. For the period of 2017–2021, we gathered the summary press releases for all the published US DOJ prosecutions that were available on the government

website, which amounted to 15 investigations. The key coding categories were: offender location, scam type, level of sophistication, any additional noteworthy points. When available, we also accessed indictments and other similar long-form documents, to provide more detailed qualitative insights. The analysis of this data was intended to address two key considerations. First, it offered additional cases from another jurisdiction, which allowed us to assess the external validity of the two core case studies. Second, by assessing cases from recent years, we are also able to assess any additional evolutions that have taken place since the earlier period of Nigerian cybercrime captured in the existing scholarly literature, mainly reflecting advance fee frauds conducted by offenders based in Nigeria.

Case 1

Advance fee fraud is a well-established cybercriminal business model, which has been carried out since the early days of the Internet (Holt and Graves, 2007). While these types of fraud can be perpetrated by anyone, they are strongly associated with Nigerian offenders. Before the arrival of the Internet, these scams were carried out through physical letters, fax-delivered messages, and phone calls.[1]

The modus operandi (MO) is much the same: the victim is contacted, notifying them that the author of the email/letter has come into some money, but they need help from the victim to pay some kind of administrative or legal fee to unlock this larger sum of money. Such scams have been structured around inheritance, packages arriving at customs, and lottery winnings, among many other examples. Victims are led to believe that paying fees and taxes are 'an investment to obtain the more substantial prize', but 'this prize never materialises'. Having committed money to the scheme, 'many victims feel compelled to keep sending payments, as they are unwilling to write off their losses'.[2]

Case 1 involved a lottery-based form of advance fee fraud, where the offenders mailed paper letters to victims, overseas in the USA, informing them they had won a prize and asking them to get in contact with an 'agent'. The initial letter looked professional, with convincing formatting and logos, and it is notable that it was a letter and not an email. When the agent was contacted, he would mention that an initial administrative fee of just under $300 was needed to access the winnings.[3] Follow-up contact would be made through emails and phone calls. The offenders would not stop after the initial fee, but would request further payments as part of the process. They might suggest, for instance, that a cheque had been blocked for one reason or another and needed to be issued again.

If a victim couldn't make the full requested payment, the 'account agent' might claim to make the payment for them, accepting whatever funds the victim was able to provide and 'loaning' them the rest.[4] In a number of cases, requests were made until the victims no longer had funds to pay in a process that might last several years. According to the investigator, victims were carefully selected from vulnerable groups, such as the elderly, and the offenders made use of 'suckers lists', which indicate the names of those who had fallen for scams in the past.[5]

Case 1 affected hundreds of victims, if not more. This fraud was carried out through both physical and cyber means, with the initial contact to victims made via letter, along

with email and calls used to build the relationship and complete the fraud. In this respect, the use of computers and technology makes this offence a form of cyber-enabled fraud. There were also other technical elements employed to aid the fraud, such as the production of documents which included logos of major corporations and other 'authentic' elements to help dupe victims.[6] It was unclear from the case whether these kind of counterfeit documents/templates were produced by the fraudsters or purchased as goods or services from external suppliers.

What was particularly noteworthy in this case is that some offenders within this network were on well-known international English and Russian cybercrime forums, with evidence that they were purchasing more technical tools/services. This is an early example of Nigerian fraudsters engaging with cybercriminals from Eastern Europe and elsewhere, who themselves were more associated with cyber-dependent crime rather than fraud. In fact, Case 1 began as a cyber-dependent investigation and took place in the early 2010s. It followed the arrest of a major European cybercriminal by American law enforcement. This man was an important figure within a leading international cybercrime forum, who had been selling access to his botnet. From the payments that were made, one of the buyers was identified as Actor 1, a Nigerian national who was resident in the UK.

In the beginning, it was thought this would be a simple case, involving prosecution of Actor 1 under the Computer Misuse Act for his involvement with the botnet. But when the arrest took place, highly detailed records on fraud victims were uncovered, indicating the major advance fee fraud campaign described above. This AFF campaign became the focus of a multi-year investigation with the cyber-dependent offences receding into a secondary concern, and eventually going 'out the window'.[7]

The botnet gave access to infected computers and allowed key logging, which may have been used to gather information on victims, though due to the shift in focus of the investigation, the role of the botnet for this fraud network was not probed in detail. Overall, the case showed the 'blurred boundaries' between the cyber-dependent and cyber-enabled, as the fraud network would not have been found without the cyber-dependent origins of the case.[8]

Actors in this case were committed to the cybercriminal business they were conducting. They ran it as self-styled 'businessmen' engaging with 'clients'.[9] The MO remained largely the same during the course of the investigation. Actor 1 would regularly change email addresses and phone numbers to protect himself. But there were limits to this, as the contact details had to be relatively steady so that victims did not become too suspicious. Even after Actor 1 was arrested, he continued committing the same crimes, simply setting up in a new residential address, with new phones and new accounts. Some of his colleagues continued despite Actor 1 eventually going to prison. The legal files paint an unclear picture of the total amount of money that was defrauded, but it appeared to be in the millions, with many of the victim payments coming through money transfer bureaus like Western Union.[10]

Network structure

This investigation was primarily centred on Actor 1, but it provided a window into the broader criminal network. There were approximately 10 individuals who were described

by an investigator as 'lieutenants'.[11] Actor 1, who was based in London, fell into this category. There were at least two other lieutenants (Actor 2 and Actor 3) with a similar role to Actor 1, who were also based in London. Their function was to manage their own list of victims and to engage with them. The evidence gathered from Actor 1 suggested that this was done in a detailed and professional way, with records on victim names, addresses, payments, personal information (e.g., children/dogs).[12] These offenders were roughly equal within this network, as Actor 1 and Actor 2 were helpful to each other in their business, even sharing a luxury rental car. If a particular victim wished to speak with the 'boss', the other scammer would step in to provide another voice for credibility. But they were otherwise independent in terms of their victim lists and operations. Importantly, they were close socially, being described like 'brothers' by Actor 1's wife.[13]

Above Actor 1 and these largely autonomous co-offenders was Actor 4. This person appeared to be a figure of authority and was based in Nigeria. He played a role in coordinating the work of others who operated from overseas bases. Actor 4 was sending 'cascade emails' down to the 10 fraud managers below him to ensure everyone had the correct information regarding the scam, as well as providing ad hoc advice and orders. He was referred to within the network as the 'chairman'.[14] In another connection to cyber-dependent crime, Actor 4 was active on one of the leading Russian cybercrime marketplaces, which was not commonly used by foreigners at the time, and housed some high-level Eastern European cybercriminals, many engaged with more technical pursuits.

Connected to the fraudsters were money mules. Actor 1 had a network he worked with, who dealt with the payments coming from victims. This included both mule herders and mules. An investigator described these as 'low-level characters', some of whom may have had links to broader criminality.[15]

Criminal cooperation

There were a number of elements which bound this criminal network together. First, of course, there were the profits derived from their fraud scheme, which generated millions from victims. Some of these profits went back to Nigeria in the form of property purchases and cars. But members also celebrated their wealth. The offenders lived in an 'exclusive' high-rent apartment complex, with lifestyles 'not in keeping with any legitimate earnings'. When one of the offenders was arrested, he was in possession of a 'large quantity of designer clothing and receipts for high end stores'. Photos obtained from his smartphone depicted expensive cars, champagne and parties.[16] Actor 3 drove a luxury European car around in Nigeria.[17]

Not only did the profits incentivise the involvement of the core group, but they also performed an important social function. They were used as 'carrots' to ensure the cooperation of more peripheral network members, such as a number of girlfriends and their friends who played ad hoc roles within the scams (see next subsection). An example was an extravagant birthday party held by Actor 1, for which he booked out a hotel and flew in by helicopter. Along with providing a good time for himself and his key partners, he would spend money on drinks and gifts for these women.[18]

While one might expect threats of violence to bind the network together, there was only moderate evidence for this within the data. At least one of the women who had

been absorbed into the network as a money mule was a friend of one of the scammer's girlfriends. No actual violence was perpetrated against her, but she was followed home and intimidated.[19]

The final element of criminal cooperation was the presence of a strong offline social network among the offenders. There were many facets to this. As noted, a number of the fraudsters socialised together. Some may have known each other from Nigeria, but others likely formed links by attending the same community venues, such as Nigerian restaurants. A number of offenders also lived in the same block of flats. The community mechanism was also relevant with regard to the money mules. Almost all of these individuals were West African, and particularly Nigerian. As such, there was a very strong national and cultural component within the network.

One way to evaluate the level of criminal cooperation within the network is through their response to being prosecuted. While more peripheral members engaged with the police, Actor 1 did not incriminate other members of the network. His strategy was to blame everything on a mule herder, who had already passed away due to ill health. He maintained this position even through the court proceedings and being sent to prison.

External interactions

There were numerous ostensibly non-criminal actors who were involved with this network. As noted, a number of women were brought into the network in the form of girlfriends and their friends. Some of these individuals then played roles within the scams. This included acting as money mules but also providing additional female voices, which could be used to engage with the victims. The investigators tracked down the girlfriend of one of the scammers who was not apprehended. She was treated as a money laundering witness, rather than an offender. She claimed she had been duped and believed that her boyfriend was a multi-millionaire, who gave her presents and was very public about his wealth on social media. She claimed to know nothing about either the victims or the money laundering.[20]

Both Actor 1 and Actor 2 were also married, providing each offender with legal immigration status within the UK (pre-Brexit), as each of these women were European nationals.[21] Both of these women were significantly older than the two offenders, and the investigation did not uncover evidence of genuine romantic involvement.[22] Without the immigration status provided by these marriages, it would have been more difficult for Actors 1 and 2 to remain within the UK and carry out their illicit operations.

Additionally, the scammers effectively converted a number of their victims into money mules. They would not only defraud victims of funds, but also ask them to assist with setting up bank accounts and moving funds.[23] In return for reduced 'fees' and 'taxes', victims would set up a business account and list the scammer on the joint account. In turn, the account could be used to move/launder money from other victims. Victim-mules were provided with very little information on the broader operation, which reduced their knowledge of the practices of the offender network should they be contacted by police. They knew only of the fictitious name of their 'agent' based in London and believed the money passing through these accounts was simply to pay for the fees/taxes.[24]

There was no real evidence that the network included insiders within financial institutions. Instead, the offenders utilised weaknesses within existing systems in order to

ensure payments and withdrawals were completed. There were, however, lawyers operating on behalf of Actor 1 in Nigeria who facilitated the purchase of property within the country. The lawyers managed funds on behalf of Actor 1 so that he never handled the funds involved in purchases.[25] There was no evidence that these offenders utilised corruption within law enforcement in order to avoid arrests or continue engaging in offences.

Case 2

The second MO discussed in this paper is business email compromise (BEC), which has also been known as Push Payment Fraud, Man-in-the-Email scams, CEO Fraud, and Change-of-Account Details Fraud. This approach is more technical than advance fee fraud, but is still a form of fraud. The legal files in Case 2 describe this type of fraud as 'sophisticated, well-organised, technologically-aware'.[26] The technical components are largely preliminary to the commission of the fraud, which itself is a form of confidence scam making use of social engineering. The scammers target companies and organisations that conduct bank transfers as part of their operations, which is most entities. The fraudsters might impersonate the CEO, CFO or another officer who can authorise bank transfers, by spoofing an email address, or creating a similar looking one so as to defeat the scrutiny of the recipient. In certain cases, official email accounts are compromised through the use of keyloggers or phishing attacks. Then the account can be used to authorise payments. It is also possible for suppliers or those who receive payments from the company to be impersonated and request that an upcoming payment be paid with 'updated' account details. BEC scams account for large losses each year. Although smaller sums are involved, cases can involve sums in the hundreds of thousands (Cross and Gillett, 2020). For Case 2, the total sum appropriated was over £500,000.[27]

We can trace a specific example of this MO through Case 2. In this case, the fraudster (Actor 1) created email templates which looked convincingly like real companies such as DropBox or PayPal.[28] These were phishing emails requesting updated details to be entered into a (spoofed) site, which was designed to be a near replica of the real company websites.[29] In order to contact a wide pool of potential victims, Actor 1 purchased very large quantities of email addresses, and then used customised mass mailers to send false emails to these people.[30] Legal files note evidence that he had over 1.5 million email addresses in his possession and had emailed hundreds of thousands of individuals.[31] Only a low percentage of these individuals would receive these emails, and even fewer would provide their details. Given the enormous number of contacts involved, this was sufficient.

Once victims entered their details into the spoof sites, this information would be captured in a spreadsheet. Actor 1 then selected what looked like business emails from these lists, trying to log in with the phished passwords. Out of the multitude of emails sent, he might end up with thousands of compromised accounts to search for invoices and other useful pieces of information to make a credible contact requesting payment to an account he controlled.[32] He also made an assessment of whether there was sufficient profitability in targeting the respective companies.[33] This contact might be made through the compromised email account of the expected sender of an invoice, or through a spoofed email if the scammer had compromised the expected recipient of the invoice.[34] Actor 1 used real invoices that he had obtained from the compromised email accounts and doctored them

with software to include account details provided to him by a partner running a team of money mules.[35] Even with the change in communication style, and poor English, an investigator in Case 2 believed these payment request emails worked around half the time (although the case files did not provide details to verify this point).[36]

This investigation into BEC took place 5 years after Case 1. It had similar origins, as it was expected to be a small discrete investigation into one instance of a £30,000 fraud. Once Actor 1 was located, digital evidence gathered showed his involvement in dozens of other frauds, as well as connections to a broader network of offenders who were not known to law enforcement up to this point. There were around 30 members of the larger network, or at least 30 online aliases. It was estimated that the inclusion of the larger network increased the attempted amount defrauded to several million pounds, though legal files listed specifically evidenced losses at around £500,000.[37]

Despite the increased scope of the network identified, the investigation was kept narrow and focussed on one or two senior money launderers in addition to the fraudster who was initially arrested. This may have been due to the fact that the investigation originated as a training exercise for a junior investigator. It was more to demonstrate what the investigator had learned, with limited expectation for a serious outcome. As the case evolved, the investigator was given more time and authority to engage with it, but it was not a strategic priority for the agency (this may connect with broader concerns around the lack of resources for fraud investigations; see Lord and Levi, 2023).

In an almost identical way to Case 1, the offenders in Case 2 assumed a degree of professionalism. They actively called themselves 'businessmen' and also called their victims 'clients'. As will be discussed below, they also gained a level of respect within their local community.[38]

Network structure

There were two components within this cybercriminal network: the fraud element and the money launderers. In each instance, a fraudster would convince the victim to make the payment into a mule account. Once completed, the money laundering team would look out for this payment and then move the funds into other accounts they controlled. They would also break the sum down into smaller amounts of £1000.[39] These funds would be sent not just around the UK, but also abroad. The mules would then withdraw the money, and hand it over to the mule herder, who would then pass the proceeds to the leader of the money laundering team. The person Actor 1 dealt with for money laundering in this way was Actor 2. Actor 2 provided the profits back to Actor 1 through both cash and transfers into a Nigerian bank account.[40]

The investigator in this case viewed the fraud element of this network structure as relatively flat. Each fraudster was a sole trader of sorts, and there was no sense of any of these equals directing the frauds. He stated this was common across other cases involving offenders from West Africa. For the fraudsters, there seemed to be a collaborative, but competitive ethos, with a desire to carry out more audacious scams than their confreres (which is a theme often found in relation to more technical cybercrime offenders).[41] The relationship between the fraud component and the money launderers was also relatively equal. Even though the money laundering teams were internally hierarchical, the

money laundering leader, Actor 2, dealt with Actor 1 (the fraudster) as a partner rather than an employer/employee. There was some tension within the partnership, as the money launderers were focussed on bank processes and the ways to move and withdraw funds without being detected. The fraud side was, however, concerned with carrying out the largest frauds possible with less concern for the practicalities, such as not transferring too much money in a single transaction from a victim.[42]

It was unclear if the fraud component of the network had connections to broader criminality, though the money mule component did. Actor 2 had a history of involvement in serious crime, involving drugs and guns. He had served time in prison, left the gang scene and engaged with cyber fraud instead. The investigator in this case surmised that this was more profitable and safer for him. He had a reputation for violence and experience managing large sums of money. These were skills he could directly transfer to this new line of work.[43]

Criminal cooperation

Several mechanisms aided cooperation within this cybercriminal network. First, there was a clear division of profits, with the fraudster generally keeping 60%, and the money mule leader claiming the remaining 40%. There was also evidence that large chunks of profits were transferred to the various mules within his team, perhaps leaving a total of 20% as personal profit.[44]

Second, reputation played an important role in terms of who worked with whom, with past dealings and 'professionalism' being highly regarded. There was a core group of around 10 offenders who were in regular contact, with a long chat history. They were risk-averse in relation to new entrants, which could relate to concerns around both competence and infiltration. It was advisable for those joining the circle to be vouched in by one or more of the core group.[45]

As with Case 1, there was also a strong national and cultural dimension connecting offenders, with almost all the networks being Nigerian. A strong offline and local dimension was also observed, with many of the offenders living in Southeast England. Given these ties, it is worth examining this element more deeply. While the investigator expected the offenders to have met online in forums or chat groups, this was not the case. Offline interactions were dominant.[46] The offenders took photos of them all working together in Actor 1's flat, sometimes around 10 offenders all using laptops.

While they ran independent fraud operations and were competitive in a certain kind of way, they would share tips and help each other. There was also a strong social component, and they would drink, smoke cigars, play table football, and bet thousands of pounds on these games. There were also hangers-on and 'groupies' who were connected to these fraudsters.[47] Additionally, church attendance in the local area appeared to be an important social context for both fraudsters and some of the money mule team. Police surveillance indicated that both Actor 1 and Actor 2 attended the same church in Southeast London, although they did not openly engage with each other in this setting and were not photographed together.[48]

Furthermore, there seemed to be some aspect of enforcement and dispute resolution within the group. On the fraud side, there was a woman, Actor 3, known as an 'Auntie'. She appeared to provide advice to the fraudsters, was aware of their activities,

and would check in on them. The investigator noted that Actor 3 was the closest to a sense of authority on the fraud side, who played a role in conflict resolution between them. He noted that some members seemed to be 'scared' of her.[49] Unfortunately, little is known about this Auntie's precise role, and whether she took a cut of the profits, as she was peripheral to the prosecution. As a result, she is not mentioned in the police files, in order to keep matters simple for the jury by having as few 'characters' as possible.

On the money laundering side, as noted, the structure was clearly hierarchical, with Actor 2 at the top. With withdrawals of £1000 each time, a large number of mules was required. Actor 2's role was more to coordinate this sub-network and to keep them in line. His past business with gangs, and managing cash within those operations, made him well suited to this new enterprise with a 'transferable skill'. He had a reputation for violence, maintained connections with gang elders, and lived a jet-setting life (even intersecting socially with an international celebrity at one point).[50] The legal files indicate an example of a dispute between Actor 2 and another money launderer over access to a high-value mule account. Actor 4 was unwilling to provide the account, and Actor 3 paid him a visit to resolve the situation.[51]

External interactions

There were two external components that aided this cybercriminal network. The first were connections to individuals and organisations who could help the scammer remain within the UK, when he lacked the right to do so under immigration rules. Actor 1 and another fraudster (Actor 5) had student visas for attending 'educational institutions' which did not require them to turn up to class and issued them with a diploma at the conclusion of the 'course'.[52] Actor 1 later had a 'sham' marriage to a European national, whom he financially supported, but they 'didn't really get on'.[53] He was charged with perverting the course of justice over this marriage and his misrepresentations about it.[54] He also hired the services of a solicitor who provided ethically inappropriate advice to Actor 1 on evading the UK immigration system.

The second external component aiding this cybercriminal network were individuals within the financial system. Actor 2 had an accountant who managed his criminal proceeds. He cooperated with the investigation and was never charged,[55] but there likely would have been some reasonable suspicions over the books this accountant was managing. The investigator in this case also had some suspicions as to whether there were insiders in the banks being used by mules. These suspicions could never be proven within the scope of the investigation. At a minimum, there were clear examples where adequate photo ID was not provided when a new account was opened. As a general rule, banks would not provide the names of employees who had opened mule accounts, seemingly preferring to deal with these matters in-house and being allowed by the investigators to continue this process for the maintenance of good relationships.[56]

Additional cases

Drawing on US Department of Justice cases from 2017 to 2021 published on their official site, we were able to increase the validity of our analyses beyond the two case studies above. 15 cases were identified after duplicate cases and documents were removed.

Official press releases were available across all 15 cases, and many also included indictments and other more detailed documents. We coded these cases according to key points of interest that were found within the above case studies, particularly in relation to the business model involved, the location of offenders and evidence of sophistication/technical components.

The findings from these 15 cases provided good support for the generalisability of our case studies. As noted earlier, 'conventional' Nigerian cybercrime was carried out by offenders based in Nigeria, with Advance Fee Fraud being the dominant business model. These more recent cases draw a picture of innovation and immigration. Only one of the 15 cases directly noted Advance Fee Fraud. At least six cases involved BEC in a significant way. At least six cases involved tax return fraud, whereby offenders would garner the personal information of victims and then claim tax refunds in their names.

Some of the cases showed networks involved in multiple business models at once. The link between all the cases and the business models used by offenders was a strong component of social engineering (often termed 'phishing' in the documents). Whether attempting to trick an organisation into paying an invoice into the wrong account, gaining access to a payroll system, or obtaining the tax forms of employees, the core of these cybercriminal business models involved convincing one or more individuals to take a requested action essential to conducting the scam. Another theme running across the cases was that it was organisations that were often the initial target of these social engineering attempts, even if individuals later became the victims.

In terms of innovation, these cases revealed a shift away from Advance Fee Fraud towards other business models. Additionally, they illustrated the sophistication – professionalism and effectiveness – of these offender networks. There were also clear indications that these offenders were adopting technical tools in support of various scams. For instance, offender networks used malware to gain access, spoofed emails, VPNs and anonymisation techniques, phishing kits, along with regular references to hacking in the documents.

Perhaps the most striking element of these cases was the prevalence of Nigerian cybercriminals being based overseas. At least 10 of the 15 cases involved key offenders based outside Nigeria. This included the USA, South Africa, Ghana, Malaysia, Canada, and UAE. In three further instances, offenders were nominally based in Nigeria but were arrested travelling to the USA, suggesting they were at least mobile, if not operating overseas. Although the immigration status of offenders could not always be determined, some cases indicated that offenders had overstayed tourist visas. One case involved a sham marriage to a US citizen.

Taken as a whole, both the USA and UK cases illustrate that Nigerian actors were engaging in more complex offences over time. There was also an increased use of tools and services to improve the offenders' overall capacity to complete a crime, such as underground markets and malware that simplifies the process of offending. They also utilised networks that involved offenders living both abroad and within their country of origin.

Discussion

There are a number of key findings that can be derived from the data presented in this paper. First, Nigerian offenders have moved beyond advance fee fraud alone and have

adopted several cybercriminal business models, including BEC. This accords with information from existing literature finding that offenders may be involved in multiple forms of fraud, such as phishing, romance scams and credit card fraud (Cretu-Adatte et al., 2024; Newell, 2021; Tade and Aliyu, 2011).

The second key finding is that while Nigerian offenders are focussed on fraud, they are increasingly engaging with some of the more technical components of cybercrime. They are not simply using the Internet to conduct fraud but are also present in online marketplaces and other settings, obtaining malware, buying data (e.g., spam lists) and using tools to automate their operations and hide their true identities (see also Lazarus, 2025; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011). These tools ensure offenders can successfully complete these fraud schemes. Taken alone, engagement with malware and tools might be considered cyber-dependent crime. But these technical components are used in support of broader fraud operations. This supports the view that there is no clear divide between cyber-dependent and cyber-enabled crime (Lusthaus, 2024; Porcedda and Wall, 2021).

Third, these offenders are mobile, which suggests that cybercrime networks can be transnational through migration and the formation of new offline/local hubs across the world, rather than through virtual means alone (see Lusthaus, 2018). This may connect to a broader phenomenon, whereby significant levels of migration from Nigeria may be tied to high unemployment, particularly among young populations and those with secondary education and college degrees (Adhikari et al., 2021). This paper provides additional evidence that some cybercriminals may form part of this brain drain in an attempt to expand their networks and opportunities to offend.

Fourth, this paper helps to answer how Nigerian offenders operate abroad, relative to their more widely known practices within the borders of Nigeria. While core aspects of their crime are online, and there is some online communication between offenders, many individuals not only knew each other in person but also appeared to engage regularly in offline settings. Many connections went even deeper, with strong friendships, shared residential buildings, and broader community settings like restaurants and churches. It appears that many of these Nigerian offenders are embedded within existing offline social networks and that these networks provide considerable support for their illicit operations. This finding builds on the importance of interpersonal networks in cybercrime within Nigeria (Babatunde and Olanrewaju, 2015; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011).

Finally, this paper provides details on the organisational structures of Nigerian offender networks and whether they are evolving. Despite the innovations described in this paper, in human terms, these structures are stable and consistent. This suggests comparable cybercriminal networks can support different business models, ranging from Advanced Fee Fraud to BEC. While we do not have direct evidence in these cases, it is also possible that groups may have evolved from carrying out AFF into carrying out BEC. There are already suggestions within Case 1 of some members of the network engaging with activities beyond conventional AFF.

Figure 1 represents the network structure of the two cases, demonstrating the strong similarities. The one key difference is whether there is a 'boss' type figure sitting above the fraudsters who seem to operate in a somehow egalitarian, competitive,

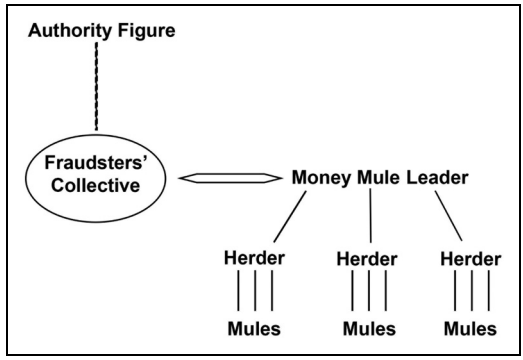


Figure 1. Nigerian cyber fraud network structure.

supportive, professional yet social collective. In Case 1, the investigator suggested this figure was in some way directing this fraud collective. In Case 2, there was the suggestion that such a figure may have existed, but no clear evidence to make this judgement. Given that the investigation in Case 2 was only allowed to penetrate part of the network before being halted, this similarity might have been borne out (or refuted) with further investigation. The spiral line in the below diagram represents the possible difference in this role between the two cases, along with the shadowy role of this figure (even, to a degree, in Case 1). The 'cyber' component within each case is not represented within the diagram, as it is both embedded within the network and outside it. In each case, there was evidence that the authority figure and/or members of the fraudster's collective had a relatively strong technical knowledge/ability, as well as access to off-the-shelf tools. This access was largely arranged through online marketplaces and customer/vendor relationships. As distinct from some more technical groups, like malware enterprises, there is no specific part of the network responsible for the 'cyber function'.

Beyond the key findings, we can also reflect on some of the secondary elements of interest that came out of the analyses. These secondary elements are, at least in part, supported by the literature, which gives further confidence around the external validity of the cases under study. First, there was a strong aspirational, profit and business-minded component within the cases. In both the core case studies and the additional cases, there were also indications of flashy lifestyles, with offenders showing off their ill-gotten gains. This resonates with other studies, which suggest that young Nigerians may engage in cybercrime as a way to earn more than their peers in legitimate employment, engage in an overt party lifestyle, and perhaps even join due to displays of wealth (Adeniran, 2008; Babatunde and Olanrewaju, 2015; Ojedokun and Ilori, 2023; Tade and Aliyu, 2011). Similar findings have been observed among studies of other cyber-enabled offender groups in African countries, which find profits going to luxury good purchases, IT infrastructure, and small businesses (see, e.g., Cretu-Adatte et al., 2024; Newell, 2021).

Second, women were involved in these cases. In many instances, this was in low-level and peripheral ways, often tied to money laundering. But there was the suggestion of a

possible female leadership figure in Case 2. While Nigerian men are the predominant proponents of online fraud schemes, women may be involved in more significant ways than what has been reported among Western offender networks (see Ojedokun and Ilori, 2023; Tade and Aliyu, 2011).

Third, the two case studies presented instances of corruption, including the possibility of criminal facilitators within banking or other professions. It has been argued that corruption within the Nigerian government and police agencies plays an important role in cybercrime offending (Ajibike, 2019; Tade, 2013). Insiders in banks and other organisations are also known to support Nigerian cybercriminal enterprises (Tade and Aliyu, 2011).

Conclusion

The central takeaway from these primary and secondary findings is that, at least for profit-driven cybercrime, cyber-dependent crime is not more important, or more worthy of study, than cyber-enabled crime. In fact, these case studies show that the boundary between cyber-dependent and cyber-enabled crimes is porous (see also Lusthaus, 2024). While the field remains focussed on hacking and other technical offences, and on the online settings where Western criminal hackers congregate, the evolution of Nigerian cybercrime provides a good example of the kind of offender that is ignored. Nigerian offenders are more sophisticated than is often allowed for in both professional and technical terms. Since the inception of AFF, Nigerian offender networks have innovated their business models, and are now engaged with key threats like BEC and beyond. These offenders also travel to different parts of the world, setting up operations within a range of jurisdictions, in ways that are clearly transnational beyond the digital components of cybercrime. Their overall gross and perhaps even net profits can be in the millions.

This paper is an illustration of the importance of cyber-enabled crime, and a call for scholars and policymakers alike to give these types of cybercriminal networks the attention that they deserve. It is essential to move beyond the bounded approach to cybercrime that focusses on Western offender networks. While the academic literature on cybercrime has been dominated by American, British, Dutch, Australian and Canadian contributions, scholars may miss important manifestations of cybercrime from around the globe. While this paper highlights the need to focus on offenders from Nigeria, the same might be said of other countries across the African continent, as well as Russia, Ukraine, Brazil, Southeast Asia, and so on.

Acknowledgements

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 for this article, and Qiaoyu Luo kindly assisted with the final preparation of the manuscript.

Funding

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

ORCID iDs

Jonathan Lusthaus https://orcid.org/0000-0002-9386-7708
Thomas Holt https://orcid.org/0000-0002-5894-0172
Michael Levi https://orcid.org/0000-0003-2131-2882
Edward Kleemans https://orcid.org/0000-0002-6986-8903
Rutger Leukfeldt https://orcid.org/0000-0002-3051-0859

Notes

1. UK Law Enforcement Files.
2. UK Law Enforcement Files.
3. UK Law Enforcement Files; Interview with UK Law Enforcement investigator.
4. Interview with UK Law Enforcement investigator.
5. Interview with UK Law Enforcement investigator; UK Law Enforcement Files.
6. Interview with UK Law Enforcement investigator.
7. Interview with UK Law Enforcement investigator.
8. Interview with UK Law Enforcement investigator.
9. Interview with UK Law Enforcement investigator.
10. UK Law Enforcement Files.
11. Interview with UK Law Enforcement investigator.
12. Interview with UK Law Enforcement investigator; UK Law Enforcement Files.
13. Interview with UK Law Enforcement investigator.
14. Interview with UK Law Enforcement investigator.
15. Interview with UK Law Enforcement investigator.
16. UK Law Enforcement Files.
17. Interview with UK Law Enforcement investigator.
18. Interview with UK Law Enforcement investigator.
19. Interview with UK Law Enforcement investigator.
20. Interview with UK Law Enforcement investigator.
21. UK Law Enforcement Files.
22. Interview with UK Law Enforcement investigator.
23. UK Law Enforcement Files.
24. Interview with UK Law Enforcement investigator; UK Law Enforcement Files.
25. Interview with UK Law Enforcement investigator.
26. UK Law Enforcement Files.
27. UK Law Enforcement Files.
28. UK Law Enforcement Files.
29. UK Law Enforcement Files.
30. Interview with UK Law Enforcement investigator.
31. UK Law Enforcement Files.
32. Interview with UK Law Enforcement investigator.
33. UK Law Enforcement Files.
34. UK Law Enforcement Files.

35. UK Law Enforcement Files.
36. Interview with UK Law Enforcement investigator.
37. Interview with UK Law Enforcement investigator; UK Law Enforcement Files.
38. Interview with UK Law Enforcement investigator.
39. Interview with UK Law Enforcement investigator.
40. UK Law Enforcement Files.
41. Interview with UK Law Enforcement investigator.
42. Interview with UK Law Enforcement investigator.
43. Interview with UK Law Enforcement investigator.
44. Interview with UK Law Enforcement investigator; UK Law Enforcement Files.
45. Interview with UK Law Enforcement investigator.
46. Interview with UK Law Enforcement investigator.
47. Interview with UK Law Enforcement investigator.
48. Interview with UK Law Enforcement investigator.
49. Interview with UK Law Enforcement investigator.
50. Interview with UK Law Enforcement investigator.
51. UK Law Enforcement Files.
52. Interview with UK Law Enforcement investigator.
53. Interview with UK Law Enforcement investigator.
54. UK Law Enforcement Files.
55. Interview with UK Law Enforcement investigator.
56. Interview with UK Law Enforcement investigator.

References

Adeniran A (2008) The internet and emergence of Yahooboys subculture in Nigeria. *International Journal of Cyber Criminology* 2: 368–381.

Adhikari S, Clemens M, Dempster H, et al. (2021) Expanding legal migration pathways from Nigeria to Europe. World Bank Publications Report No. 35996, The World Bank Group, Washington, DC.

Ajibike T (2019) Youth and cybercrime in Nigeria. *Punch Newspaper*, 15 March. https://punchng.-com/youth-and-cybercrime-in-nigeria/.

Babatunde MM and Olanrewaju MK (2015) Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in Southwestern Nigeria. *International Journal of Technology in Teaching and Learning* 11(1): 50–59.

Cretu-Adatte C, et al. (2024) Unravelling the organisation of Ivorian cyberfraudsters: Criminal networks or organised crime? *Journal of Economic Criminology* 3: 1–9.

Cross C and Gillett R (2020) Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime* 27(3): 871–884.

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

Dupont B and Lusthaus J (2021) Countering distrust in illicit online networks: The dispute resolution strategies of cybercriminals. *Social Science Computer Review* 40(4): 892–913.

Grabosky P (2001) Virtual criminality: Old wine in new bottles? *Social & Legal Studies* 10(2): 243–249.

Holt T (2023) Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior* 139: 1–9.

Holt T and Graves D (2007) A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology* 1(1): 137–154.

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

Holt T, et al. (2016) Examining signals of trust in criminal markets online. *Journal of Cybersecurity* 2(2): 137–145.

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

Hutchings A and Holt TJ (2015) A crime script analysis of the online stolen data market. *The British Journal of Criminology* 55(3): 596–614.

Igwe U (2021) *Nigeria's growing cybercrime threat needs urgent government action*. Available at: https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/ (accessed 16 August 2021).

Kleemans ER (2015) Organized crime research. Challenging assumptions and informingpolicy. In: Ella C and Johannes K (eds) *Applied police research. Challenges and opportunities*. New York: Routledge, 57–67. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315815305-6/organized-crime-research-edward-kleemans

Lazarus S (2025) Cybercriminal networks and operational dynamics of Business Email Compromise (BEC) scammers: Insights from the "Black Axe" confraternity. *Deviant Behavior* 46(4): 456–480.

Leukfeldt ER and Holt TJ (2019) 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 R (2014) Cybercrime and social ties. *Trends in Organized Crime* 17(4): 231–249.

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

Lord N and Levi M (2023) Economic crime, economic criminology, and serious crimes for economic gain: On the conceptual and disciplinary (dis)order of the object of study. *Journal of Economic Criminology* 1: 1–8.

Lusthaus J (2018) *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, MA: Harvard University Press.

Lusthaus J (2024) Reconsidering crime and technology: What is this thing we call cybercrime? *Annual Review of Law and Social Science* 20: 369–385.

Lusthaus J, Kleemans E, Leukfeldt R, et al. (2024) Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime* 27(3): 364–387.

Lusthaus J and Varese F (2021) Offline and local: The hidden face of cybercrime. *Policing* 15(1): 4–14.

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

McGuire M and Dowling S (2013) *Cyber Crime: A Review of the Evidence*. London: Home Office.

Monsurat I (2020) African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: A study of the Yahoo boys in Ilorin, Nigeria. *International Journal of Cyber Criminology* 14(1): 300–315.

Motoyama M, McCoy D, Levchenko K, et al. (2011) An analysis of underground forums. In: IMC'11: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement

conference, Berlin, Germany, 2–4 November 2011, pp. 71–80. New York: Association for Computing Machinery.

Newell S (2021) Hackers of the heart: Digital sorcery and virtual intimacy in Côte d'Ivoire. *Africa* 91(4): 661–685.

Ojedokun UA and Ilori AA (2023) Agency banking business and operators' risk of exposure to criminal victimisation in Ibadan, Nigeria. *International Review of Victimology* 29(3): 507–519.

Porcedda MG and Wall D (2021) Modelling the cybercrime cascade effect in data crime. In: 2021 IEEE European symposium on security and privacy workshops (EuroS&PW), Vienna, Austria, 29 October 2021. Piscataway, NJ: IEEE.

Roks RA, Leukfeldt ER and Densley JA (2021) The hybridization of street offending in The Netherlands. *British Journal of Criminology* 61(4): 926–945.

Tade O (2013) A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs* 23(4): 689–705.

Tade O and Aliyu I (2011) Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology* 5(2): 860–875.

Thisse J-F and Zenou Y (2000) Skill mismatch and unemployment. *Economics Letters* 69(3): 415–420.

Tiwari S (2022) *FBI: Rise in business email-based attacks is a $43B headache*. Available at: https://threatpost.com/fbi-bec-43b/179539/ (accessed 16 August 2022).

Wall D (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wall DS (1998) Catching cybercriminals: Policing the internet. *International Review of Law, Computers & Technology* 12(2): 201–218.