Deviant Behavior

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

Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity

Suleman Lazarus

To cite this article: Suleman Lazarus (14 May 2024): Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity, Deviant Behavior, DOI: 10.1080/01639625.2024.2352049

To link to this article: https://doi.org/10.1080/01639625.2024.2352049

Published online: 14 May 2024.

DEVIANT BEHAVIOR
https://doi.org/10.1080/01639625.2024.2352049

Routledge
Taylor & Francis Group

Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity

Suleman Lazarus [a,b]

[a]University of Surrey, Guildford, UK; [b]London School of Economics and Political Science (LSE), London, UK

ABSTRACT

I explored the relationship between the "Black Axe" Confraternity and cybercrime, with a particular emphasis on the structural dynamics of the Business Email Compromise (BEC) schemes. I investigated whether a conventional hierarchical system governs the membership and remuneration for BEC roles as perpetrators by interviewing an accused "leader" of the "Black Axe" affiliated cybercriminal incarcerated in a prominent Western nation. I supplemented the analysis of interview data with insights from tapped phone records monitored by a law enforcement entity. I merged Actor-network theory and Social Network theory as analytical frameworks and thematically analyzed data to produce six overarching themes: (1) The fluidity of Structure and Adaptive Roles in BEC, (2) Challenges in Visualizing Criminal Networks, (3) Globalization and Transnational Dimensions, (4) Social and Cultural Influences, (5) Internal Cybersecurity Threats and Money Laundering, and (6) Remuneration and Influences of Cryptocurrency, casting a brighter light on the topic. Unlike traditional organized crime, BEC scammers have adopted a nonhierarchical model that is flexible and fluid. I found no evidence of a rigid hierarchy dictating positions and remuneration for BEC roles. Instead, I observed that cybercriminals involved in BEC activities functioned horizontally, promoting fluidity, maneuverability, collaboration, and specialization across various facets of their illicit pursuits. I also highlighted the cross-border links BEC offenders have with other criminal actors facilitated by Black Axe organizational machinery. My research adds value to the existing body of knowledge, utilizing a unique dataset comprising direct testimonies of a high-profile BEC offender affiliated with the 'hard–to–access,' Black Axe gang.

ARTICLE HISTORY
Received 10 November 2023
Accepted 1 May 2024

Introduction

Nigeria has emerged as a significant hub for cybercrime, fueled by the activities of online fraudsters (Ibrahim 2016; 2018). While this group of Nigerian nationals within and beyond the country's borders has gained notoriety for their involvement in internet fraud (Ibrahim 2016; 2018; Okosun and Ilo 2022), they are commonly referred to as Yahoo Boys. The term "Yahoo Boys" has become ingrained in various discourses, including academic research (Aborisade 2023; Lazarus and Button 2022; Ogunleye et al. 2019); law enforcement documentation (Trend Micro and INTERPOL 2017), and media coverage (Longgreads 2023; Blomberg 2021), underscoring its widespread recognition. In reflecting on my doctoral studies from a few years ago (Lazarus 2020), my initial curiosity about this social group and

CONTACT Suleman Lazarus suleman.lazarus@gmail.com Department of Sociology, University of Surrey, Stag Hill, Guildford GU2 7XH, UK

the denied opportunity for extended "fieldwork" in its context, as outlined in my autoethnographic article (Lazarus 2021:3), sparked my interest in exploring this intriguing phenomenon further.

However, my focus transcends the activities of common Yahoo Boys, sending thousands of e-mails to unsolicited recipients to the targeting and "hit-and-missed emails," hoping that some people would respond. In this article, I explored the direct testimonies of high-profile and sophisticated cybercriminals specializing in pervasive threats known as Business Email Compromise (BEC) schemes. While the BEC schemes are complex cybercrimes that target mostly organizations via email, the perpetrator impersonates a trusted figure within a company to solicit funds, confidential data, or financial transfers, according to Trend Micro and INTERPOL (2017). In the United States, BEC accounted for $50 billion in losses, according to the Internet Crime Complaint Center (IC3) (Valimail 2023). Although $50 billion may seem staggering, this figure only represents reported losses, and many more crimes go unreported. Unlike the United States, such detailed data archiving practices are not commonplace in Nigeria. It is fascinating how much we have yet to uncover about the sophisticated networks orchestrating these BEC schemes.

In organized crime, hierarchical structures are common, with well-defined roles and clear lines of authority. However, the online fraud context, particularly BEC schemes, presents a unique challenge to these traditional paradigms. The BEC cybercriminals' operational and structural model may not conform to conventional models of organized criminal syndicates. I aim to unravel the intricate social dynamics and organizational structures that define the criminal actors in the BEC scams.

Findings derived from this study have implications beyond academia. They are relevant to law enforcement agencies and policymakers who are engaged in the fight against cybercrime. Additionally, insights from this study are vital in aiding decision-makers in understanding how their organizations may better approach BEC scams, appreciate victims' vulnerabilities, and support employees both before and after an incident. Understanding the complex social dynamics inherent in cybercriminal networks specializing in BEC scams can empower authorities to target their efforts strategically, resulting in more effective disruption of illicit operations. My study examines BEC scams and the social structures of scammers. Against this backdrop, I aim to answer the following question:

- What are the structural and operational dynamics within cybercriminal networks engaged in Business Email Compromise (BEC) cybercrime, and how do these dynamics impact the organization and operation of BEC schemes?

Literature review

Legal meaning of organized crime

Legal definitions of organized crime exhibit significant variations, shaped by the particular criminal contexts within different countries and periods (Lavorgna and Sergi 2014). How the law defines organized crime and membership in such criminal groups are paramount. These baseline definitions profoundly influence the endeavors of law enforcement agencies (e.g., Lavorgna and Sergi 2014; 2016).

This article recognizes the overarching term "organized crime" (Lavorgna and Sergi 2014; Sergi and Storti 2021). International and European legal instruments addressing organized crime provide extensive definitions for terms like "organized crime" or "criminal organization" (Lavorgna and Sergi 2014). These instruments also establish relatively stringent thresholds, including mandatory minimum sentences (Lavorgna and Sergi 2014). As defined by the United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 in November 2000, an "organized criminal group" is described (Lavorgna and Sergi 2014:18):

> a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit (article 2(a)),

With "structured group" refers to:

> a group that is not formed arbitrarily for the immediate commission of an offense and that is not required to have formally defined roles for its members, continuity of membership, or a developed structure. (article 2c)

The European Framework Decision (2008/841/JHA) defines "criminal organization" as follows:

> structured association, established over time, of more than two persons acting in concert with the intention of committing offences punishable by deprivation of liberty or a detention order of at least four years or a more severe penalty, to obtain, directly or indirectly, a financial or other material benefit (art. 1.1)

A "structured association" consisting of:

> an association that is not randomly formed for the immediate commission of an offence, nor does it need to have formally defined roles for its members, continuity of its membership, or a developed structure. (art. 1.2)

While these definitions encompass a wide range of phenomena through broad interpretations, they fundamentally enable the evaluation of organized crime primarily based on the seriousness of specific offenses. Focusing on the core nature of crimes rather than specific structural elements allows practitioners to concentrate on the practical aspects of combatting organized crime, thereby promoting implementable strategies (Sergi 2013; Lavorgna and Sergi 2014). However, Italian legal conceptions of organized crime, for example, focus on a mafia-style hierarchical model and assessing group structures (Sergi 2013; Lavorgna and Sergi 2014). I aim to shed light on the operational and structural dynamics of criminal actors involved in the Business Email Compromise, affiliated with the "Black Axe" gang.

Cybercriminal organizations and networks

In recent years, criminologists have disputed Grabosky's (2001) concept of "virtual criminality" as a mere rehash of existing criminal behavior in the context of cybercrime organizational structures. In particular, numerous studies have critically examined the presence of conventional organized crime structures within cybercriminal networks (e.g., Wall 2015; Lavorgna 2020). Research contends that the legal definitions of organized crime groups, as delineated in European article 1.1 and United Nations article 2 (a), examined by Lavorgna and Sergi (2014:18), fail to correspond precisely with the characteristics of online offenders. In contrast to mafia-style organized crime, which is distinguished by enduring and independent affiliations with rigid hierarchical systems, cybercriminal networks operate in the virtual domain with characteristics such as agility, dynamism, relative anonymity, and global reach (e.g., Leukfeldt et al. 2017a; 2017b; Lusthaus et al. 2023; Wall 2015). These attributes differentiate them from conventional mafia-like structures that rely on coercion and the threat of noncompliance (e.g., Leukfeldt et al. 2017a; Lusthaus et al. 2023; Wall 2015). Therefore, it can be concluded that cybercriminal networks deviate from the essential attributes associated with organized crime (Leukfeldt et al. 2017a; Lusthaus et al. 2023).

Levi's research,[1] conducted in 2008 and 2017, examines cybercrime networks, emphasizing a victim-centric typology and various fraud categories. The research systematically reveals the participants, environments, and cooperative endeavors of coconspirators involved in various fraudulent activities. Additionally, Levi investigates the organizational dimensions of distinct categories of fraudulent activities and scrutinizes how individuals establish connections with coconspirators and victims via remote and in-person exchanges. According to Levi (2017; 2008), the globalization of crime is due to interdependent connections between contexts, such as business, consumer, and investment patterns. Levi (2017; 2008) and Lavorgna and Sergi (2016) highlight a shift in the conceptualization of "organized crime," with the emphasis moving from structural attributes exclusively to the motivations

[1]Levi (2008) and Levi (2017) have identical titles and present similar arguments on the topic. Levi (2017) was published as a book chapter, while Levi (2008) was initially published as a journal article. I interpret the similarities between these works as indications of an evolution and expansion of ideas over time.

of individuals who engage in fraudulent activities in both illicit and lawful domains. Levi (2017; 2008) also acknowledges the presence of small mobile groups or individuals who can modify their methods to suit novel surroundings.

Similarly, Leukfeldt et al. (2017a) developed four growth models after analyzing 18 criminal investigations involving phishing and malware networks. Social connections remain crucial in facilitating the inception and expansion of numerous networks. Leukfeldt et al. (2017a; 2017b) state that cyberspace platforms, specifically forums, considerably contribute to network development by facilitating recruitment and interaction with enablers. Further investigating Dutch cases, Leukfeldt et al. (2017c) analyzed 22 cybercriminal networks operational in the United States, Germany, and the United Kingdom. The significance of social connections in forming networks was underscored by the research. Leukfeldt et al. (2017c) noted that networks frequently expand via social interactions or a blend of social interactions and specialized recruitment forums. It was determined that forums facilitate more adaptable modes of collaboration by allowing a restricted subset of fundamental participants to emerge as global participants. Also, Leukfeldt et al. (2017b) investigated 18 Dutch police investigations into phishing and banking malware networks in a separate study, differentiating between low-tech and high-tech networks with distinct distinctions. High-tech networks commonly comprise more global components, whereas low-tech networks predominantly function locally, according to the above authors (cf. Lazarus and Okolorie 2019). Low-tech and high-tech networks both contain specialized networks that concentrate on particular types of criminal activity, frequently with a regional rather than global scope (Leukfeldt et al. 2017b).

In a Vietnamese context, Nguyen and Luong (2021) studied cybercriminals by examining criminal profiles and conducting in-depth interviews with law enforcement officers. The study revealed that transnational computer fraud in Vietnam occurs both online and offline, with bank card fraud and phone scams being the primary methods. The organizational mechanisms of international computer fraud in Vietnam differ significantly from conventional organized crime models. The leadership dynamics within online purchasing networks were found to have a horizontal structure without a distinct hierarchical chain of command. This configuration, similar to Wall's (2015:71) notion of assemblage, corresponds to a "distributed" or "disorganized" network. Nguyen and Luong (2021) further elaborated that the leadership position within online purchasing networks showed flexibility, as some participants smoothly shifted between core members and enablers. However, bank card fraud and phone scam networks were more similar to conventional criminal organizations. Nguyen and Luong (2021) and Leukfeldt et al. (2017a) argue that cybercrime networks lack a clear leadership hierarchy, which sets them apart from typical criminal organizations such as Mafias, which have well-defined hierarchical structures.

In a Nigerian context, Lazarus and Okolorie (2019) conducted in-depth interviews with 40 law enforcement officers to shed light on cybercriminal actors' collaborative nature and modus operandi. Their study reveals distinctions between university-educated cybercriminals and their non-educated counterparts. University-educated individuals tend to collaborate and network with music celebrities, employ sophisticated technology, and pose challenges for prosecution. In contrast, non-educated actors collaborate and network more with spiritualists, use less advanced technology, and are comparatively easier to prosecute. Lazarus and Okolorie (2019) emphasize that the social organization of educated cybercriminals is more structured, leveraging existing relationships from their university era to recruit new individuals for criminal activities and money laundering. Consistent with Lazarus and Okolorie's (2019) research, Lazarus et al. (2023a:2) explained that cybercriminals (Yahoo Boys) do not adhere to "*a hierarchical mafia-style organizational model*" while engaging in various online fraudulent practices. Similarly, empirical investigations in the Ivory Coast (Cretu-Adatte et al. 2024) and the United Kingdom (Lusthaus et al. 2023) failed to find support for a hierarchical framework among online offenders. While offenders engage in collaborative efforts, they do not uphold a hierarchical system regarding the distribution of profits derived from their illicit activities.

While there are indications of labor division within cybercrime networks (Leukfeldt and Holt 2020), the research suggests that the durability and cohesion of these networks vary significantly. Core

members often engage in diverse activities such as hacking, extortion, and money trafficking, establishing enduring partnerships. However, networks lacking clear structure and distinct leaders tend to be transitory and of limited duration (Broadhurst et al. 2014; Zeng and Buil-Gil 2023).

Not all research uniformly supports the idea of nonhierarchical cybercriminal networks. Zeng and Buil-Gil's (2023) review of various articles elaborates that the structure of certain cybercriminal groups is driven by shared interests or goals rather than a hierarchical model centered around a single leader. However, this structure is not universal among all cybercriminal groups (Zeng and Buil-Gil 2023). Contrary to the perception of cybercriminal groups as frequently sporadic and loosely organized, researchers (Décary-Hétu and Dupont 2012; Zeng and Buil-Gil 2023) indicate that their core members maintain robust connections. The emphasis is on strong ties and relationships within the group rather than suggesting a high frequency of interactions or a rigid hierarchical structure (e.g., Décary-Hétu and Dupont 2012). Moreover, network boundaries are not always distinct, as cyber-offenders may establish communication with individuals external to the group, enhancing the network's resilience even without centralized actors (Décary-Hétu and Dupont 2012). For instance, Leukfeldt (2014) highlighted that some cybercrime enablers may originate from the legitimate economy, including postal workers and short-tenured bank employees, providing victims' information and modifying account settings to facilitate phishing.

Cybercriminal groups exhibit a disorganized and distributed model, with shared interests instead of central leaders (Leukfeldt et al. 2017a; Lusthaus et al. 2023; Wall 2015). These groups can vary in organizational complexity, from loosely connected entities with shared interests to highly interconnected core groups coordinating enablers through the division of labor (Zeng and Buil-Gil 2023). Research on cybercriminal networks challenges traditional organized crime definitions, highlighting the distinct nature of cybercrime characterized by fluidity, flexibility, and global reach (Lazarus and Okolorie 2019; Leukfeldt et al. 2017a; Levi 2017; Nguyen and Luong 2021). While cybercrime networks differ from conventional organized crime, which operates within a jurisdictional framework similar to the mafia (Wall 2015), focusing on cybercrime networks redirects analytical attention toward the foundational actors, relationships, and networks that comprise cybercrimes.

However, empirical evidence on traditional organized crime in cyberspace remains inconclusive, challenging conventional perspectives. It is also important to note that convicted cybercriminals are not well-studied, especially those in the West and linked to the Black Axe group. Hence, any information collected on this group is valuable, and it is worth exploring the activities of the "Black Axe Confraternity."[2]

The Black Axe Confraternity

The Black Axe Confraternity, originating from Nigeria, extends its influence globally (Cohen 2023; Ellis 2016). Known by various epithets such as the "most notorious" organized criminal group, the "most feared organized crime syndicate," and counted among the "more prominent confraternities/cults," it stands as an enigmatic and highly scrutinized organization within Nigeria's criminal landscape (Harper's Magazine 2019; BBC 2021a; Australian Government, Department of Foreign Affairs and Trade [DFAT] 2020; VICE 2015). It has also emerged as a social problem outside Nigeria (Cohen 2023; Ellis 2016).

However, the group's history is a subject of ongoing debate, contributing to a complex narrative of identity (Cohen 2023; Harper's Magazine 2019; BBC 2020). The Neo Black Movement of Africa (NBM), initially conceived as a movement championing the Black Power ideal (Ellis 2016), has evolved over the years, detaching itself from any specific political ideology (Ellis 2016; Harper's Magazine 2019; BBC 2020). Law enforcement officials have raised concerns about the NBM's association with the Black Axe Confraternity, linking them to increasing transnational organized crime and cybercriminal activities worldwide (Cohen 2023; Harper's Magazine 2019).

[2]In this article, I interchange the terms "confraternities" and "fraternities" when referring to groups like the Black Axe organization. My decision acknowledges that different terminologies are used in various contexts and includes different interpretations and descriptions of these groups within academic and media discourse.

The international perception of the NBM-Black Axe relationship differs; the United States (Harper's Magazine 2019) and Canadian authorities (VICE 2015) categorize the NBM as a "criminal organization," intertwining its fate with that of the Black Axe. However, the NBM vehemently denies these allegations, emphasizing its commitment to nonviolence and lawful activities (BBC 2021a; Vanguard 2022; Immigration and Refugee Board of Canada 2023). The group operates under aliases such as the Neo-Black Movement of Africa (NBM) (2022) and "Ayee," further complicating its identity (Immigration and Refugee Board of Canada 2023).

From campus cult to criminal enterprise

The origins of the "Black Axe" organization can be traced back to Nigerian universities (Cohen 2023). Specifically, founded in the 1970s at the University of Benin, Black Axe Confraternity was established by students with the aim of reducing oppression and racist actions in Africa and advancing research on local cultures and Traditional Spiritual Systems (Cohen 2023; Ellis 2016). But nothing lasts indefinitely. Surajo and Karim (2017) discovered that the group was involved in election violence, abuse of fellow students, and intimidation of staff. According to a participant in Ibrahim's (2017) study, who claimed membership in the Black Axe fraternity during his university days, campus cults were initially established to combat oppression and advocate for those too vulnerable to defend themselves. "*The beginning of cultism in Nigerian universities in those days was to fight against oppression, fight for people who were too weak to fight for themselves . . .*" (Ibrahim 2017:6). However, over time, a transformation took place, with cult members evolving into perpetrators of crimes.

Black Axe members have been implicated in a wide range of organized criminal activities, from running prostitution rings and engaging in human trafficking to grand theft, cyber-fraud, and money laundering (BBC 2021a; Meyers 2018). While many of these criminal activities are centered within Nigeria, their reach extends beyond national borders to countries like Canada and Malaysia (Ellis 2016; Meyers 2018). For example, both Canadian authorities (CBC News 2015) and Irish authorities (AML Intelligence 2024) have apprehended members of the Black Axe and exposed their participation in wire frauds, romance scams, and Business Email Compromises. Much information regarding the Black Axe organization, particularly its involvement in cybercrime, has emerged in recent years, primarily through media reports and law enforcement agencies outside Nigeria (BBC 2021a; CrowdStrike 2018).

Academic invisibility and media dominance

Academic literature focusing on the "Black Axe" organization is notably scarce (e.g., Cohen 2023; Ellis 2016; Meyers 2018; Surajo and Karim 2017). Academic discussions surrounding Black Axe members outside Nigeria predominantly revolve around topics like human trafficking and the management of Nigerian prostitutes in Western nations, such as Italy (e.g., Cohen 2023; Campana 2016; Ellis 2016; Meyers 2018; United Nations 2010). This disparity between academic research and media reports blurs the line between the media's portrayal of the "Black Axe" organization and its reality, resulting in significant challenges in discerning the true nature of the organization.

This divergence between academic study and media representation has implications for conceptualizing and understanding the "Black Axe" organization. It underscores the reliance on media and law enforcement agencies for the primary source of "authentic" information about issues such as crime (Ibrahim 2016:51; cf. Reiner 2010; Reiner 2016). Consequently, media discourse, often favoring cybercrime as newsworthy, tends to overshadow the organization's involvement in other criminal activities, like running prostitution rings. The rise of cybercrime in Black Axe's illegal activities can be attributed to the growth of the internet (Ellis 2016) and, perhaps, the transferability of some aspects of Nigerian 419 fraud templates from paper to digital format (Ibrahim 2016). There is a significant presence of Nigerian university students and graduates in online fraudulent activities originating from Nigeria and Nigerians abroad (e.g., Lazarus and Okolorie 2019; Ogunleye et al. 2019). The "Business Email Compromise" (BEC) is not only prominent among these online fraudulent activities but also popular among Black Axe syndicates (e.g., Vanguard 2021).

Business Email Compromise (BEC)

Business Email Compromise (BEC) schemes are exceedingly complex and sophisticated fraudulent operations. As defined by the Federal Bureau of Investigation, FBI (2018) and, Trend Micro and INTERPOL (2017), BEC involves an elaborate ruse where the perpetrator assumes the identity of a corporate executive or an employee through email communication. This deceptive act serves the purpose of fraudulently soliciting funds or gaining unauthorized access to confidential data. It is predicated on exploiting the victim's perception of authority, compelling swift and discreet compliance with instructions for financial transfers. Perpetrators display remarkable adaptability by assuming various deceptive personas, posing as high-ranking figures within organizations, including corporate executives, legal practitioners, or trusted suppliers. They tailor their deceptive methods to target specific individuals to maximize their illicit financial gains. These malefactors utilize BEC activities to acquire personally identifiable information, which is then traded on the Dark Web or used in fraudulent tax return submissions. These schemes often involve compromising the email accounts of employees in businesses or manipulating publicly accessible services to mimic the email domains of their chosen victims (Federal Bureau of Investigation, [FBI] 2018; Trend Micro and INTERPOL 2017).

The emergence of BEC schemes exemplifies the adaptability of criminals to the advancements of the digital age. In our contemporary digital landscape, a cohort of cybercriminals colloquially called "Yahoo Boys" primarily comprises individuals pursuing higher education. These cybercriminals leverage cutting-edge technologies to expand the reach of their illicit activities globally. This criminal paradigm encompasses a complex network of individuals performing diverse roles, including hacking, recruiting individuals with bank accounts to facilitate fund access, procuring "Trojans" and "malware" from the Dark Web, and acting as intermediaries between account holders and bank officials, as demonstrated by Lazarus and Okolorie (2019:21).

Nigerian cybercriminals can be categorized into two distinct groups: (a) "Yahoo Boys Digital" and (b) "Yahoo Boys Analogue." "Cyber-fraudsters who rely more on magical knowledge (Yahoo Boys Analogue) than technological knowledge may be facing a less certain situation in [online fraud schemes] than the Yahoo Boys Digital group" (Lazarus and Okolorie 2019:21–22). Examining social classifications is crucial to understanding the nuances of BEC schemes orchestrated by groups in Nigeria and beyond. Lazarus and Okolorie (2019) emphasize that "analog" cybercriminals often operate within a localized context, exploiting immediate opportunities and frequently lacking formal secondary education. In contrast, offenders operating within the "digital" crime field typically exhibit higher levels of education, showcasing a more sophisticated approach to their illicit activities. Apart from the above classification, Lazarus and Button (2022) researched the geographies of online offenders and demonstrated that a significant proportion of these two cohorts, both street-level and high-profile, originate from the southern region of Nigeria rather than the northern region.

Moreover, the role of high-profile Nigerians in BEC is worth noting. Essentially, there have been extensive media sensations about the centrality of high-profile Nigerian citizens regarding the BEC schemes and the evolution of these criminal methodologies in the digital domain (e.g., BBC 2021b; Bloomberg 2021). While entities, such as Yahoo Boys Digital, have been implicated in driving these fraudulent operations, impacting many businesses globally (e.g., BBC 2021b; Bloomberg 2021), Business Email Compromise (BEC) is underresearched. Cross and Gillett (2020) emphasize the need for research to address existing knowledge gaps in BEC research and practices for prevention and response.

First, the existing general body of literature on BEC is sparse. Second, there is no empirical research on the testimonies of scammers affiliated with the "Black Axe" organization, which originated in Nigeria. However, a vital empirical contribution to the limited body of work on the BEC has been made by Okpa et al. (2022). Okpa et al. (2022) analyze the impact of Business Email Compromise (BEC) scams on corporate organizations in Nigeria using qualitative and quantitative data. The findings revealed a significant increase in the number of BEC scam victims, which has severely

affected various industries such as banks, telecommunications corporations, and manufacturing firms. Okpa et al. (2022) highlight the significance of organizations' hiring process in assessing susceptibility to BEC scams. However, they did not investigate the culprits. My research provides insights into the perspectives of offenders.

In this present study, I analyze the structural, operational, and socio-cultural aspects of BEC scammers through the lens of two related theories: (a) Actor-Network Theory (cf. Callon 1986; Vicsek, Király and Kónya 2016) and (b) Social Network Theory (cf., Simmel 1964; Granovetter 1973 1983) to contribute to the existing limited body of empirical literature.

Theoretical background

Actor-network theory

Actor-network theory (ANT) explores the complex relationships and connections within a network, emphasizing the importance of both human and non-human actors (Callon 1986; Latour 1997; 2017; Vicsek et al. 2016). Within BEC networks, ANT provides a lens for understanding the intricate structural dynamics inherent in cybercrime networks. This framework illuminates the fluid and adaptive architecture characterizing BEC networks, which are marked by adaptability, specialization, and a clandestine structure. BEC networks exhibit features reminiscent of specific social network typologies, where participants assume diverse roles. Their operational efficiency lies in seamlessly transitioning between roles, resembling the operational flexibility seen in certain social networks. ANT proves instrumental in investigating the evolutionary trajectories of BEC networks, examining the flow of information and resources among participants, and discerning the role of adaptive structures in fortifying operational success (cf. Callon 1986; Latour 1997; 2017; Vicsek et al. 2016).

Social network theory

Social Network Theory places a strong emphasis on social connections, interactions, and the roles adopted by individuals within a network (cf. Simmel 1964; Granovetter 1973). The global nature of BEC cybercrime operations and the collaboration among cybercriminals from diverse geographical regions underscore the relevance of Social Network Theory. This framework elucidates the formation, operation, and adaptation of criminal networks that transcend national borders. My findings reveal that cybercriminals engaged in BEC schemes operate transnationally, often without comprehensive knowledge of their fellow network members' true identities or locations. Social Network Theory allows a nuanced exploration of the convoluted social connections underpinning these criminal collaborations. It also sheds light on the convergence of cybercriminals from different nations, their establishment of relationships, and their leveraging of collective expertise in online offenses. Additionally, the blurring of boundaries between online fraudsters and government representatives in specific regions underscores the substantial role of cultural and social factors in facilitating criminal enterprises. Social Network Theory provides a framework for understanding how these cultural and contextual influences shape the dynamics of criminal networks. It facilitates a deep dive into social ties, norms, and interactions that enable cybercrime activities.

Overlap between the two theories

While both Actor-Network Theory and Social Network Theory share fundamental commonalities in their focus on relationships, adaptability, and role specialization within networks, they diverge in scope and emphasis (Vicsek et al. 2016). I outlined the propositions of the two theories in Table 1.

Actor-network theory exhibits interdisciplinary versatility, addressing various network types, while Social Network Theory specializes in scrutinizing social relationships and interactions within networks within the social sciences (Vicsek et al. 2016). Actor-network theory's examination of social interactions

Table 1. Key propositions of actor-network theory and social network Theory*.

Theory	Key Propositions
Actor-Network Theory (ANT)	1. **Entities Actants**: ANT suggests that entities, both human and non-human, actively shape social phenomena. 2. **Network Dynamics**: Social phenomena emerge through dynamic interactions and relationships among actants in a network. 3. **Fluidity and Adaptability**: ANT emphasizes the fluidity and adaptability of networks, with relationships and entities constantly evolving.
Social Network Theory	1. **Social Connections**: Social structures and phenomena can be understood by examining connections and relationships between individuals or entities. 2. **Structural Patterns**: Patterns of ties, such as clustering, centrality, and density, impact individual and collective behavior within a social network. 3. **Information Flow**: Social Network Theory highlights the role of information flow through social ties, influencing the spread of ideas, behaviors, and resources.

*These propositions are broad summaries; the specific nuances of each theory can vary based on different interpretations.

and networks, incorporating the role of non-human actors, distinguishes it from more conventional sociological approaches. The two theories complement each other, offering a better understanding of the multifaceted dynamics inherent in BEC networks. Therefore, integrating both theories is appropriate.

Originality: how this present work contributes to and differs from prior contributions

This study contributes to the existing body of knowledge in the following ways. While prior studies have explored the narratives of self-proclaimed internet fraudsters within Nigerian university contexts (e.g., Aransiola and Asindemade 2011; Ogunleye et al. 2019), none have ventured to interview incarcerated cybercriminals within and outside Nigeria. Although many media outlets have drawn connections between internet fraudsters and the "Black Axe" organization (e.g., CBC News 2015; Toronto Sun 2018), academic research substantiating these associations through qualitative inquiry is conspicuously absent. Similarly, while a few non-empirical papers (e.g., Cross and Gillett 2020) and empirical investigations (e.g., Okpa et al. 2022) have explored Business Email Compromise (BEC), none obtained contextualized testimonies directly from BEC offenders to provide "real-life" insights.

Furthermore, existing empirical literature on cybercriminal networks and dynamics (e.g., Leukfeldt et al. 2017a; 2017b; 2017c; Lazarus and Okolorie 2019; Nguyen and Luong 2021), did not focus specifically on the topic of Business Email Compromise (BEC), except in "Case J," as reported by Lusthaus et al. (2023). Still, this study diverges from Lusthaus et al. (2023) in multiple ways. Unlike my investigation, Lusthaus et al. (2023) did not involve direct testimonies from any BEC perpetrator, and the BEC case they reported, "Case J," has no links to the Black Axe fraternity. Additionally, while Lusthaus et al. (2023) conducted a multi-case study, my research is only based on a single-case study. In spite of this numeric difference, my research adds value to the existing body of knowledge as it utilizes a unique dataset comprising direct testimonies of a high-profile offender affiliated with the 'hard–to–access' Black Axe gang. Using Actor-network and social network theories as analytical frameworks to explore BEC networks adds a layer of originality to this study.

Method and materials

Data collection and considerations

The limited availability of direct testimonies from incarcerated high-profile fraudsters associated with the "Black Axe" fraternity on the social dynamics of membership and remuneration within BEC schemes attributed to the exceptional value of such data. This research method follows a single case-study approach, central to developing various criminological fields. This is exemplified by Shaw's (1930/2013) seminal work and Carter's research (2021), each focusing on a single case (see also Marquart and Thompson 2024).

A few years ago, I received an initial email contact from a legal team representing a cybercriminal incarcerated in a prominent Western nation. This Nigerian national faced numerous charges related to Business Email Compromise (BEC) offenses and was in a detention facility awaiting sentencing. The law enforcement agency and the prosecutors identified him as the alleged leader of a cybercriminal syndicate affiliated with the "Black Axe" organization. The charges against the cybercriminal amounted to several millions of US dollars, primarily in various BEC schemes.

The legal team invited me to serve as an "expert witness" in the case. Before assuming this role, I consulted with senior academics in my network and researched the responsibilities associated with serving as an expert witness. Multiple virtual meetings with the legal team and a thorough review of official court documents were integral parts of my decision-making process. Ultimately, I accepted the role with the primary objective of enhancing my understanding of cybercriminals and the phenomenon of BEC by gaining insights from an experienced criminal actor. "*Neither condemn nor ridicule but try to understand*" (Thomas 1923:v), and such an attitude led me to the research path that produced this qualitative study. The absence of first-hand accounts from imprisoned high-profile scammers linked to the "Black Axe" organization involved in BEC scams can be attributed to the immense worth of this dataset.

As an expert witness, I assisted the court in achieving the overriding objective by providing objective and unbiased opinions on matters within my expertise. This duty was owed to the court and superseded any obligations to the party from whom I received instructions. My responsibilities encompassed a multifaceted approach, including the analysis of law enforcement-monitored phone conversations and WhatsApp messages. Additionally, I conducted multiple virtual interviews with the incarcerated cybercriminal, facilitated after obtaining the necessary clearance from prison authorities. The primary objective of these tasks was to decode cryptic messages into plain language and provide deeper insights into police interview records and phone records. These findings were triangulated with extensive interviews conducted with the offender, who had already entered a guilty plea to all charges except one area of disagreement – between the prosecuting and defending legal teams – according to the court's Statements of Agreed Facts. Consequently, the legal team and relevant authorities sought a deeper understanding of the case to inform the impending sentencing.

I engaged in extensive discussions with the legal team, including over 20 WhatsApp calls and standard video conferences, to deliberate on the subject matter. As an expert witness, I also ensured informed consent from the inmate before conducting the interviews, clearly articulating the research's academic purpose and guaranteeing the exclusion of direct quotes and identifying information. These interviews occurred on multiple occasions, with each session spanning approximately 240 minutes. To establish the operational parameters following my participant's sentencing, I rigorously implemented various anonymization measures within this article to safeguard the individual's identity and adhere to ethical standards. These measures entailed (a) excluding the individual's name and his place of origin in Nigeria, (b) extracting insights from the individual's statements instead of using direct quotes, and (c) referring to the nation of arrest and imprisonment as "*one of the Western nations*" instead. In addition, before I embarked on my dual role as an expert witness and researcher conducting the interviews, ethical approval was obtained from my university to conduct the study. Accordingly, all processes followed relevant guidelines and regulations, including the declaration of Helsinki and its revisions.

Data analysis

The data sets were thematically analyzed guided by Braun and Clarke's (2006) early work (involving (a) becoming familiar with the dataset, (b) generating initial codes, (c) searching for emerging themes, (d) reviewing and refining identified themes, (e) defining and labeling these themes, and (f) preparing the final analytical report). These steps provide a thematic description of discrete dataset components and elucidate overarching thematic patterns that encapsulate the entirety of the data before extracting insights from them. Although the primary source was interviewing data from the inmate,

I triangulated this data set with insights from tapped phone data and conversations with the legal team. To maintain a confidential agreement with the interviewee and his legal team before the interviews, I did not include direct quotes[3] from the interviewee – serving a jail term, the legal teams, tapped phone data, or any other document I accessed as an expert witness in the criminal case. Instead, I utilized insights from data to generate and discuss the themes outlined in Table 2.

Additionally, the interviewee was a high-profile figure linked to the dangerous and notorious Black Axe fraternity that has members all over the world. Therefore, it was essential for me to take the necessary precautions to ensure that I did not compromise the security of both the interviewee and myself, the researcher. In pursuing a nuanced understanding of cybercriminal networks, this study underwent meticulous analysis following the distinct stages outlined by Braun and Clarke (2006). The resulting analytical framework, encapsulated in Table 2, illuminates vital themes central to my investigation. Each theme is accompanied by a precise definition, a distinct label facilitating easy reference, and elucidative characteristics. Table 2 also serves as a guide into the subsequent section: the "Findings and Discussion."

Findings and discussion

My data analysis produced interconnected themes that mutually interact, forming a crucial foundation for the ensuing discussion. The main finding is a marked dynamism in the organization of BEC cybercriminal networks compared to traditional criminal models. The focal points of inquiry are the

Table 2. Thematic analysis summary map.

Themes	Definitions	Labels	Characteristics	Subthemes/Sub-Codes
Theme 1: The Fluidity of Structure and Adaptive Roles in BEC	Investigating the adaptability and fluidity of roles within Business Email Compromise (BEC) networks.	Structure and Adaptive Roles in BEC (1)	Role Flexibility and Adaptability, Fluidity in Network Boundaries and Resilience	(a) Role Flexibility and Adaptability (b) Fluidity in Network Boundaries and Resilience
Theme 2: Challenges in Visualizing Criminal Networks	Exploring difficulties in visualizing and understanding the structures of criminal networks.	Challenges in Visualizing Criminal Networks (2)	Passive Enablers and Parasitic Platform Criminality, Technological and Cultural Strategies	(a) Passive Enablers and Parasitic Platform Criminality
Theme 3: Globalization and Transnational Dimensions	Analyzing the global reach and complexity of cybercrime networks.	Globalization and Transnational Dimensions (3)	Global Operations and Network Complexity	None
Theme 4: Social and Cultural Influences	Investigating societal and cultural factors influencing cybercrime structures.	Social and Cultural Influences (4)	Technological and Cultural Strategies	None
Theme 5: Internal Cybersecurity Threats and Money Laundering	Examining internal threats within financial institutions and associated money laundering.	Internal Cybersecurity Threats and Money Laundering (5)	Financial Institution and Cybercriminal Manipulations, Continuity and Contrast: A Comparative Analysis	(a) Continuity and Contrast: A Comparative Analysis (b) Financial Institution and Cybercriminal Manipulations
Theme 6: Remuneration and Influences of Cryptocurrency	Exploring the impact of cryptocurrency on money laundering and repatriation of illicit funds	Remuneration and Influences of Cryptocurrency (6)	Influence of Cryptocurrency on money laundering and repatriation of illicit funds	None

[3]I understand the significance of relevant quotes in interview-based studies. However, I made a conscious decision not to include any direct quotations from the interviewee. This was due to the legal process I followed to obtain the data for research purposes.

sociological, structural, and organizational aspects of persons implicated in BEC fraud. Therefore, the subsequent discourse sequentially centers on these overarching themes and subthemes I outlined in Table 2. These themes shed light on the complex operations of cybercriminals affiliated with the infamous "Black Axe" syndicate.

The fluidity of structure and adaptive roles in BEC

The data analysis unveils intriguing insights into the organizational structures of cybercriminal networks, specifically the "Yahoo Boys." These structures markedly differ from the hierarchical frameworks commonly associated with traditional organized criminal groups like the Italian mafia (Campana 2016; Ellis 2016). What sets these cybercriminal networks apart is their exceptional fluidity and specialization. Within BEC cybercrime networks, roles exhibit remarkable flexibility and specialization, which are fundamental to their success. These networks are characterized by high specialization among participants and a covert, often concealed network system that is not easily discernible by law enforcement entities.

Within these networks, an individual leading one operation may seamlessly transition to a subordinate role in a different criminal endeavor, even when multiple operations run concurrently. This contrasts starkly with the rigid hierarchical structures often linked to traditional crime models (e.g., the Yakuza in Japan, the Bratva in Russia, the Triads in China, and the Mafia in Italy). Consequently, traditional crime paradigms inadequately capture the dynamic nature of Nigerian crime networks, which defy the stereotypical hierarchy. Instead, as per the interviewee, these networks showcase an exceptionally fluid and adaptable structure, particularly in the case of BEC cybercrime.

Implications extend to the remuneration structure, where, unlike traditional organized crime, compensation for BEC roles is variable and dependent on the perceived value of each function. The concept of cybercriminal networks operating within a jurisdictional framework distinct from traditional organized crime is evident in the literature (Lavorgna 2019; 2020; Lazarus et al. 2023a; Wall 2015; Whittaker et al. 2024). Precisely, playing a central role in some BEC transactions within a cybercriminal network does not necessarily imply leadership or governance of the entire organization, according to the testimonies of the interviewee. On the one hand, these findings align with previous studies investigating the interconnectedness of dating scammers, some Afrobeats musicians, and Yahoo Boys, illustrating a departure from the conventional mafia-style hierarchical model (Lazarus et al. 2023a). On the other hand, these findings align with the broader literature on cybercrime networks, emphasizing the importance of social connections in forming and expanding networks (Cretu-Adatte et al. 2024; Leukfeldt et al. 2017a; 2017c; Nguyen and Luong 2021). The fluidity and adaptability described align with the dynamic nature of cybercrime networks revealed in both the current research and the broader literature.

The discussion of fluidity and specialization in BEC cybercrime networks adds nuance to understanding cybercriminal organization models, echoing the insights derived from various studies on cybercrime networks' organizational structures (Cretu-Adatte et al. 2024; Lazarus and Okolorie 2019; Leukfeldt et al. 2017a; Lusthaus et al. 2023; Nguyen and Luong 2021). The findings from this research align with existing literature on cybercriminal networks, emphasizing their unique fluidity and adaptability. The in-depth analysis of BEC cybercrime networks contributes to the broader understanding of cybercriminal organization models, showcasing the exceptional nature of these networks within the cybercrime landscape. The identified fluid and adaptable structure within BEC cybercrime networks is a pervasive characteristic across a broader spectrum of activities undertaken by Internet fraudsters, collectively known as Yahoo Boys. These discoveries challenge established notions of the criminal organization and offer insights into the nature of cybercriminal networks involved in BEC, aligning with other subsets of online offenders. This fluidity of structure is closely linked to role flexibility and adaptability.

Role flexibility and adaptability

The data analysis highlights a pivotal aspect of BEC schemes: the remarkable adaptability and flexibility displayed by the individuals involved. An individual who assumes a specific role in one transaction may readily transition into an entirely different role in another context, mirroring the network's inherent adaptability and fluidity. This fluid organizational structure enhances maneuverability and operational efficiency, allowing the network to function swiftly and effectively.

In cases where a specific role cannot be filled with available talent in a given region, recruiters seek candidates from the broader "Black Axe" network. With many members located worldwide, the "Black Axe" network offers diverse expertise to execute BEC transactions involving its members in various nations. This strategic and logistic value of the "Black Axe" network aligns with Social Network Theory's emphasis on weak ties, which provide information about job opportunities unavailable within one's close-knit network (cf. Granovetter 1983).

BEC networks exhibit a profound ability to dissolve and reconfigure their structures with each new transaction, a characteristic that ensures the network's enduring flexibility and dynamism. This adaptability finds its historical roots in criminal templates, such as the "419 fraud templates" from the 1980s, as observed by Ibrahim (2016:54). This very adaptability, fluidity, and heightened maneuverability have significantly contributed to the success of BEC scams in recent years. This bears a resemblance to Actor-Network Theory (cf. Latour 1997; 2017).

The utilization of the Actor-Network Theory analytical framework aligns with the dynamic circulation of information and resources among the BEC network's participants, shedding light on the pivotal role of adaptable and flexible structures in fortifying operational efficiency (cf. Callon 1986, Latour 1997; 2017; Vicsek et al. 2016). The "Fluidity and Adaptability" aspect of actor-network theory emphasizes the fluidity and adaptability of networks, with relationships and entities constantly evolving. Thus, the Actor-Network Theory is a valuable tool for understanding BEC organizations' complexity, fluidity, flexibility, and adaptability. It provides a lens through which researchers can explore how these networks adapt and evolve, highlighting the dynamic nature of their operations and the strategies employed to maintain efficiency in the face of changing circumstances. Furthermore, the manifestations of social interactions and networks that encompass both human and non-human actors, such as objects and technologies, are in harmony with the Actor-Network Theory, which distinguishes it from more traditional sociological approaches. These insights illuminate the dynamic nature of BEC operations and underscore the importance of adaptability in the continued efficacy of such criminal networks. The transnational character of criminal networks is closely related to actors' flexibility.

Additionally, these findings resonate with the broader literature on cybercriminal organizations and networks, emphasizing the importance of adaptability and flexibility in criminal enterprises (Leukfeldt et al. 2017a; Lusthaus et al. 2023). The discussion of BEC networks' ability to dissolve and reconfigure aligns with the dynamic nature of cybercriminal organizations described in the literature, reinforcing the idea that adaptability is a key characteristic of successful criminal networks (Leukfeldt et al. 2017a; Lusthaus et al. 2023). This further confirms the unique nature of BEC networks within the broader context of cybercrime.

Fluidity in network boundaries and resilience

The examination of BEC cybercrime networks reveals a noteworthy feature in the fluidity of network boundaries and the resulting resilience. Unlike traditional criminal organizations with clear delineations, cyber-offenders within BEC networks often establish communications beyond the group, enhancing the network's resilience without centralized actors. This characteristic is not only observed in the context of BEC but is also recognized in broader studies on cybercriminal networks (e.g., Décary-Hétu and Dupont 2012; Leukfeldt 2014).

The ability of cybercriminals to communicate with individuals external to the group contributes to the adaptability and longevity of the network. This fluidity in network boundaries is crucial in navigating the

dynamic landscape of cybercrime, allowing for collaboration with external actors when necessary. Such characteristics resonate with the broader canon of cybercriminal psychology and innovations (e.g., Décary-Hétu and Dupont 2012; Leukfeldt 2014).

Moreover, the role of enablers from the legitimate economy, such as postal workers and short-tenured bank employees, aligns with the notion that cybercrime networks often extend their reach beyond the immediate confines of the criminal group (Leukfeldt 2014; Wang, Su, and Wang 2021). Including these enablers in the network contributes to its resilience and adaptability, as their involvement adds a layer of complexity that enhances the network's ability to navigate legal and logistical challenges. The fluidity in network boundaries observed in BEC cybercrime networks is a strategic adaptation that promotes resilience and longevity. These characteristics emphasize the interconnected nature of cybercrime beyond traditional organizational boundaries. These insights complement existing literature on cybercriminal organizations and networks, reinforcing that fluid boundaries contribute to criminal networks' overall resilience and adaptability (Décary-Hétu and Dupont 2012; Leukfeldt 2014; Tropina 2012).

Challenges in visualizing criminal networks

Understanding the organizational structures of cybercriminal networks, especially within BEC schemes, presents unique challenges. Unlike traditional organized crime groups, these networks lack hierarchical structures that can be easily visualized. The BEC networks demonstrate a remarkable degree of fluidity and specialization, making them difficult to categorize using conventional models.

Drawing upon Actor-Network Theory, which emphasizes the dynamic circulation of information and resources among network participants, the BEC networks lack the rigid hierarchies often found in traditional organized crime groups. In contrast, BEC networks are marked by a high degree of specialization and a network system that remains concealed from external scrutiny. The interplay of various roles within these networks is fluid and adaptable, with individuals readily transitioning between roles in different criminal endeavors. This dynamic nature contrasts the rigid hierarchical structures often associated with Western crime models. This fluidity in roles and adaptability can be understood through the lens of Social Network Theory, which emphasizes the importance of weak ties. Within BEC networks, individuals seamlessly move between roles, optimizing the network's effectiveness.

Interview narratives shed light on the perspective that BEC criminal networks typically elude the purview of law enforcement entities, aligning with existing literature on traditional organized crime. For example, previous research (Campana 2016; Campana and Varese 2012) on Nigerian organized crime networks in Italy, where the roles and structures are often ambiguous to the Italian police force dealing with various criminal activities, such as prostitution and human trafficking. This perspective became evident through a comparative analysis of intercepted WhatsApp messages on tapped phones and the conclusions drawn before in-depth interviews with the offender. Visualizing criminal networks involved in BEC scams is a formidable challenge because they largely remain concealed from external observation. Any attempts at visual representation can lead to inaccuracies in attributing specific characteristics, thus posing substantial challenges for ensuring external validity. Consequently, frequently resorting to information from external interviews with offenders, their associates, and key informants can be more effective than relying heavily on tapped phone information in isolation. This approach facilitates a comprehensive understanding of these complex criminal networks by amalgamating content from intercepted phone calls and messages with metadata.

These challenges align with the complexities highlighted in the existing literature on traditional organized crime, emphasizing the elusive nature of criminal networks and the need for innovative approaches in visualization (Campana 2016; Campana and Varese,*2012*). Actor-Network Theory and Social Network Theory share fundamental commonalities in their focus on relationships, adaptability, and role specialization within networks (Vicsek et al. 2016). Therefore, both lenses align with the fluid and specialized dynamics of BEC networks. They offer insights that can guide the development of more effective visualization strategies, aiding in understanding and analyzing BEC network structures and behaviors.

Passive enablers and parasitic platform criminality

Analysis of interview data exposes a discernible schism within the realm of BEC operations. This schism distinguishes between individuals who consciously facilitate criminal activities and those who, often inadvertently, become unwitting enablers, contributing to the world of cybercrime without full awareness. Professionals such as bankers, and accountants are among these enablers of cybercrime, which is consistent with previous studies like Wang, Su, and Wang (2021). In their legitimate careers, they may choose to avert their gaze from the presence of cybercrime enterprises rather than report them, thus acting as passive agents in the cybercriminal landscape. For instance, consider the accountants who, while conducting business on behalf of a cybercriminal entity, deliberately overlook its nefarious activities, effectively condoning cybercrime.

Furthermore, the interviewee underscored the emergence of a converging trend in criminal activities within the digital landscape. The narratives provided by the interviewees illuminate a phenomenon best characterized as parasitic platform criminality,[4] where cybercriminals turn legal apps offered by platform providers into a discordant symphony of malice to advance their unlawful pursuits (cf. Cyware 2019; The Register 2018). The advent of this type of illicit innovation not only imperils the reputation and integrity of these industry giants such as Apple, Google, and Yahoo but also exposes their vulnerable facets. Its manifestation is evident in the proliferation of scams infiltrating these platform providers' ecosystems and the widespread misuse of their technological resources. Insights from my data analysis indicate that dominant platform providers have become a target for a multitude of cyber scams, and their resources are frequently abused to support nefarious cyber activities.

Navigating the landscape of cybercriminal networks reveals not only the passive enablers and parasitic platform criminality but also the fascinating technological and cultural strategies employed within BEC operations. The intricate landscape of cybercriminal networks, as explored in the general literature[5] regarding cybercriminal networks (Leukfeldt et al. 2017a; 2017b; Nguyen and Luong 2021; Lazarus and Okolorie 2019), underscores not only the presence of passive enablers but also the phenomenon of parasitic platform cybercriminality. This dynamic interplay aligns with discussions in the literature on the evolving nature of cyber threats and the challenges legitimate platforms face in safeguarding their ecosystems. The similarity between insights from the broader canon of the empirical literature on cybercriminal networks (Cretu-Adatte et al. 2024; Lazarus and Okolorie 2019; Leukfeldt et al. 2017a; Nguyen and Luong 2021) and my study on Business Email Compromise scams places this study's findings into a broader context, shedding brighter light on the multifaceted strategies employed within cybercriminal operations globally.

Globalization and transnational dimensions

The data analysis sheds light on the sophisticated and transnational character of cybercriminal networks, exemplified by the "Yahoo Boys" activities involved in BEC actions. This international BEC network revolves around the broader "Black Axe" organization, facilitating its transnational nature. The BEC operation includes individuals from diverse geographical locations, such as Canada, Australia, the United Kingdom, the United States, and Nigeria, all concurrently participating in BEC operations, as revealed in the interview data. Business Email Compromise offenders demonstrate a global operational reach. For example, insights from interviews indicate that individual cybercriminals often lack knowledge about their collaborators' true identities or physical locations. However, this changes when collaboration is recommended among members of the Black Axe fraternity. The multi-layered complexity observed among Business Email Compromise (BEC) offenders underscores a recurring theme in the broader literature on online offenders and their actions, such as Ibrahim

[4]The term "parasitic platform criminality" was introduced in an unpublished project proposal on online fraud in 2022 by S. Lazarus, M.R. McGuire, M. Edwards, and J.M. Whittaker.

[5]While the general empirical literature on cybercriminal networks has not focused specifically on Business Email Compromise, Lusthaus et al. (2023) reported Case J, which highlights the uniqueness and value of my contribution.

(2016), Nguyen and Luong (2021), Yar and Steinmetz (2019), Hall et al. (2021), Hall and Scalia (2019), Wall (2021), Lazarus (2022), Lazarus et al. (2023b), Button, Hock, and Shepherd (2022), Wang and Topalli (2024), and Whittaker et al. (2024). This broader canon of literature has consistently emphasized the transnational and transcontinental dimensions of cybercrime and the origins of both cybercriminals and their victims.

Interview narratives shed light on the diverse roles inherent in BEC transactions, ranging from identifying potential victims to managing the distribution of illicit gains among participants. (a) Key positions within this network include recruiters ("handlers" according to law enforcement terminology) responsible for enlisting money mules, particularly international students willing to lend their bank accounts, including online banking details for BEC transactions. The recruiter or handlers also maintain records on assignment completion, acting as a liaison between the manager and the conduit. (b) Conduits play another critical role in facilitating the execution of these illicit operations. The conduits also act as liaisons between the handlers and managers. (c) Managers play a pivotal role in handling the transaction's business aspects and taking directives from the primary source of information that leads to the operation. The managers liaise with other criminal actors, often in foreign jurisdictions, such as characters that are the primary source of information that leads to the operation or hackers who steal funds from legitimate businesses (e.g., victims).

The roles of the criminal actors performing as conduits, recruiters, and managers interchange depending on how their expertise aligns with a role in a single Business Email Compromise transaction at one point in time and space. An intriguing facet emerges in remuneration, where compensation for these roles depends on the perceived value of each function within the context of a specific transaction. This arrangement results in significant variations in compensation from one operation to another rather than being based on role titles (e.g., conduit, recruiter, or manager). These above insights resonate with the existing empirical literature on cybercriminal networks and their diverse roles, ranging from identifying potential victims to governing the distribution of illicit funds among criminal actors (Leukfeldt et al. 2017a; 2017b, Lusthaus et al. 2023; Nguyen and Luong 2021). While my discoveries align with the existing empirical literature (e.g., Leukfeldt et al. 2017a; Lusthaus et al. 2023; Nguyen and Luong, *2021*) regarding the organization, structure, and dynamics of cybercriminal networks, my research distinguishes itself from prior studies by focusing specifically on Business Email Compromise (BEC) operations. The cultural influences on BEC schemes are worthy of examination.

Social and cultural influences

Understanding the elastic strategies employed in BEC operations necessitates a profound exploration of the complexities involved, including social and cultural influences. In this regard, gaining insights into the roles of platform crime enablers, their distinctive contributions, and the influence of regional and cultural factors on their activities is imperative. For instance, while technologically proficient cybercriminals exploit Google's applications for money laundering and repatriating illicit gains, online fraudsters utilize tools like Google Translate and Google Maps to identify locations for recruiting potential participants or informants (Cyware 2019; The Register 2018). In addition to the above tools, more sophisticated tools such as deepfakes come into play in BEC operations, involving fabricated images for video calls with employees from targeted companies, according to the interviewee.

Contrary to supernatural techniques, such as the "Yahoo Plus" method described by Agunbiade and Ayotunde (2011), Lazarus (2019), and Akanle and Shadare (2019) in the context of BEC operations, the interviewee emphasized that individuals involved in Business Email Compromise (BEC) cybercrime rarely use such tactics when interacting with victims. However, Black Axe-affiliated BEC scammers use supernatural tactics merged with violence to assert dominance over co-offenders who may contemplate deviating from previously established agreements. While some internet fraudsters involved in various illicit schemes have integrated supernatural strategies (Yahoo Plus approach) to manipulate victims (cf. Agunbiade and Ayotunde 2011; Lazarus et al. 2023a). BEC cybercriminals, particularly those classified as Yahoo Boys Digital, typically refrain from using supernatural methods

to defraud victims. In contrast, the Yahoo Boys Analogue group frequently incorporates such strategies, as discussed by Lazarus and Okolorie (2019). This classification has implications for a deeper understanding of the vulnerabilities of victims within the BEC domain.

The synthesis of these technological, cultural and spiritual strategies, as discussed in the literature (Agunbiade and Ayotunde 2011; Akanle and Shadare 2019; Lazarus 2019; Lazarus and Okolorie 2019; Lazarus et al. 2023a), offers a transferable helpful perspective on the dynamic nature of BEC operations. It underscores the adaptability of cybercriminals in leveraging diverse tools and approaches, taking into account regional variations and cultural nuances. These insights contribute to a nuanced understanding of the strategies employed within BEC networks, shedding light on the evolving tactics in the cybercriminal landscape.

Internal cybersecurity threats and money laundering

Cybercrime has a spatial dimension, occurring within and across localities, influencing behaviors within spaces, and being concealed or exposed by spatial and cultural forces (Hall and Yarwood 2024 Lazarus and Button 2022). Context serves as a valuable asset for understanding. The demarcation between online fraudsters and government representatives, particularly in money corruption, laundering, and fraud, has become increasingly blurred in West Africa. Extensively documented in prior research on the illicit actions of influential members of society, including politicians, celebrity statecrafts, and internet fraudsters (e.g., Lazarus, Button and Adogame 2022; Lazarus and Button 2022; Zakari and Button 2022), this phenomenon is further affirmed by the findings of this study. The interview data confirms that BEC offenders in the West collaborate with representatives of authority and celebrity figures in Nigeria, such as musicians. First, the above finding aligns with previous research on the interconnected relationship between online fraudsters and Afrobeats musicians (Lazarus 2018; Lazarus et al. 2023a). Interviews with 40 law enforcement operatives indicated that these musicians and online fraudsters share common interests and engage in mutual economic practices, including money laundering (Lazarus and Okolorie 2019). Second, it also aligns with the "Network Dynamics" aspect of actor-network theory, which suggests that social phenomena emerge through dynamic interactions and relationships among actors within a network. Therefore, "Network Dynamics" offers a valuable framework for understanding the complexity of interactions between BEC offenders in the West and their collaborators in Nigeria (cf. Latour 1997; Callon 1986; Vicsek et al. 2016).

To better grasp criminal organizations' adaptability, one must navigate the convoluted interplay of local and global influences. Key dimensions like local culture, politics, celebrity statecraft, and utilitarian interests shed light on the significance of organized crime within a globalized context. The interplay of BEC-oriented money laundering and contextual factors within Nigeria emerges as a significant facilitator in these multifaceted criminal enterprises, exposing the inherent intricacy of the issue. In West Africa, the collaboration between cyber fraudsters and certain government representatives in financial crimes blurs traditional boundaries, fostering an environment conducive to the unrestricted practice of money laundering and fraud. The interviewee revealed that certain prominent Nigerian figures were implicated in laundering the proceeds of BEC scams, which echoes the perspective put forth by Lazarus, Button, and Adogame (2022:8): The distinction between purported non-offenders and cybercriminals is ambiguous, making it difficult to classify the actions of cybercriminals as a distinct "subculture" separated from the prevailing societal norms.

Although the Black Axe Confraternity, akin to traditional criminal gangs, employs coercion to enforce governance and further their objectives, the operational and contextual conditions in West Africa differ significantly from practices observed in Western jurisdictions. The interviewee underscored that individuals in authoritative positions, such as accountants or bankers, participate in illicit activities in Nigeria in a manner distinct from their counterparts in Western countries. While cybercriminals affiliated with groups like "Black Axe" may employ persuasive tactics to

secure cooperation in the West, encountering minimal resistance, the situation contrasts in Nigeria, where participants typically engage willingly, lured by the opportunity to augment their income through involvement. This discrepancy may arise because many Nigerians struggle to differentiate between the fraudulent activities of internet scammers (Yahoo Boys) and figures of authority, particularly politicians who are referred to as "*Yahoo Men*" (Lazarus, Button, and Adogame 2022; Lazarus 2023). Nigerians' skepticism stems from perceived similarities between the two cohorts (Yahoo Boys and Yahoo Men) in their expertise in scamming people. However, such comparisons may not hold true for many Westerners. Without a doubt, contextual public perception regarding internet scammers and governmental figures offers valuable insights into the diverse manifestations of such collaborations.

Continuity and contrast: a comparative analysis

My exploration of BEC's dynamics reveals the interconnectedness between local influences and the broader canvas of globalized criminal activities. In contrast to Lusthaus et al. (2023:14), who lacked sufficient details on foreign jurisdictions to ascertain the potential involvement of corrupt law enforcement agents or government officials in protecting overseas network members, my interview data fills this crucial gap. Lusthaus et al. (2023) observed that "*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*" (Lusthaus et al. 2023:14). In contrast, my research provides the aforementioned details, which are unavailable in Lusthaus et al. (2023). This study does so, by interviewing the high-profile and Black Axe affiliated Business Email compromise (BEC) offender beyond the parameters of the court's Statements of Agreed Facts. My research provides valuable insights into cybercriminal enterprises through direct and contextualized testimonies from critical figures within the BEC enterprise I interviewed.

In alignment with the findings of Lusthaus et al. (2023) "Case J," my data analysis recognizes the ongoing adjustments within cybercriminal networks to navigate shifts in bank payment thresholds and address practical challenges, such as evading security measures like double authentication for account payment changes. While sharing commonalities with the Lusthaus et al. (2023) case study, this investigation distinguishes itself by presenting analysis derived from the direct testimonies of a critical figure in the cybercriminal syndicate associated with the rarely studied Black Axe fraternity, providing unique insights. My analysis of data also aligns with Lusthaus et al. (2023) observation that criminal connections within cybercrime schemes exhibit varying durations, encompassing short-lived and transactional partnerships to longer-term alliances. Particularly noteworthy are the partnerships that often emerge between the "managers" of cybercrime schemes and their cashing-out providers, forming distinct yet allied groups. The above alignment, by implication, puts the findings of this study into a broader context.

Financial institution and cybercriminal manipulations

Under the canopy of Western financial institutions, specific individuals collaborate willingly or unknowingly with external entities. These individuals often provide external criminal actors with opportunities to identify vulnerabilities and exploit them for financial gain, all while maintaining a low risk of detection. The revelations illuminate instances where individuals in positions of trust have divulged sensitive information to those affiliated with cybercriminal networks. The dynamics of these collaborations within the financial sector align with insights from Social Network Theory, which emphasizes the relationships and connections between individuals and organizations (Granovetter 1983; Vicsek et al. 2016). Recruits, often sourced from establishments in Western nations, may have participated in these activities under various forms of coercion, including experiences of minor sexual duress and engagement in deceptive information-seeking tactics. For instance, a high-profile prostitute might be compensated for extracting information from their target.

Therefore, cybercriminal networks, closely associated with the infamous "Black Axe" organization, wield substantial influence in this sophisticated landscape. These networks actively facilitate and manipulate these criminal liaisons, fostering a covert environment where cooperation with individuals often coerced or deceived becomes common. This manipulation of individuals is further illustrated by the scripts and tactics devised by the cybercriminal networks, orchestrating the exploitation of sensitive information while shielding the perpetrators from detection.

Remuneration for roles and influences of Cryptocurrency

Cryptocurrency transcends jurisdictional banking constraints (Butler 2022; Foley et al. 2019). It enables and protects illicit e-commerce (Foley et al. 2019) Cryptocurrency's influence on money laundering and repatriating illicit gains reshapes traditional practices through strategic integrations. The narratives of the participant in this study articulate the intersectionality between money laundering and repatriating illicit gains and the strategic incorporation of cryptocurrency. These narratives highlight that the fluidity of cryptocurrency is a valuable asset within the money laundering ecosystem. This transformative impact of cryptocurrency unfolds through various mechanisms, each contributing to a nuanced reconfiguration and fortification of money laundering and repatriating illicit gains. Decentralized financial transactions, exemplified by the use of cryptocurrencies like Bitcoin, empower BEC organizations to orchestrate decentralized financial dealings, challenging the historical reliance on centralized financial systems prevalent in traditional organized crime groups. Introducing pseudonymity and anonymity in cryptocurrency transactions not only disrupts the traditional hierarchical structure but allows participants in BEC schemes to engage without necessarily revealing their true identities while sharing and repatriating illicit gains. This departure from explicit identification reflects a dynamic shift discussed by Foley et al. (2019).

Furthermore, direct peer-to-peer transactions facilitated by cryptocurrencies eliminate the need for intermediaries and central authorities, fostering more sophisticated ways of money laundering and repatriating illicit gains to their desired locations. This finding aligns with the transformative impact of Bitcoin, in general, discussed by Butler (2022). Cryptocurrencies enable BEC organizations to collaborate worldwide, transcending geographical and jurisdictional limitations (cf. Butler 2022; Foley et al. 2019, who did not inquire about the Business Email Compromise or online scammers). Moreover, reduced dependence on traditional banking systems, according to the interviewee, further underscores the parallel transformative impact of Bitcoin on money laundering and repatriating illicit gains. Additionally, according to the interview data analysis, adopting cryptocurrency opens avenues for broader participation, attracting a more expansive array of participants, including those hesitant to engage in traditional criminal activities involving bank-to-bank transfers. It spotlights not only lower entry barriers in BEC schemes, but also cryptocurrency's influences on money laundering and repatriating illicit gains.

Limitations and constraints

However, my study, employing a series of interviews with a single participant, has three main limitations:

(a) **Reliance on Self-Reported Data**: The study heavily relies on self-reported data from the interviewed cybercriminal. There is an inherent risk in the accuracy and truthfulness of the information provided, as the interviewee, a convicted cybercriminal, may present distorted narratives for various reasons, including self-preservation.
(b) **Ethical and Security Considerations**: While efforts have been made to anonymize the participant, the ethical and security implications of engaging with a convicted criminal for research purposes need careful consideration. The interviewee is a member of a notorious and

violent gang, Black Axe Confraternity. Therefore, I needed to take the necessary precautions, such as referring to the nation of arrest and imprisonment as "*one of the Western nations,*" to ensure that I did not compromise the security of the interviewee and myself, the researcher (see the "*Data Collection and Consideration*" section).

(c) **Absence of Diverse Perspectives**: Even though efforts were made to triangulate data with tapped phone data and conversations with the legal team, my study lacks diverse perspectives, as it relies solely on the insights of a single participant. The absence of contrasting views or experiences within the BEC criminal networks might have limited the breadth of the research findings.[6] I acknowledge the above limitations and constraints for interpreting the study's findings and considering the context in which the research was conducted.

Conclusion

This research explored the Business Email Compromise (BEC) cybercrime networks, working within the limitations of what is available (a small sample size, $n = 1$). The study revealed significant aspects that enhance our comprehension of this intricate matter. BEC networks defy conventional hierarchical models of organized crime and are characterized by fluidity and adaptability. Both Actor-network theory and social network theory have been instrumental in shedding light on the fluid and adaptive nature of these networks, emphasizing the role flexibility and adaptability of individuals within them. I highlighted cultural and social factors as profound influencers on the activities of cybercriminals in this domain.

The global scale of these BEC networks, their ability to shift and adapt their structures, and the convergence of various roles underscore their adaptability. BEC scammers' adaptability is deeply rooted in historical criminal blueprints. The invisibility of these networks adds an additional layer of complexity to this phenomenon. This study has decoded the inner workings of these cybercriminal networks by drawing insights from direct testimonies of the perpetrators and their associates, complemented by metadata analysis.

A distinction between conscious and unconscious enablers within the BEC and online fraud has emerged. This distinction has illuminated the convergence of criminal activities within the digital domain, emphasizing the influence of regional and cultural factors. Although cyber spiritualism was uncommon in BEC schemes, technological instruments, networks, and social engineering were identified as the primary drivers of these scams. This finding aligns with the classification proposed by Lazarus and Okolorie (2019:20), which distinguishes between "*Yahoo Boys Analogue*" and "*Yahoo Boys Digital*." Unlike the "Yahoo Boys Digital" group, such as BEC scammers primarily relies on information technology to defraud victims, the "Yahoo Boys Analogue" group predominantly employs supernatural strategies.

Furthermore, the study has emphasized blurred boundaries between cyber fraudsters and government representatives, especially in regions like West Africa, reflecting the complexity of this issue interwoven with cultural and contextual nuances. This convergence poses multifaceted threats, not only to the security and reputation of legitimate platforms but also to the broader global digital ecosystem. Internal threats within financial institutions have far-reaching consequences in our interconnected world. Trust emerges as a precious commodity, and the impact of cyberattacks extends beyond monetary losses to affect job markets, societal fabric, and the elements of our digitalized world. Such real-life repercussions have further implications. Police forces generally lack cross-border powers, making it challenging to tackle cybercriminals without relying on intelligence from outside their boundaries.

[6]This limitation arises from the confidentiality agreement I entered into with the interviewee and their legal team before the series of interviews I conducted as an expert witness seeking data for research purposes. In my capacity as an expert witness, I followed a legal procedure to procure data from the case for research pertaining to the high-profile cybercriminal linked to the "Black Axe" fraternity. The distinctive circumstances of the case preclude me from conducting interviews with individuals who possess knowledge of the cybercriminal, as he has already been sentenced, especially – in case the inmate decides to appeal.

Lastly, recognizing the depth of these multifarious losses underscores the significance of robust cybersecurity measures and the preservation of trust in an increasingly digitized global landscape. The findings of this study provide a substantial contribution to our understanding of BEC networks and the intricate challenges they pose in the contemporary digital milieu. This research has contributed by exploring incarcerated individuals' narratives in internet fraud, validating connections between internet fraudsters and the "Black Axe" group, and analyzing BEC networks' structural and operational dynamics. These contributions are unique (see "*Originality: How this present work contributes to and differs from prior contributions*" section). Findings derived from this study have implications beyond academia. They are relevant to law enforcement agencies and policymakers who are engaged in the fight against cybercrime. Additionally, insights from this study are vital in aiding decision-makers in understanding how their organizations may better approach BEC scams, appreciate victims' vulnerabilities, and support employees both before and after an incident. While this study provides valuable insights, it also points to the need for further research to shed light on the evolving landscape of BEC scams and cybercrime in general.

Acknowledgements

Dr. Peter Tickner provided valuable feedback on my manuscript, which I greatly appreciate.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Dr. Suleman Lazarus holds a Ph.D. in Cybercrime and Criminology from the University of Portsmouth, UK. He serves as an Associate Editor for the Association for Computing Machinery (ACM) journal "Digital Threats: Research and Practice." He is a visiting fellow at the Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), and he is also undertaking postdoctoral research at the University of Surrey, UK. Dr. Lazarus created the "Tripartite Cybercrime Framework (TCF)," categorizing cybercrimes into socioeconomic, psychosocial, and geopolitical motivational groups. He has authored numerous peer-reviewed articles in journals such as "Telematics and Informatics" and "Cyberpsychology, Behavior, and Social Networking." Dr. Lazarus's research focuses on cybercriminals and society. Additionally, he integrates poetry with academic discourse, as demonstrated in his work published in "Methodological Innovations." He tweets at @DrSLazarus.

ORCID

Suleman Lazarus http://orcid.org/0000-0003-1721-8519

References

Aborisade, R. A. 2023. "Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of parents' Disposition Towards children's Involvement in Cybercrimes." *Deviant Behavior* 44(7):1102–20. doi:10.1080/01639625.2022.2144779

Agunbiade, M. O., and T. Ayotunde. 2011. "Spirituality in Cybercrime (Yahoo Yahoo) Activities Among Youths in South West Nigeria." Pp. 357–80 in *Youth Culture and Net Culture: Online Social Practices*, edited by E. Dunkel, G.-M. Franberg and C. Hallgren. Hershey: IGI Global.

Akanle, O. and B. R. Shadare. 2019. "Yahoo-Plus in Ibadan: Meaning, Characterization and Strategies." *International Journal of Cyber Criminology* 13 (2): 343–357.

AML Intelligence. (2024). News: Irish Authorities Detain Suspected Leader of Black Axe Gang in Connection with Money Laundering Investigation. Retrieved from https://www.amlintelligence.com/2024/01/irish-authorities-detain-suspected-leader-of-black-axe-gang/#:~:text=Detectives%20from%20Irish%20authorities%20have,"person%20of%20major%20interest"

Aransiola, J. O. and S. O. Asindemade. 2011. "Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria." *Cyberpsychology, Behavior, and Social Networking* 14(12):759–63. doi:10.1089/cyber.2010.0307
Australian Government, Department of Foreign Affairs and Trade (DFAT). (2020). *DFAT Country Information Report: Nigeria*. Retrieved from https://www.dfat.gov.au/sites/default/files/dfat-country-information-report-nigeria-3-december-2020.pdf
BBC (2020). Helen Oyibo. *Nigeria's Campus Cults: Buccaneers, Black Axe, and Other Feared Groups*. Retrieved from https://www.bbc.co.uk/news/world-africa-52488922
BBC (2021a). Black Axe: Leaked Documents Shine Spotlight on Secretive Nigerian Gang. Retrieved from https://www.bbc.co.uk/news/world-africa-59630424
BBC (2021b).Hushpuppi: The Instagram Influencer and International Fraudster. Retrieved from https://www.youtube.com/watch?v=mXA7rcVBslU
Bloomberg (2021)."The Fall of the Billionaire Gucci Master," Retrieved from https://www.bloomberg.com/features/2021-hushpuppi-gucci-influencer/
Braun, V. and V. Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2):77–101. doi:10.1191/1478088706qp063oa
Broadhurst, R., P. Grabosky, M. Alazab, B. Bouhours, and S. Chon. 2014. "Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime." *International Journal of Cyber Criminology* 8(1):1–20. doi:10.2139/ssrn.2345525
Butler, S. 2022. "The Philosophy of Bitcoin and the Question of Money." *Theory, Culture & Society* 39(5):81–102. doi:10.1177/02632764211049826
Button, M., B. Hock, and D. Shepherd. 2022. *Economic Crime: From Conception to Response*. London: Routledge.
Callon, M. 1986. "The Sociology of an Actor-Network: The Case of the Electric Vehicle." Pp. 19–34 in *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*, edited by M. Callon, J. Law, and A. Rip. London: Palgrave Macmillan UK.
Campana, P. 2016. "Explaining Criminal Networks: Strategies and Potential Pitfalls." *Methodological Innovations*. 9:1–10. doi:10.1177/2059799115622748
Campana, P. and F. Varese. 2012. "Listening to the Wire: Criteria and Techniques for the Quantitative Analysis of Phone Intercepts." *Trends in Organized Crime* 15(1):13–30. doi:10.1007/s12117-011-9131-3
Carter, E. 2021. "Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud." *The British Journal of Criminology* 61(2):283–302. doi:10.1093/bjc/azaa072
CBC News (2015). Romance Scam Victim 'Bled dry' As Con Artists Steal $1.3M, Retrieved from https://www.cbc.ca/news/canada/toronto/romance-scam-fbi-1.3284484
Cohen, C. 2023. "The "Nigerian mafia" Feedback Loop: European Police, Global Media and Nigerian Civil Society." *Trends Organised Crime* 26(4):340–57. doi:10.1007/s12117-022-09471-0
Cretu-Adatte, C., J. W. Azi, O. Beaudet-Labrecque, H. Bunning, L. Brunoni, and R. Zbinden. 2024. "Unravelling the Organisation of Ivorian Cyberfraudsters: Criminal Networks or Organised Crime?" *Journal of Economic Criminology* 3:100056–59. doi:10.1016/j.jeconc.2024.100056
Cross, C. and R. Gillett. 2020. "Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud." *Journal of Financial Crime* 27(3):871–84. doi:10.1108/JFC-02-2020-0026
CrowdStrike (2018). Intelligence Report: CSIR – 18004 Nigerian Confraternities Emerge As Business Email Compromise Threat, Retrieved from https://www.crowdstrike.com/wpcontent/uploads/2020/03/NigerianReport.pdf
Cyware (2019). Cybercriminals Leverage Google Translate to Hide Their Phishing Sites. Retrieved from https://cyware.com/news/cybercriminals-leverage-google-translate-to-hide-their-phishing-sites-644caf13
Décary-Hétu, D. and B. Dupont. 2012. "The Social Network of Hackers." *Global Crime* 13(3):160–75. doi:10.1080/17440572.2012.702523
Ellis, S. 2016. *This Present Darkness: A History of Nigerian Organized Crime*. Oxford: Oxford University Press.
Federal Bureau of Investigation, FBI, (2018). "Business Email Compromise Contributes to Large Scale Business Losses Nationwide," Retrieved March 1, 2022, from https://www.ic3.gov/Media/Y2018/PSA180611
Foley, S., J. R. Karlsen, and T. J. Putniņš. 2019. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" *The Review of Financial Studies* 32(5):1798–853. doi:10.1093/rfs/hhz015
Grabosky, P. N. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10(2):243–49. doi:10.1177/a017405
Granovetter, M. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78(6):1360–80. doi:10.1086/225469
Granovetter, M. 1983. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* 1:201–33. doi:10.2307/202051
Hall, T., B. Sanders, M. Bah, O. King, and E. Wigley. 2021. "Economic Geographies of the Illegal: The Multiscalar Production of Cybercrime." *Trends in Organized Crime* 24(2):282–307. doi:10.1007/s12117-020-09392-w
Hall, T. and V. Scalia. 2019. "Thinking Through Global Crime and Its Agendas." in Pp. 1–10 in *A Research Agenda for Global Crime*, edited by T. Hall and V. Scalia. Northampton: Edward Elgar Publishing
Hall, T. and R, Yarwood. 2024. New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*. doi: 10.1177/03091325241246015.

Ibrahim, S. 2016. "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals." *International Journal of Law, Crime and Justice*. 47:44–57. doi:10.1016/j.ijlcj.2016.07.002
Ibrahim, S. (2017). Causes of Socioeconomic Cybercrime in Nigeria. Paper presented at IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, pp. 1–9. 10.1109/ICCCF.2016.7740439
Ibrahim, S. (2018). "The View That '419' Makes Nigeria a Global Cybercrime Player Is Misplaced." *The Conversation*, Retrieved from https://theconversation.com/the-view-that-419-makes-nigeria-a-global-cybercrime-player-is-misplaced-73791
Immigration and Refugee Board of Canada (2023). *Black Axe*. Retrieved from https://irb.gc.ca/en/country-information/rir/Pages/index.aspx?doc=458713&pls=1
Latour, B. (1997). On Actor-Network Theory. *A Few Clarifications Plus More Than a Few Complications*. Retrieved November 10, 2018, from http://www.bruno-latour.fr/sites/default/files/P-67,20
Latour, B. 2017. "On Actor-Network Theory. A Few Clarifications, Plus More Than a Few Complications." *Philosophical Literary Journal Logos* 27(1):173–97. doi:10.22394/0869-5377-2017-1-173-197
Lavorgna, A. 2019. *Cybercrimes: Critical Issues in a Global Context*. London: Palgrave Macmillan.
Lavorgna, A. 2020. "Organized Crime and Cybercrime." in Pp. 117–34 in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by T. Holt and A. Bossler. Cham: Palgrave Macmillan
Lavorgna, A. and A. Sergi. 2014. "Types of Organised Crime in Italy. The Multifaceted Spectrum of Italian Criminal Associations and Their Different Attitudes in the Financial Crisis and in the Use of Internet Technologies." *International Journal of Law, Crime and Justice* 42(1):16–32. doi:10.1016/j.ijlcj.2013.11.002
Lavorgna, A. and A. Sergi. 2016. "Serious, Therefore Organised? A Critique of the Emerging "Cyber-Organised crime" Rhetoric in the United Kingdom." *International Journal of Cyber Criminology* 10(2):170–87.
Lazarus, S. 2018. "Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists." *Criminology, Criminal Justice, Law & Society* 19(2):63–80.
Lazarus, S. 2019. "Where Is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth." *Religions* 10(3):146. doi:10.3390/rel10030146
Lazarus, S. (2020). Establishing the Particularities of Cybercrime in Nigeria: Theoretical and Qualitative Treatments (Doctoral dissertation, University of Portsmouth).
Lazarus, S. 2021. "Demonstrating the Therapeutic Values of Poetry in Doctoral Research: Autoethnographic Steps from the Enchanted Forest to a PhD by Publication Path." *Methodological Innovations* 14(2):1–11. doi:10.1177/20597991211022014
Lazarus, S. 2022. "Just Married: The Synergy Between Feminist Criminology and the Tripartite Cybercrime Framework." *International Social Science Journal* 69(231):15–33. doi:10.1111/issj.12201
Lazarus, S. (2023). Social Media Users Compare Internet Fraudsters to Nigerian Politicians. Africa at LSE. Retrieved from https://blogs.lse.ac.uk/africaatlse/2023/02/02/social-media-users-compare-internet-fraudsters-to-nigerian-politicians/?_gl=1*1ysrg8j*_ga*MTc4NDYzMDk2My4xNjk4MTUwNzQw*_ga_LWTEVFESYX*MTcxMDc3MjkwOC4yNTIuMC4xNzEwNzcyOTEwLjU4LjAuMA
Lazarus, S. and M. Button. 2022. "Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide." *Cyberpsychology, Behavior, and Social Networking* 25(8):504–11. doi:10.1089/cyber.2021.0332
Lazarus, S., M. Button, and A. Adogame. 2022. "Advantageous Comparison: Using Twitter Responses to Understand Similarities Between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men")." *Heliyon* 8(11):e11142. doi:10.1016/j.heliyon.2022.e11142
Lazarus, S. and G. U. Okolorie. 2019. "The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents." *Telematics and Informatics*. 40:14–26. doi:10.1016/j.tele.2019.04.009
Lazarus, S., O. Olaigbe, A. Adeduntan, E. T. Dibiana, and G. U. Okolorie. 2023a. "Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps." *Journal of Economic Criminology* 2(100033):1–17. doi:10.1016/j.jeconc.2023.100033
Lazarus, S., J. M. Whittaker, M. R. McGuire, and L. Platt. 2023b. "What Do We Know About Online Romance Fraud Studies? A Systematic Review of the Empirical Literature (2000 to 2021)." *Journal of Economic Criminology* 2 (100013):100013–17. doi:10.1016/j.jeconc.2023.100013
Leukfeldt, E. R. 2014. "Cybercrime and Social Ties." *Trends in Organized Crime*. 17:231–49. doi:10.1007/s12117-014-9229-5
Leukfeldt, E R, and T J, Holt. 2020. Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *Int J Offender Ther Comp Criminol* 64(5):522–538. doi: 10.1177/0306624X19895886.
Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017a. "Cybercriminal Networks, Social Ties and Online Forums: Social Ties versus Digital Ties within Phishing and Malware Networks." *The British Journal of Criminology* 57(3):704–22. doi:10.1093/bjc/azw009
Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017b. "Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis." *Crime, Law and Social Change* 67(1):39–53. doi:10.1007/s10611-016-9663-1
Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017c. "A Typology of Cybercriminal Networks: From Low-Tech All-Rounders to High-Tech Specialists." *Crime, Law and Social Change* 67(1):21–37. doi:10.1007/s10611-016-9662-2

Levi, M. 2008. "Organized Fraud and Organizing Frauds: Unpacking Research on Networks and Organization." *Criminology & Criminal Justice* 8(4):389–419. doi:10.1177/1748895808096470
Levi, M. 2017. "Organized Fraud and Organizing Frauds: Unpacking Research on Networks and Organization." Pp. 309–40 in *Transnational Financial Crime*, edited by Nikos, P. London: Routledge.
Longgreads. 2023. Inside the World of Nigerian "Yahoo Boys". https://longreads.com/2023/07/11/inside-the-world-of-nigerian-yahoo-boys-atavist-excerpt/
Lusthaus, J., E. Kleemans, R. Leukfeldt, M. Levi, and T. Holt. 2023. "Cybercriminal Networks in the UK and Beyond: Network Structure, Criminal Cooperation and External Interactions." *Trends in Organized Crime*. 1–24. doi:10.1007/s12117-022-09476-9
Marquart, J. W., and R., Alan Thompson. 2024. Exploring relation fraud, murder,and the Fraud Triangle. *Journal of Economic Criminology* 4: 100061. doi: 10.1016/j.jeconc.2024.100061.
Meyers, A. 2018. "Not Your Fairy-Tale Prince: The Nigerian Business Email Compromise Threat." *Computer Fraud & Security* 2018(8):14–16. doi:10.1016/S1361-3723(18)30076-9
Neo Black Movement of Africa (NBM). 2022. *NBM Disassociates Self from July 7 Celebration*. Retrieved https://nbmofafrica.org/nbm-disassociates-self-from-july-7-celebration/
Nguyen, T. and H. T. Luong. 2021. "The Structure of Cybercrime Networks: Transnational Computer Fraud in Vietnam." *Journal of Crime and Justice* 44(4):419–40. doi:10.1080/0735648X.2020.1818605
Ogunleye, Y. O., U. A. Ojedokun, and A. A. Aderinto. 2019. "Pathways and Motivations for Cyber Fraud Involvement Among Female Undergraduates of Selected Universities in South-West Nigeria." *International Journal of Cyber Criminology* 13(2):309–25. doi:10.5281/zenodo.3702333
Okosun, O. and U. Ilo. 2022. "The Evolution of the Nigerian Prince Scam." *Journal of Financial Crime* 30(6):1653–63. doi:10.1108/JFC-08-2022-0185
Okpa, J. T., B. O. Ajah, O. F. Nzeakor, E. Eshiotse, and T. A. Abang. 2022. "Business E-Mail Compromise Scam, Cyber Victimization, and Economic Sustainability of Corporate Organizations in Nigeria." *Security Journal* 36(2):350–72. doi:10.1057/s41284-022-00342-5
The Register (2018). How to Make Your Very Own Google HQ for a Phishing Scam. Retrieved from https://www.theregister.com/2018/05/01/google_maps_url/
Reiner, R. 2010. *The Politics of the Police*. Oxford: Oxford University Press.
Reiner, R. 2016. *Crime, the Mystery of the Common-Sense Concept*. New York: John Wiley and Sons.
Harper's Magazine. (2019). Sean Williams. *The Black Axe: How a Pan-African Freedom Movement Lost Its Way*. Retrieved from https://harpers.org/archive/2019/09/the-black-axe-nigeria-neo-black-movement-africa/
Sergi, A. 2013. "Structure Vs Activity: Two Models to Fight Organised Crime and Their Criticisms." *Policing: A Journal of Policy and Practice*. doi:10.1093/police/pat033
Sergi, A. and L. Storti. 2021. "Shaping Space. A Conceptual Framework on the Connections Between Organised Crime Groups and Territories: An Introduction to the Special Issue on 'Spaces of Organised Crime'." *Trends in Organized Crime* 24(2):137–51. doi:10.1007/s12117-021-09415-0
Shaw, C. R. 2013. *The Jack-Roller: A Delinquent Boy's Own Story Original work published 1930*. Chicago: University of Chicago Press.
Simmel, G. 1964. *Conflict and the Web of Group-Affiliations*. New York: The Free Press.
Surajo, A. Z. and A. H. M. Z. Karim. 2017. "An Assessment of Black Axe Confraternity Cult in Nigeria: Its Impact on the University Educational System." *South Asian Anthropologist* 17(1):1–7.
Thomas, W. I. 1923. *The Unadjusted Girl*. Boston: Little Brown and Company.
Toronto Sun. 2018. Toronto Romance Scam Linked to Global Fraud Case. Retrieved from https://torontosun.com/2015/10/22/toronto-romance-scam-linked-to-global-fraud-case
Trend Micro and INTERPOL. 2017. 'Cybercrime in West Africa: Poised for an Underground Market'. Retrieved from https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf
Tropina, T. 2012. "The Evolving Structure of Online Criminality: How Cybercrime Is Getting Organised." *Eucrim - the European Criminal Law Associations' Forum* 4:158–65. Retrieved from https://www.corteidh.or.cr/tablas/r15111.pdf. doi:10.30709/eucrim-2012-022
United Nations. 2010. TRAFFICKING of NIGERIAN GIRLS in ITALY: The Data, the Stories, the Social Services Retrieved from https://documentation.lastradainternational.org/lsidocs/trafficking%20nigerian%20girls%20in%20italy.pdf
Valimail. 2023. BEC Scams Cost Companies $50 Billion in Losses. https://www.valimail.com/blog/bec-scams-cost-companies-50-billion-in-losses/
Vanguard. 2022. Evelyn Usman. *We Kill Rivals, Cut off Their Hands for Rituals — Self-Confessed Cultist*. Retrieved from https://www.vanguardngr.com/2022/08/we-kill-rivals-cut-off-their-hands-for-rituals-self-confessed-cultist/
Vice. 2015. Tamara Khandaker. *The Notorious Black Axe Has Put Down Roots in Canada*. Retrieved from https://www.vice.com/en/article/vb835b/the-notorious-black-axe-has-put-down-roots-in-canada#
Vicsek, L. M., G. Király, and H. Kónya. 2016. "Networks in the Social Sciences: Comparing Actor-Network Theory and Social Network Analysis." *Corvinus Journal of Sociology and Social Policy* 7(2):77–102. doi:10.14267/CJSSP.2016.02.04

Wall, D. S. 2015. "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime." *The European Review of Organised Crime* 2(2):1–20. doi:10.2139/ssrn.2677113

Wall, D. S. 2021. "Cybercrime As a Transnational Organized Criminal Activity." in Pp. 318–36 in *Routledge Handbook of Transnational Organized Crime*, edited by F Allum and S. Gilmour. London: Routledge

Wang, P., Su, M, and Wang, J. 2021. Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. *The British Journal of Criminology* 61(2): 303–324. doi: 10.1093/bjc/azaa064.

Wang, F. and V. Topalli. 2024. "The Cyber-Industrialization of Catfishing and Romance Fraud." *Computers in Human Behavior* 154:108133. doi:10.1016/j.chb.2023.108133

Whittaker, J. M., S. Lazarus, and T. Corcoran. 2024. "Are Fraud Victims Nothing More Than Animals? Critiquing the Propagation of "Pig butchering" (Sha Zhu Pan, 杀猪盘)." *Journal of Economic Criminology* 3(100052):100052–58. doi:10.1016/j.jeconc.2024.100052

Yar, M. and K. F. Steinmetz. 2019. *Cybercrime and Society*. London: SAGE Publications Limited.

Zakari, M. B. and M. Button. 2022. "Confronting the Monolith: Insider Accounts of the Nature and Techniques of Corruption in Nigeria." *Journal of White Collar and Corporate Crime* 3(2):100–08. doi:10.1177/2631309X211004567

Zeng, Y. and D. Buil-Gil. 2023. "Organizational and Organized Cybercrime." *Criminology & Criminal Justice*. doi:10.1093/acrefore/9780190264079.013.798