Pathways, Pressure, and Profit: Adaptive Innovation and Strain in a Convicted Cybercrime Academy Called Hustle Kingdom

Cite as:

- Lazarus, S., Soares, A. B., & Button, M. (2025). Pathways, Pressure, and Profit: Adaptive Innovation and Strain in a Convicted Cybercrime Academy Called Hustle Kingdom. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2025.2551790

Abstract

This research offers the first empirical examination of the "Hustle Kingdom (HK)" phenomenon. Hustle Kingdoms are underground cybercrime training centers in West Africa that recruit and train young men to become digital fraudsters. The empirical foundation of this study draws on case files from the Economic and Financial Crimes Commission (EFCC) concerning the prosecution and eventual conviction of the proprietor and students of a Hustle Kingdom. Ethnographic field notes and informal conversations with relevant authorities supplement this dataset. It examines the significance of Merton's Strain Theory, focusing on the innovation mode of adaptation, to understand how economic pressures and socio-fabric elements of society drive individuals toward illicit entrepreneurship. Our findings reveal key characteristics of these academies, including their structure, recruitment and governance strategies, motivations, indirect enablers, and prosecutorial challenges. While this pioneering investigation positions Hustle Kingdoms as an alternative route to economic mobility for many youths, it situates Hustle Kingdoms within broader processes of deviant innovation and informal economic adaptation. The study concludes by reflecting on the broader ecosystem of subtle enablers.

Introduction

Nigeria's global reputation in cybercrime

When formal pathways to success are blocked, deviance becomes not simply a violation of norms, but a calculated pursuit of survival, opportunity, and status (Merton 1938). This broader logic is particularly salient in settings where structural conditions fuel the growth of online deviance in West Africa (Abubakari and Blaszczyk 2023; Button et al. 2024; Hall et al. 2021). Numerous studies, including a qualitative investigation commissioned by the UK Home Office (Button et al. 2024) and the World Cybercrime Index (Bruce et al. 2024), have consistently ranked Nigeria among the highest-risk jurisdictions for cybercrime involving fraud. This reputation is rooted in the globally oriented activities of cybercriminal groups popularly referred to as "Yahoo Boys" (Adeniran 2008; Lazarus and Okolorie 2019; Lazarus et al. 2023; Soares and Lazarus 2024). Yahoo Boys' fraud schemes are embedded within illicit economies that convert digital deception into material capital (Garba et al. 2024; Uroko and Obiorah 2025). Despite this widespread recognition, little is known about the underground institutions that incubate and train these offenders, namely, the scamming schools known as “Hustle Kingdoms.[1]”

Precisely, Hustle Kingdoms have not been empirically examined in academic scholarship before; this article provides the first data-driven study of its structure, recruitment, and operations. The term “Hustle Kingdoms” is a sociological concept developed to describe semi-institutionalized cybercrime “academies” operating in West Africa, particularly Nigeria and Ghana (Lazarus and Soares 2025). These formations are not ad hoc scam groups but structured environments where digital fraud is taught through routinized schedules, ritual obligations, and hierarchies. Thus, Hustle Kingdoms function as informal schools of deviance, serving as spaces of criminal apprenticeship (Lazarus and Soares 2025). While Hustle Kingdoms have produced thousands of cybercriminals across the region, scholars indicated that internet fraudsters themselves are implicated in the neologism, having introduced the term “Hustle Kingdoms” to describe their own illicit schools (Lazarus and Soares 2025).

The rise and role of Hustle Kingdoms

This article examines convicted cases involving Hustle Kingdoms (HKs), cybercrime apprenticeship schools, also known as scamming schools, operating in Africa south of the Sahara. Our analysis focuses particularly on Nigeria. Hustle Kingdoms function as sites of deviant socialisation and organised learning (Lazarus and Soares 2025). Hustle Kingdoms is a newly coined sociological term that refers to semi-structured underground cybercrime academies functioning as alternative institutions of deviant learning (Lazarus and Soares 2025). Although embedded within illicit economic systems, these entities replicate features of formal education, including hierarchies, mentorship, and structured curricula.

Empirical contribution and research gaps

This study pioneers the first empirical investigation of Hustle Kingdoms. It does so by applying institutional and educational analogies to cybercrime research, a topic that has, at best, received minimal attention in academic literature. Until now, Hustle Kingdoms have been mentioned only in media reports (PM News 2024), blog commentaries (Lazarus and Button 2024), and a single conceptual paper (Lazarus and Soares 2025). We acknowledge the limited academic literature on Hustle Kingdoms. Owing to the almost non-existent body of scholarship on Hustle Kingdoms, our analysis relies on the few available sources that discuss them directly or indirectly. Drawing on a unique dataset of convicted case files, supplemented with ethnographic fieldnotes and expert interviews, this article offers a grounded and sociological analysis of how cybercriminal labor is shared, socialized, and legitimized in these deviant educational settings. Legitimisation occurs through both family and community endorsement. Parents and significant others often help secure enrolment, sustain participation, and even provide legal or financial support when prosecutions occur (Button et al. 2024; Lazarus and Soares 2025).

[1] Throughout this article, the term “Hustle Kingdom” (singular) refers specifically to one cybercrime apprenticeship academy documented in the EFCC conviction dataset used in this study. This site serves as the primary empirical locus for analyzing cybercrime training environments in Nigeria. In contrast, “Hustle Kingdoms” (plural) is used as an analytic category to describe a broader sociological phenomenon: cybercrime academies across Nigeria and similar contexts that combine hierarchical mentorship, spiritual discipline, and economic extraction. This pluralized form allows for generalization beyond the focal case while maintaining attention to its structural logics. Thus, singular usage denotes a particular ethnographic case; plural usage signals a conceptual typology of networked formations that share core features. The dual usage reflects both empirical specificity and theoretical generalization, aligned with sociological traditions that move between case and category.

Historically, Hustle Kingdoms were valued for their low barriers to entry, offering accessible alternatives to costly formal education (Lazarus and Soares 2025). Because these cybercrime academies typically require no upfront fees, they are particularly attractive to young people excluded from formal schooling due to financial constraints. In other words, Hustle Kingdoms reconfigure blocked pathways to education and employment into structured systems of deviant apprenticeship. Their social legitimacy is rooted not only in the criminal opportunities they provide for struggling youths but also in the support of parents, peers, and wider community networks (Button et al. 2024; Lazarus and Soares 2025). Within this context, many Nigerians struggle to distinguish between the fraudulent practices of internet scammers[2] (Yahoo Boys) and those of political elites (Lazarus, Button, and Adogame 2022), as well as religious leaders (Lazarus, Tickner, and Button 2025), who are widely referred to as "Yahoo Men." In this way, Hustle Kingdoms gain social legitimacy not only as sites of training and socialisation but also as socially sanctioned pathways to economic survival in contexts where formal education is financially prohibitive.

Structural strain and the political economy of digital fraud

Situated within a broader socio-economic crisis (Abubakari and Blaszczyk 2023; Ajayi, Adesope and Oso 2024; Hall et al. 2021; Lazarus and Okolorie 2019; Yushawu and Jaishankar 2025), it is reasonable to argue that Hustle Kingdoms have emerged in response to persistent poverty, high youth unemployment, entrenched political corruption, and the near-total absence of state-sponsored social welfare systems (Lazarus and Soares 2025). In this context, these academies offer not only training in digital fraud but also a perceived pathway to financial survival and upward mobility for many young Nigerians. While Nigerian online fraudsters in Lagos, British cyberbullies in Manchester, Armenian ransomware operators in Yerevan, Russian hackers in Saint Petersburg, and "Jamaican lottery scammers" in Kingston may use similar digital infrastructures, the underlying motivations and social meanings attached to their activities differ markedly (cf. Lazarus, Button and Adogame 2022:1). These differences are shaped by the cultural, economic, and political ecologies within which both the technologies and their users are embedded (according to numerous studies, e.g., Aborisade 2022; Abubakari and Blaszczyk 2023; Hall and Yarwood 2024; Hall and Ziemer 2024; Hall et al. 2021; Lazarus et al. 2025; Whittaker et al. 2025).

In Nigeria, many internet fraudsters' careers have emerged as adaptive strategies for economic survival. These individuals innovatively navigate their socio-economic landscapes through digital deviance (cf. Merton 1938), engaging in various forms of fraud, including advance-fee scams, cryptocurrency scams, romance fraud, and business e-mail compromise (BEC) schemes (Garba et al. 2024). Such activities represent a form of cultural innovation where actors reproduce and reimagine economic practices in a digital context (Button et al. 2024; Lazarus 2018; Lazarus and Okolorie 2019). Their actions carry transnational intentions and consequences, predominantly targeting victims in the Global North (Hall and Yarwood 2024; Hall et al. 2021; Lazarus et al. 2025; Lazarus, Chiang and Button 2025; Yushawu and Jaishankar 2025), creating new globalized networks of exchange that blur the boundaries between legality and deviance.

[2] This article employs "scammers"/"fraudsters" and "scam"/"fraud" interchangeably, recognizing that these labels are socially constructed and legitimized within different institutional arenas. "Scam" circulates widely in media, finance, and everyday discourse, evident in the naming practices of organizations such as the Global Anti-Scam Alliance, Scamwatch, Scam Survivors, and Scam Baiters. However, academic and legal contexts tend to privilege "fraud" to underline its juridical and financial connotations (see also Lazarus et al., 2025).

As global digital networks proliferate, localized criminal practices increasingly exert transnational impacts, challenging the boundaries of traditional criminological inquiry (Cross 2020; Franceschini et al. 2025; Hall and Yarwood 2024; Hall et al. 2021; Lazarus 2024; Lusthaus et al. 2023). Studies focusing on Nigerian cybercriminals reveal the global implications of their actions, with data from 40 officers of the Economic and Financial Crimes Commission (EFCC) (Lazarus and Okolorie 2019) and research involving 40 cybercriminals (Aransiola and Asindemade 2011) highlighting these far-reaching impacts. Such findings underscore the importance of studying illicit institutions, or "Hustle Kingdoms," which sustain and reproduce cybercriminal networks. The phenomenon calls for methodologies that capture the socio-political, economic, and technological complexities of both the social actors and their activities.

From business centres to the "Hustle Kingdom" (HK) phenomenon

The contemporary Hustle Kingdoms in Nigeria did not emerge in a vacuum. Rather, they are part of a longer trajectory of deviant apprenticeship traced back to the "business centres" of the 1980s and 1990s (Lazarus and Soares 2025:5). The term "Hustle Kingdoms" originates from the vernacular of scammers and refers to cybercrime training centers that serve as spaces of deviant apprenticeship (Lazarus and Soares 2025). These centers, also referred to as "Hustle academies," provide instruction in digital fraud, targeting individuals disenfranchised by socio-economic constraints and equipping them with the skills and strategies to engage in various forms of cybercrime (Lazarus and Soares 2025; Lazarus and Button 2024).

While ostensibly legitimate, these "business centers," the past that created Hustle Kingdoms, operated at the intersection of legality and informality (Lazarus and Soares 2025). At a time when few Nigerians had private access to telecommunications infrastructure, business centers provided essential services such as photocopying, faxing, and international phone calls. However, these services coexisted with illicit scamming activities. Business centers were open to the public and functioned as walk-in facilities. One could photocopy documents, send a fax, or make international calls without raising suspicion.

In contrast, Hustle Kingdoms are enclosed, highly restricted spaces that operate beyond the public gaze. They no longer function as hybrid public-private service points. Instead, they serve as closed cybercrime academies where criminal skill sets are cultivated, refined, and disseminated through structured hierarchies (Lazarus and Soares 2025). This transformation reflects more than a technological shift. It marks a fundamental reorganization of space, visibility, and institutional form. Importantly, this continuity challenges binary framings of criminal innovation as either spontaneous or disorganized. Instead, it reveals a grounded lineage of locally embedded socio-technical practices (Lazarus and Soares 2025).

Real-life scams linked to "graduates" of these academies fuel widespread fraud globally (Lazarus and Soares 2025), with senior citizens among the most vulnerable targets (Cross and Holt 2025; Lazarus, Tickner and McGuire 2025; Parti, Tahir and Teaster 2025; Uroko and Obiorah 2025). Hustle Kingdoms, prevalent in West Africa (e.g., Nigeria and Ghana), mimic the structure of formal educational settings but redirect the purpose toward illicit activities (Lazarus and Soares 2025). The Hustle Kingdom exemplifies a deviant adaptation of conventional educational models. While traditional schools pursue societal goals of knowledge dissemination and skill acquisition (cf. Merton 1938), Hustle Kingdoms re-channel these innovations toward illicit economic gains. "The delinquent may not stand as an alien in the body of society but may represent a disturbing reflection or a caricature instead"

(Matza and Sykes 1961:717). This provocation invites us to reconsider deviance not as external to society but as embedded within its structures. This study takes up that invitation by examining the case of a convicted Hustle Kingdom that mirrors legitimate institutions. Rather than anomalies, such spaces reflect broader social strains and adaptive innovations, offering a window into the institutionalization of deviant opportunity in contexts of persistent inequality and state neglect. These academies combine virtual learning with face-to-face instruction, effectively functioning as incubators for digital deviance, and graduates engage in a range of cybercrimes, such as romance fraud and BEC scams (Lazarus and Soares 2025; Lazarus and Button 2024).

By 2023, the global impact of these academies was evident, with the U.S. reporting nearly $50 billion in losses due to online scams, much of it traced to West African fraudsters (Valimail 2023). If accurate, this statistic indicates that such deviant entities, despite their illicit orientation, may mimic legitimate institutions in both structure and purpose. Nonetheless, as Merton (1938) theorized, individuals may innovate by pursuing alternative, often deviant, paths when access to legitimate success is blocked. Hustle Kingdoms embody this adaptive deviance, creating parallel institutions that circumvent traditional education and employment barriers while mirroring legitimate outcomes. West Africa, particularly Nigeria and Ghana, has seen a surge in these academies, which teach cyber deception as a viable career alternative (Lazarus and Soares 2025; Lazarus and Button 2024). By adapting educational frameworks to serve deviant goals, Hustle Kingdoms illustrate a subcultural innovation that navigates the scarcity of legitimate opportunities, as illustrated in Table 1.

Table 1. Merton's five modes of adaptation summary

Mode of Adaptation	Description	Example
Conformity	Aligns with societal norms, pursuing accepted goals through legitimate means.	An office worker aiming for career advancement by following company policies.
Innovation	Embraces cultural goals but rejects lawful means, often leading to deviant behaviour.	A young entrepreneur engaging in online fraud to achieve financial success.
Ritualism	Rejects societal goals but adheres to prescribed methods.	A bureaucrat who follows rules without personal ambition for success.
Retreatism	Withdraws from societal aspirations and legitimate means.	A person experiencing homelessness and addiction, opting out of societal goals.
Rebellion	Rejects both cultural goals and means, seeking to replace them with new values.	An activist advocating for a new societal structure through radical movements.

Source: Adapted from Merton (1938), Social Structure and Anomie. Examples are original.

The case of the proprietor and his "Hustle Kingdom"

A prominent example is Mr Michael Akpan[3]'s (pseudonym used) "Hustle Kingdom," which operated in Akwa Ibom State, Nigeria. The case of this proprietor and his "Hustle Kingdom" students is the only known cybercrime academy in Nigeria to have led to a conviction. This evidentiary gap highlights the near-total absence of scholarly research on such organisations, forcing most existing analyses to rely heavily on gray literature. Mr Akpan's establishment mirrored a conventional school in structure but was dedicated to cybercrime. He trained young men in hacking, identity theft, and advance fee fraud, specifically romance scams, equipping them to deceive victims (EFCC 2024; PM News 2024). Merton's (1938) Strain Theory offers insight into how individuals like Mr Akpan, faced with limited legitimate paths, innovate to create alternative, deviant careers. Mr Akpan's Hustle Kingdom reflects the ambition and structure of traditional institutions, yet redefines success through illicit means.

Theoretical insights: strain theory

Deviant behavior often emerges not as random defiance but as a structured response to the disjunction between culturally prescribed goals and the limited legitimate means available to attain them (Merton 1938). Merton's Strain Theory provides a critical lens through which to examine the Hustle Kingdom phenomenon. The core argument of Strain Theory is that deviance emerges when there is a gap between societal goals and the legitimate means available to achieve them (Merton 1938). The five modes of adaptation outlined in Table 1 are pivotal to Strain Theory, as they represent various ways individuals respond to the tension between cultural aspirations and institutionalized pathways. Merton (1938) uses this framework to explore how socioeconomic pressures can drive individuals toward deviant behaviors, and we specifically focus on the innovation mode of adaptation. This mode is particularly relevant in examining the Hustle Kingdom phenomenon and internet scammers in general, where individuals bypass legitimate means in favor of alternative, often illicit, strategies for economic success. The focus here on innovation aligns with the conditions within the Hustle Kingdom and provides a lens through which to interpret the motivations and choices of its participants.

In Nigeria, access to higher education is primarily restricted to the elite or those with substantial financial backing. "Formal education in countries like Nigeria and Ghana has historically imposed significant financial burdens on families. The high cost of tuition across all levels – nursery, primary, secondary and tertiary – has excluded large proportions of the population" (Lazarus and Soares 2025:8). As a result, many young people are excluded from legitimate pathways to socio-economic mobility, such as stable employment, vocational advancement, or entrepreneurial opportunities. This exclusion fosters a structural strain, where aspirations for financial stability clash with limited legitimate means. This disparity creates fertile ground for the emergence of illicit entities like Hustle Kingdoms. Hustle Kingdoms position themselves as alternative routes to mobility by offering training in activities such as hacking, sextortion, romance fraud, and Business Email Compromise (BEC) schemes (Lazarus and Soares 2025). In this context, Mr Akpan's cybercrime academy becomes a conduit for achieving financial success that may seem otherwise unattainable through conventional avenues.

[3] While this case is documented in Nigerian media and EFCC press releases, this study incorporates additional unpublished material (court files, interviews). In accordance with COPE guidance and criminological ethics, a pseudonym is used to minimise harm and reduce the risk of re-identification through new contextual detail.

Strain theory and cybercrime research

Although early cybercrime research was dominated by frameworks such as Gottfredson and Hirschi's (1990) General Theory of Crime (e.g., Donner 2016), recent scholarship has increasingly applied strain perspectives to explain online offending. Agnew's General Strain Theory (GST) (2013) posits that strainful events and social relationships generate negative emotional states, particularly anger and frustration, which may be resolved through deviant coping mechanisms. Hay and Ray (2019) argue that GST is especially useful in cybercrime contexts because it incorporates social-psychological processes often overlooked by other models, such as the role of perceived injustice and the translation of emotional strain into online aggression or fraud.

Empirical research has supported the link between GST and cybercrime in diverse contexts. Parti and Dearden (2024), using a nationally representative U.S. sample, found that strain variables predicted both general and specific forms of cyber-offending, with notable gender differences: women's offending was linked to anonymity and online gaming, while men's offending was tied to victimization experiences and dark web activity. Wilson and Seigfried-Spellar (2022) reported that financial and social strains, alongside victimization in online spaces, were significant predictors of trolling behavior, reinforcing the salience of both economic and interpersonal strains in digital aggression.

Strain perspectives have also been extended to technocrime and politically motivated hacking. Chism and Steinmetz (2017) emphasize the importance of qualitative studies in exploring the lived experiences of strain in online environments, including indirect or vicarious strains, such as witnessing inequitable treatment. Unlike the other studies mentioned above, Chism and Steinmetz (2017) examined both Merton's Anomie Strain Theory and Agnew's General Strain Theory. However, these studies (e.g., Chism and Steinmetz 2017; Parti and Dearden 2024) affirm the relevance of GST in explaining cyber-offending. They also highlight that strains may be context-specific, intersecting with factors such as gender, socioeconomic position, and subcultural norms. However, little research has explored strain in Africa south of the Sahara, especially within cybercrime training contexts such as the Hustle Kingdom. In these settings, structural unemployment and blocked mobility can act as powerful drivers of deviant innovation.

While Agnew's General Strain Theory (GST) (2013) offers valuable insights into the sociocultural and psychological dimensions of strain, the decision to frame this study using Merton's strain theory (1938) is deliberate. As evidenced in Table 2, the Hustle Kingdom analysis focuses on structural and opportunity-based constraints, particularly the disjunction between culturally prescribed success goals and limited legitimate means. These conditions align more directly with Merton's macro-sociological emphasis. GST's broader emotional-psychological mechanisms, while relevant, would expand the theoretical scope beyond the paper's primary aim: situating Hustle Kingdoms within systemic socio-economic pressures rather than individual emotional responses. This targeted framing ensures conceptual coherence and sharper alignment with the study's research questions. In this context, Mr Akpan's cybercrime academy acts as a bridge to attaining financial success that might otherwise be out of reach through traditional means.

Table 2. Thematic contributions of Hustle Kingdom conviction data

Theme	Dominant View in Literature	Findings from Hustle Kingdom Cases	Key References	Clarification of Citation Input
Network Structure	Cybercrime networks are decentralised, fluid, and leaderless.	Hustle Kingdoms display a rigid hierarchy, with a 'chair' overseeing logistics and profit-sharing.	Nguyen and Luong (2021); Décary-Hétu and Dupont (2012); Lazarus (2024)	Discuss other cybercriminal networks; applied here by comparison. Only Lazarus and Soares (2025) directly analyzed Hustle Kingdoms.
Organisation Type	Typically informal, temporary associations.	Resembles a deviant learning institution with formal roles and mentoring structures.	Garba et al. (2024); Lazarus and Soares (2025)	Garba et al. (2024) explored cryptocurrency fraudsters in West Africa; applied here comparatively.
Educational Role	Cybercrime erodes academic engagement; seen as a distraction from schooling.	Hustle Kingdoms function as alternative schools, with structure, discipline, and skill development.	Ojedokun and Eraye (2012); Lazarus and Soares (2025)	Ojedokun and Eraye (2012) on online fraudsters who are students in a conventional university setting. However, Hustle Kingdoms treated as a deviant academy by Lazarus and Soares (2025).
Group Cohesion	Loosely connected individuals engaging intermittently.	High internal cohesion, frequent contact, and shared commitment to the 'hustle' as a deviant enterprise.	Décary-Hétu and Dupont (2012); Lazarus (2025); Leukfeldt and Holt (2019)	Studies on cybercrime networks; applied comparatively.
Spatial Mobility	Limited attention to relocation; operations are often static or assumed digital.	Hustle academies are physically mobile and spatially adaptable, enhancing resistance to law enforcement detection.	Leukfeldt et al. (2017a); Lazarus (2024)	Relocation and evasion studies used here by analogy; Hustle Kingdoms' mobility is unique.
Cultural Framing	Fraud as criminal entrepreneurship, often mimicking corporate rationality.	Fraud is framed as a survivalist pedagogy within contexts of exclusion and marginalisation.	Martin et al. (2024); Paternoster et al. (2025); Lazarus and Soares (2025)	All works on deviant entrepreneurship; Hustle Kingdoms uniquely frames fraud as survival pedagogy discussed by Lazarus and Soares (2025).

Strain Theory suggests that when access to socially sanctioned means of success is blocked, individuals may resort to deviance as an alternative (Merton 1938). In the socio-economic situation of Nigeria, where restricted educational access and a stagnant economy prevail, these pressures intensify. Cybercrime thus becomes not only a viable option but, for some, a necessary one. The lack of higher education among Hustle Kingdom participants exemplifies how socio-economic strain can propel marginalized individuals toward cybercrime as a pathway to survival and upward mobility (e.g., Lazarus and Soares 2025). Therefore, Strain Theory provides a valuable framework for understanding how systemic inequalities fuel environments like Hustle Kingdoms. Exploring the conditions that foster these deviant pathways provides a nuanced understanding of Hustle Kingdoms' role as a consequence, symptom and catalyst of socio-economic strain.

Originality and contribution to prior research

The empirical foundation of this study draws on case files concerning the prosecution and conviction of the proprietor and students of a Hustle Kingdom. Table 2 summarizes the key contributions of this study by juxtaposing our findings against dominant themes in the literature. These core contributions outlined in Table 2 extend the boundaries of cybercrime scholarship in African nations and worldwide. In particular, it offers new empirical grounding for theorising criminal innovation under structural constraint.

Methods and materials

This study employed a documentary analysis of case files, supplemented by informal conversations with law enforcement officers and ethnographic observations in court. The primary focus was the convicted case of Mr Akpan, the operator of the cybercrime academy known as the Hustle Kingdom (HK). No other known case has attained comparable legal closure or evidentiary richness. Its uniqueness, together with access to full court records and insider testimony, makes it an analytically valuable site for advancing theoretical and policy insights into offender demographics and recruitment in digital fraud economies.

Case files

Data was obtained from a Zonal Command of the Economic and Financial Crimes Commission (EFCC) in Nigeria[4]. Twelve individuals (n = 12) associated with HK were arrested between 2023 and 2024. Of these, six were convicted and six were released due to factors such as insufficient evidence, prosecutorial discretion, age, limited involvement, and absence of material benefit. Material benefit refers to tangible gains from scam activities (e.g., cash proceeds, assets, or other economic advantage). All 12 case files were analyzed, including demographic details (e.g., age, educational background), offense-related factors, and other relevant information. These cases were selected because, to date, they represent the only concluded HK-related prosecutions in Nigeria.

Pioneering analysis of Hustle Kingdom cases

This study combines classic documentary analysis (Platt 1981; Scott 2014) with field observations and practitioner insights. While informed by case file research in South Korea (Hock et al. 2025), Western Europe (Lusthaus et al. 2023), and West Africa (Soares et al. 2025), it is the first to apply this approach to convicted Hustle Kingdom cases, both in Nigeria and globally, and the first to empirically examine the Mertonian “innovation” mode of adaptation within cybercrime academies.

Documentary analysis process

Document analysis followed Scott’s (2014) and Platt’s (1981) frameworks, involving four steps:

- **Authenticity**: confirming each document originated from legitimate EFCC legal proceedings.

[4] The study’s focus is rooted in Nigeria. Regional references are used analytically, not as empirical generalisations. Findings are situated within a broader West African context to highlight cross-border spillover and strategic relocation. Prior research has documented Nigerian cybercriminals’ migration to Ghana, driven by uneven enforcement and legal surveillance (Lazarus, et al., 2025).

- **Credibility**: cross-checking the accuracy of statements against other sources, including investigative records and court documents.
- **Representativeness**: ensuring the documents reflected the full scope of HK-related prosecutions rather than isolated cases.
- **Meaning**: interpreting documents within the broader socio-political and economic context of cybercrime in Nigeria.

Analytical steps included:

- Initial reading of all files to familiarize with the content.
- Manual coding of recurrent themes (e.g., operational roles, legal strategies).
- Cross-case comparison to identify consistencies and divergences between the 12 cases.
- Thematic extraction aligned with the study's research questions, shedding light on an empirically underexplored phenomenon in academia.

While the dataset also contained accounts of coercion (e.g., restrictions on movement and communication control), we do not examine those themes here, as they align more closely with frameworks of coercive dependency and trafficking-type exploitation[5].

Informal conversations with law enforcement officers

Three law enforcement officers participated: two investigators and one prosecutor, all of whom were directly involved in HK investigations and prosecutions. These conversations occurred informally, during breaks and other free moments, as the officers were colleagues of the law enforcement members of the research team. Notes and diary entries were kept during and immediately after these exchanges. Conversations were manually coded and thematically analyzed to identify clarifications, insights, and contextual details absent from case files. The findings were integrated with the documentary analysis and ethnographic observations through triangulation, enabling richer interpretation and cross-verification of data.

Ethnographic court observations

One researcher, also a member of the EFCC, conducted participant observation of numerous court proceedings related to all 12 HK defendants. Although the observations were unstructured (as they were not formal interviews), detailed ethnographic diary entries captured the courtroom dynamics, interactions between legal teams, defendants' demeanor, and procedural elements. These notes were later reviewed to identify patterns and institutional narratives relevant to HK operations. Ethnographic methods were informed by established court observation practices (e.g., Callaghan 2005; Mulcahy 2010). Observations were used for triangulation and to add socio-cultural context to the case file and conversation data.

Ethics and approval

A law enforcement team member (A.B.S.) had detailed knowledge of the cases and obtained the official agency approval number CB:4000/EFCC/UYO/LEGAL/VOL.1/45 for the use of

[5] Following recommendations received during the peer-review process, these findings on coercion and exploitation are analyzed in a separate paper, allowing this article to maintain a more precise and coherent storyline (Lazarus, Soares, & Button, forthcoming).

the data. Additionally, ethical clearance was granted by the former university of one author (S.L.) under approval number Ethics RM ref: 0713. All procedures adhered to the standards outlined in the Helsinki Declaration to ensure confidentiality, participant integrity, and data protection.

Reflexivity and research challenges

The empirical investigation that informs this study was shaped by a series of sociologically significant challenges, particularly at the pre-investigation stage. These challenges are not merely procedural obstacles but are themselves embedded in the socio-spatial dynamics of cybercriminal organizations, secrecy, and state surveillance. The Hustle Kingdom (HK), under investigation, operated as a highly controlled, clandestine environment. The lead operator, the proprietor, maintained an elaborate pattern of temporal evasion, limiting his physical presence at the HK to nocturnal hours between 2 a.m. and 6 a.m., thereby complicating both physical surveillance and intelligence gathering. This pattern reflects a form of spatial-temporal insulation, a deviant adaptation designed to limit visibility and reduce risk of detection, consistent with what Goffman (1963) would describe as information control within stigmatized or illicit roles.

The investigative team overcame these challenges by employing extended covert surveillance over several weeks, adopting methods typically associated with the sociology of covert fieldwork (Lee 1993). Daily observations allowed the identification of core actors (the proprietor, a gatekeeper, and an errand boy), despite the low frequency of observable movements in and out of the building. Importantly, the investigation demonstrates how surveillance operates not only as a law enforcement tactic but also as a negotiated form of social proximity. State agents adapt their gaze in response to the strategic concealment of illicit actors.

To supplement physical surveillance, the investigative team integrated open-source intelligence (OSINT) and social media intelligence (SOCMINT), critical forms of digital ethnography in contemporary cybercrime investigations. Through online platforms such as Facebook and Instagram, the proprietor's conspicuous display of unexplained wealth, lavish lifestyle, and absence of legitimate income sources were documented and triangulated. These digital traces served not only as evidence but also as windows into the self-curated moral economies that offenders construct online. Indeed, displays of wealth function as both status signals and rationalizations of success.

The arrest phase introduced additional challenges. The proprietor's irregular visiting patterns complicated efforts to match his real-time appearance with online profiles. Law enforcement faced a critical dilemma when it ceased visiting the HK for several days, heightening concerns about operational compromise. This moment reflects a broader tension in deviance research between overt enforcement and covert observation: the risk that intervention will prematurely undermine long-term evidence accumulation. To navigate this, investigators executed a preemptive arrest operation on January 22, 2024, resulting in the detention of 10 Hustle Kingdom members and the seizure of digital devices, vehicles, and financial documents. Although these arrests were crucial, the absence of the proprietor posed a threat to fully establishing the hierarchical structure of the operation. This speaks to the fluidity and resilience of deviant networks, where leadership nodes may temporarily disengage to preserve operational continuity.

Following the initial arrests, investigators adapted by leveraging institutional bureaucratic intelligence, extracting bank records, analyzing financial transactions, and identifying registered business addresses linked to the proprietor. An invitation letter was strategically delivered through intermediaries, eventually leading to the proprietor voluntarily presenting himself for questioning on January 31, 2024, where he admitted to being the mastermind behind the Hustle Kingdom operations. These challenges were temporally confined to the pre-investigation and early operational phases. Once core actors were detained and documentary evidence secured, the inquiry proceeded along more linear investigative lines, involving document analysis, suspect interrogation, and financial profiling.

From a reflexive standpoint, this investigation underscores the methodological complexity of studying concealed deviant organizations. Access is not granted but constructed through layered forms of observation, digital surveillance, informant collaboration, and adaptive strategy. The process reflects the negotiated tension between deviant efforts to conceal and institutional efforts to reveal, each constituting distinct forms of boundary work (Gieryn 1983) within the criminological field. The findings derived from this analysis are presented in the following sections.

Findings

The investigation into the Hustle Kingdom, a cybercrime school led by Mr Akpan, reveals insights into its demographics, training duration, operational structure, and prosecution outcomes. We summarize these findings from the case files, integrating them with insights from conversations with investigating officers.

Demographic patterns

The Hustle Kingdom, operated by Mr Akpan, targeted young adults, specifically those aged between 16 and 32 years. Most learners fell within the 16 to 23 age range, illustrating a focus on exploiting the aspirations of younger individuals for financial success through cybercrime. Among the 12 identified learners, ages 18 (3) and 16 (2) were the most common. The rest of the learners ranged from 19 to 32 years, with one learner in each age group: 19, 21, 22, 23, 25, 27, and 32.

Educational attainment of learners

Most learners in the Hustle Kingdom had only a secondary education, reflecting a recruitment focus on individuals with limited educational attainment. Among the twelve identified learners, ten had completed secondary education, while only two had primary education. This highlights that the academy primarily targeted individuals with basic educational backgrounds, emphasizing practical digital skills rather than formal academic qualifications.

An EFCC officer reinforced this observation, stating:

“Educational background did not play a key role in the crime. What the learners already knew was how to operate a computer and their familiarity with social media networks.”

Economic vulnerability and informal recruitment pathways

Testimonies from Hustle Kingdom (HK) learners revealed that recruitment often occurred through informal social networks, including friends, acquaintances, family members, or casual encounters, and was driven by economic need or perceived opportunity. Several learners explicitly linked their decision to join the academy to their inability to secure a stable income or start small-scale businesses.

EAD (18 years) explained:

I was introduced to the academy by my friend Faith (a guy) … I did not pay any money to join the academy.

COE (19 years) recounted:

I asked him to give me a job … he picked me up and took me to the academy where I was arrested.

MEN (22 years) described entrepreneurial frustrations:

I asked my friend Goodnews to borrow me N200k to start my carpenter business … he sent me N4,000 as transport fare to travel … where he taught me how to hack Facebook accounts.

DNE (21 years) followed a job offer after a workplace dispute, while **US (16 years)** accepted an opportunity arranged by his father's friend. Others (EOG, ISC, SSI) recounted recruitment through friends or relatives who framed the academy as a place to learn profitable skills.

These narratives illustrate that economic vulnerability was intertwined with interpersonal trust and opportunistic recruitment, often bypassing formal job-seeking channels.

Duration of training and operational structure

Learners spent varying lengths of time at the Hustle Kingdom, ranging from one to five months, with the majority staying between one and three months. Specifically, three learners each stayed for one and three months, while two stayed for four months, and one each stayed for two and five months. This relatively short duration suggests an intensive training model designed to quickly produce proficient cybercriminals. However, this time frame may have been influenced by the timing of arrests, making it difficult to confirm the exact operational structure.

The Hustle Kingdom operated from a well-equipped five-bedroom duplex, which indicated a significant level of planning and investment. Describing Mr Akpan's strategy to avoid detection, one EFCC officer stated:

"It was only one [operator] (Mr Akpan) who visited the Hustle Kingdom, and it was always at the wee hours… it was not easy to ascertain the number of persons in the building because movement in and out was less frequent."

This deliberate secrecy and infrequent movement made monitoring the facility challenging, requiring weeks of intensive surveillance.

The cost of "free" training

Although only one principal operator, the owner, was physically based at Hustle Kingdom, the operation exhibited hallmarks of an organized crime enterprise. All learners were personally recruited by him and channeled into the academy, where he provided food, accommodation, equipment, and training materials at no upfront cost. No school fees or maintenance charges were required, making entry appear gratis. These provisions were an investment to be repaid. Once learners began earning from scam activities, a percentage of their proceeds was taken until the cost of training and logistics was fully recovered.

This structured arrangement, with defined roles, profit-sharing, and sustained criminal collaboration, satisfies criminological definitions of organized crime despite the absence of multiple managers on site.

The socioeconomic backgrounds of participants reinforce the Mertonian "innovation" mode of adaptation. Most entered with limited formal employment prospects, viewing cybercrime training as a practical route to culturally endorsed goals of financial stability and independence. As one 21-year-old learner explained:

I used to work at Terminal Hotel, Benin City, Edo State. One day I had a payment problem with my manager and [the Hustle Kingdom Proprietor] was there during the argument … he later asked me to follow him to Uyo that he can give me a job … I have to pay my transport by myself … He picked me from the park and took me to the house (academy) where I was arrested.

Such accounts show how financial strain, exacerbated by workplace disputes, underpayment, or unemployment, pushed learners toward "innovative" adaptations: pursuing legitimate aspirations through illegitimate but accessible means. The academy taught not only the technical skills for hacking, sextortion, romance fraud, and BEC schemes, but also methods of victim approach, persuasive scripting, and operational security, providing a full deviant opportunity structure for rapid income generation.

Investigation process and challenges

Investigators faced difficulties due to the academy's secrecy and Mr Akpan's sporadic late-night visits. However, using daily covert surveillance, OSINT, and SOCMINT, they gathered sufficient evidence. One officer reflected:

"The operators were careful about their activities… this challenge was overcome through the use of daily covert surveillance."

Legal strategy and prosecution outcomes

Among the 12 individuals connected to the Hustle Kingdom, only half (six individuals) were prosecuted. The remaining six were excluded from prosecution due to age, involvement level, and lack of substantial material benefit from the operation. For instance, minors and those who did not gain significantly from the crimes were not charged.

Mr Akpan, the operator of the Hustle Kingdom, pled guilty, which resulted in a reduced sentence. One EFCC officer explained:

“The evidence against [the proprietor] was strong because the students indicted him in their statements. He agreed to plead guilty, and the charges were reduced from 10 to 2.”

This plea agreement highlights how evidence and cooperation influenced the prosecution process. Selective prosecution in these cases illustrates the balancing act between ensuring accountability and considering mitigating factors, such as the offenders’ age and degree of involvement.

Assets recovery and financial gains

The proprietor benefited ₦15,000,000 from his Hustle Kingdom enterprise; this amount was not recovered as cash but indicates the scale of the operations. As one officer confirmed:

“The proprietor had no legitimate business. He admitted that the assets were acquired through proceeds from the HK.”

These assets linked the operation to cybercrime and money laundering activities.

Operational structure and training focus

The Hustle Kingdom was a structured, single-operator establishment. An EFCC officer explained:

“There was one aim: teach students how to hack Facebook accounts and hand over the task to the proprietor.”

Friends introduced students to Mr Akpan, indicating a hierarchical recruitment model under the figure known as “chairman.”

Law enforcement and policy implications

The case highlighted areas for policy intervention, particularly regarding property owners who unknowingly aid criminal enterprises. One officer suggested:

“Property owners are creating safe havens for cybercriminals… they should face sanctions where they fail to conduct due diligence.”

The case also stressed the importance of intelligence sharing and interagency collaboration in cybercrime investigations.

Institutional framing and prosecutorial narrative

Court observations revealed how the prosecution consistently portrayed the Hustle Kingdom as a sophisticated and well-structured criminal enterprise, rather than a loosely coordinated network. In one proceeding, the prosecuting counsel repeatedly referred to the academy as a “factory of fraudsters,” echoing public rhetoric that seeks to pathologise youth cybercrime as a threat to national security. Although this phrase did not appear in the case files, the courtroom discourse helped us understand the state's framing of cybercrime academies not merely as legal infractions but as existential risks, which shaped both the charges and sentencing recommendations.

Operational secrecy and isolation

While the case files provided detailed testimony about the restricted mobility of academy members, fieldnotes from EFCC proceedings underscored the performative emphasis placed on this isolation during trials. Judges and prosecutors often returned to the theme of "indoctrination" and "in-house confinement" to differentiate these actors from independent fraudsters. Observing these interactions in court helped clarify how prosecutors construct narratives of structure and hierarchical control to elevate the severity of the offense.

Multipurpose scam infrastructures

The Hustle Kingdom ran multiple scam platforms. These included fake flower delivery services, counterfeit online stores, and fraudulent foreign exchange trading. These platforms served as fronts for cyber fraud and demonstrated the group's logistical and technical capacity.

Fraud via compromised social media accounts

A recurring tactic involved hijacking victims' social media profiles. Offenders then impersonated contacts to request money. These scams exploited digital trust networks and channelled funds through transnational laundering routes. Chinese bank accounts featured in multiple transactions.

Structured revenue sharing

The group used a fixed 60/40 profit split. Mr Michael Akpan received the larger share; his key associate took the rest. Official records confirmed this split. The model reflects a stable internal hierarchy and a rational, business-like approach to fraud.

Concealment strategies and surveillance evasion

Restricted movement and erratic visit patterns shielded the Hustle Kingdom from early detection. Investigators struggled to map the number of residents or the scope of activities. As one officer remarked:

"It was not easy to ascertain the number of persons in the building."

These secrecy measures frustrated enforcement efforts until the final coordinated raid.

Discussion

The Hustle Kingdom phenomenon exemplifies how young people, faced with persistent economic exclusion and systemic marginalisation, mobilise illicit innovation as an adaptive strategy within limited opportunity structures. The investigation into the Hustle Kingdom, operated by Mr Akpan, provides important insights into the structure, recruitment strategies, and motivations of individuals involved in this cybercrime operation. Additionally, it sheds light on the socio-economic factors that drive young men into digital fraud activities. To situate these findings within a wider context, cybercrime in Nigeria is best understood within its dominant motivational and sociocultural framework. As outlined by Ibrahim (2016), while the Tripartite Cybercrime Framework (TCF) categorises cybercrime motivations into three domains (socio-economic, psychosocial, and geopolitical), socio-economic motivations overwhelmingly dominate in Nigeria. Most online offences involve financially driven fraud schemes, according to many prior empirical studies in this region (e.g., Akanle et al. 2016; Aransiola and Asindemade 2011; Garba et al. 2024; Ibrahim 2017; Lazarus and Okolorie 2019; Ogunleye et al. 2019; Soares et al. 2025). The Hustle Kingdom case exemplifies this pattern, with participants primarily motivated by blocked economic opportunities and aspirations for material advancement. Against this backdrop, the discussion that follows situates Hustle Kingdom within broader debates on strain, gender, education, politics, colonial legacies, and cultural dynamics shaping cybercrime.

Gender, motivations, and the role of masculinity

The Hustle Kingdom case reveals insights into the socio-economic and cultural forces that drive young Nigerian men toward cybercrime, particularly regarding notions of masculinity and material wealth. As seen in the wider internet fraud trend in Nigeria, participants in the Hustle Kingdom were predominantly young men. This part of our findings reflects a gendered pattern observed in existing cybercrime research in Nigeria (Aransiola and Asindemade 2011; Lazarus 2018; Lazarus and Okolorie 2019; Soares and Lazarus 2024). Even when studies have interviewed female online scammers in Nigeria, the data reveal that they often occupy subordinate roles, while men in their lives, such as brothers or boyfriends, tend to play core roles and act as mentors (e.g., Ogunleye et al. 2019). This male dominance is often attributed to the socialisation of men into roles that emphasise masculinity and the pursuit of material success, which drives them toward these criminal activities (cf. West and Zimmerman 1987).

This gendered pattern is neither static nor universal, but reflects culturally specific constructions of masculinity and femininity. Although gender roles are shaped by social norms globally, their articulation in Nigeria contrasts sharply with patterns observed in the Global North (Obioma et al. 2022). The "image of womanhood" reflects societal expectations imposed on women, shaping both their participation in male-dominated spheres and collective notions of femininity (cf. Ibrahim and Komulainen 2016:60). Such perceptions shape how women interact with men and how female citizens are culturally perceived. Viewed through sociocultural and feminist lenses, online scamming is often more socially rationalised for men than women, aligning with normative ideals of assertiveness and financial provision in Nigeria (Lazarus and Okolorie 2019:23):

"*Our culture is that a man as a man you have to take the girl o-u-t! And when a man has one, two, three of them [women], he has to find means to support them. You see, some married men have concubines. You also see some married men; their religion allows them to marry three, four! So, a man with four wives in a culture where the man has to be the provider, the bait would be much more for him than for women whose business it is to receive and look good*"

These relations align with broader gendered patterns of how men and women "do gender" in Nigeria, where cultural and structural norms shape differential expectations and opportunities

(Ibitoye et al. 2024; Lazarus et al. 2017; Ononokpono, Ugwu, and Odimegwu 2025; Udoh, Folarin and Isumonah 2020). What occurs offline reverberates online. Hence, these dynamics are generally reflective of broader analyses of gender and cybercrime (Bada et al. 2021; Lam and Mesch 2025; Lazarus, Button and Kapend 2022; Steinmetz, Holt, and Holt 2019). The Hustle Kingdom's male-dominated environment reinforces the notion that cybercrime in Nigeria follows a gendered structure, where men are viewed as economic providers, and wealth becomes a critical aspect of male identity and social status. This gendered expectation places additional pressure on men to meet cultural standards of success, which can illuminate why some turn to alternative means when legitimate opportunities are blocked.

Strain Theory (Merton 1938) helps explain this phenomenon, suggesting that individuals may turn to deviant behaviours to achieve their goals when legitimate paths to success are inaccessible. In Nigeria, where higher education is largely out of reach for many due to financial constraints, Hustle academies emerge as an alternative. According to our data, Hustle academies operate on a gratis model, requiring no upfront payment: "I did not pay any money to join the academy," one learner noted. Consequently, young men who are financially excluded from the formal education system often turn to illicit avenues such as the Hustle Kingdom for economic advancement. Socio-economic strain intersects with culturally ingrained ideas about masculinity to amplify these pressures.

As West and Zimmerman (1987) argue, masculinity is cultivated through socialisation processes that position men as economic providers. In Nigeria, this expectation is further intensified by cultural norms linking wealth with social prestige and influence. The pressure on men to acquire wealth, often by any means necessary, is pervasive and deeply rooted in these cultural expectations. Popular culture, particularly the rise of Afrobeats music, reinforces these socio-economic and gendered pressures. Many Afrobeats artists glamorise internet fraudsters in their lyrics, portraying them as successful figures who embody the aspirations of young men. This cultural artefact becomes an agent of social enculturation, influencing perceptions of cybercrime as a legitimate path to material wealth. Adeduntan (2022), Lazarus (2018), Onanuga (2020), and Lazarus et al. (2023) argue that Afrobeats lyrics socially legitimise deviant figures, normalising cybercrime across Nigeria, the African diaspora, and beyond. The conspicuous consumption flaunted by internet scammers, glamorised in popular music, has consequences. For example, it serves as a public display of wealth and masculinity, further embedding these values within society (Lazarus et al. 2023).

For young men in the Hustle Kingdom, accumulating material wealth through cybercrime becomes not only a means of financial survival but also a way to perform masculinity and secure social respect (Lazarus and Soares 2025). As Lazarus and Okolorie (2019), Richards and Eboibi (2021), Smith (2017) and Ibrahim (2015) discuss, the value of money and participation in illicit economies in Nigeria extends beyond its economic utility. It is deeply entangled with sociocultural dynamics and individual relationships (Smith 2017). Spending on significant life events, such as weddings, funerals, and other celebrations, serves both functional and symbolic purposes, transforming wealth into social prestige (Lazarus 2019). This focus on wealth aligns with the concept of "doing gender" (West and Zimmerman 1987), where conspicuous consumption is employed as a visible marker of masculine success.

Cybercrime academies or Hustle Kingdoms should be seen as more than just criminal enterprises. They are adaptive responses to socio-economic challenges and cultural demands for material success. The intersection of economic strain, cultural expectations, and popular culture's influence underscores how cybercrime becomes a path not only to economic stability but also to social validation. This combination of factors demands a nuanced understanding of the socio-cultural forces that shape cybercriminal pursuits. Thus, we argue that the enterprise and entrepreneurship within the Hustle Kingdom are like an insect suspended in the intricate webs of culture and society, and to analyse these entities, their actions, and those who observe, critique, or question them, one must seek out meaning and subjective experience (cf. Geertz 2017).

In West Africa, media portrayals of scammers do not generate significant moral panic (Abubakari 2025; Abubakari and Blaszczyk 2023; Fuh 2021; Lazarus, Button, and Adogame 2022), as these individuals are seen as marginalised "boys" engaged in entrepreneurial activities. Even as online scammers face condemnation, social media narratives simultaneously reveal moral ambivalence, framing such fraud as a response to economic deprivation (Abayomi-Alli et al. 2022). Precisely, public discourse on social media often collapses the boundaries between the perceived fraudulence of Nigerian religious leaders (Lazarus, Tickner and Button 2025) and that of politicians and cybercriminals (Lazarus, Button, and Adogame 2022). These blurred boundaries between symbolic power figures, such as politicians and religious leaders, dilute and redirect moral outrage.

Aransiola and Asindemade (2011), Lazarus and Button (2022), Orhero and Nwoke (2025), along with Richards and Eboibi (2021), implicated symbolic power actors (cf. Bourdieu 1991) and other influential elites as accomplices in cybercrime, further weakening the moral condemnation of scam entrepreneurs. These reflections highlight an under-researched paradox. Institutional watchdogs share the same moral playbook as the wolves they guard against, invoking similar justificatory narratives to rationalise their failings or even their own illicit practices (Shepherd and Button 2019). This broader paradox aligns with a classic sociological insight about deviance as a mirror of society rather than its outsider. Following Matza and Sykes (1961:717), the Hustle Kingdom participants illustrate that "the delinquent… may not stand as an alien in the body of society but may represent a disturbing reflection or a caricature instead." Therefore, unlike the "folk devil" image assigned to other groups, such as "sharenters" (Ugwudike, Lavorgna, and Tartari 2023:516), a shared cultural tolerance diminishes the intensity of societal backlash, further entrenching the normalisation of cybercrime within this context. Building on the structural and cultural drivers of Hustle academies, we now examine economic precarity as a recruitment lever.

Economic precarity and structural exclusion as gateways to cybercrime training

As one 18-year-old learner recalled:

My friend "Nikki" told me about the academy … when I got there, I saw [the proprietor], who we call chairman or boss, and he teach us how to hack Facebook accounts.

This testimony captures two key recruitment logics: social-tie mediation and the framing of illicit skill acquisition as a pathway to economic advancement. Across participants, economic precarity repeatedly operated as the entry lever, whether to start a small business, escape exploitative employment, or secure any form of paid work. The absence of upfront fees rendered participation seemingly cost-free, yet it functioned as a debt arrangement to be repaid from scam earnings, binding recruits into sustained criminal collaboration.

These trajectories align with Merton's (1938) strain theory, in which blocked access to legitimate economic opportunities creates disjunction between culturally prescribed goals and available lawful means. Hustle Kingdom embodied an innovative adaptation: culturally sanctioned aspirations (such as financial stability and independence) pursued through illegitimate yet accessible means. Socially, recruitment followed the logic of differential association theory (Sutherland, Cressey, and Luckenbill 1992), where entry is facilitated through interpersonal trust and normative reframing of deviance.

The learners' biographies reveal structural exclusion from Nigeria's postcolonial educational hierarchy. Similarly, prior research highlights a hierarchy deeply shaped by colonial-era disparities in access to Western education, stemming from uneven patterns of Christianisation and colonisation in Nigeria (Lazarus and Button 2022). In southern Nigeria, the site of this Hustle Kingdom case, university credentials serve as both class capital and moral endorsement. This status function is a historical legacy rooted in missionary schooling and elite networks (Lazarus and Button 2022). Higher education operates not merely as a route to employment, but also as a means of conferring symbolic capital and legitimacy within elite social circles. By contrast, the Hustle Kingdom cohort, none with university degrees, most with only secondary or primary schooling, stood outside these legitimising structures.

Their exclusion was not simply poverty-driven but rooted in systemic disqualification from institutionalised pathways to status and mobility. This disqualification renders the promise of upward mobility highly visible yet materially inaccessible, producing what might be termed status strain: acute awareness of societal success norms without viable lawful routes to achieve them. In this sense, Hustle Kingdom functioned as a deviant substitute for the absent university, mimicking its institutional form while inverting its purpose, providing illicit skill training and spiritual discipline in place of accredited curricula, and generating illicit capital in place of socially sanctioned credentials. We now examine the scam methodology of the Hustle Kingdom enterprise.

Scam methodology

Founded in August 2023, Mr Akpan's "Hustle Kingdom" operated from a five-bedroom duplex, showcasing his academy's scale and organisational prowess. At Hustle Kingdom, Mr Akpan taught his recruits how to hack social media accounts, such as Facebook, which was a foundational step in his broader scam network (according to our data analysis). Once students successfully compromised these accounts, Mr Akpan would assume control and employ various social engineering techniques to deceive the contacts of the original account holders. These individuals were often unwittingly enlisted as "money mules" – persons who received and transferred illicit funds from fraudulent activities.

These scams included fake foreign exchange (FX) trading platforms and phoney online shopping websites that Mr Akpan had established. One fraudulent site, "Express Line Logistics," was advertised as a provider of diverse services, from product sales to flower deliveries. Victims were lured in, making payments for products that were never delivered. In addition to these schemes, Mr Akpan utilised hacked social media accounts to solicit direct financial assistance from the compromised account holders' contacts, thus widening his web of deception.

The financial proceeds from these scams were predominantly laundered through Chinese bank accounts, illustrating a broader pattern characteristic of transnational cybercrime networks. According to Mr Akpan, the distribution of profits followed a 60/40 formula, with him and his brother, who remains at large, claiming sixty per cent. The remaining forty per cent was allocated to intermediaries who facilitated the transactions by providing the essential banking infrastructure.

This operational model underscores the clandestine nature of Mr Akpan's Hustle Kingdom, marked by its stringent control over movement and secrecy. Law enforcement noted that Mr Akpan was the only individual observed visiting the premises, and only during the early morning hours, further obscuring the scale of participation within the building. This deliberate restriction of access reflects the strategic use of both technological and covert practices to manage his network and avoid detection.

Mr Akpan's role as a cybercrime entrepreneur represents a form of adaptive innovation within the economic constraints of his environment, aligning with Merton's theory of "innovation under strain" (Merton 1938). The socio-economic pressures that drive young men to cybercrime, as discussed earlier, are further exemplified by Mr Akpan's establishment of an alternative criminal pathway to achieve financial success. The Hustle Kingdom can be viewed as a social institution in its own right, designed to systematically train and deploy emerging cybercriminals. The adaptability and fluid structure of the organisation, similar to Lazarus (2024) and Leukfeldt, Kleemans, and Stol (2017a, 2017b), further enable the rapid indoctrination and mobilisation of "new" scammers, reflecting the evolving nature of the criminal enterprise. Much like other subcultural networks reported by Nguyen and Luong (2020), this system thrives on its capacity to innovate in response to socio-economic constraints, thereby perpetuating its existence and expanding its influence.

Structure and operational efficiency of Hustle Kingdom

The Hustle Kingdom, operating from a sophisticated, secretive five-bedroom duplex, epitomises high-tech cybercrime operations. While Nguyen and Luong (2020), Lazarus (2024), Cretu-Adatte et al. (2024), and Leukfeldt, Kleemans, and Stol (2017a) did not examine Hustle Kingdoms, their research provides pertinent insights into similar phenomena. The facility's covert operational design, marked by limited and odd-hour visitations, complicates the tracking of occupancy and activity, thereby enhancing its secrecy.

"It was only one [operator] (The proprietor) who visited the HK, and it was always at the wee hours of the day… it was not really easy to ascertain the number of persons in the building because movement in and out of the building was less frequent,"

noted one officer. This highlights the clandestine nature of the Hustle Kingdom. Despite its structured organisation, the network's high mobility enhances its adaptability and manoeuvrability against law enforcement detection. Unlike conventional institutions like polytechnics or cosmetology schools, Hustle academies' agility in relocating significantly bolsters their evasion capabilities, as evidenced by our data.

The training at Hustle Kingdoms, ranging from one to five months, underlines its operational efficiency[6]. It swiftly equips recruits with digital fraud skills, specifically focusing on

[6] The duration of training varies considerably depending on the Hustle Kingdom's internal curriculum, the areas of expertise of the "owner," and the capacities of the individual learner. While some may graduate and begin earning substantial sums from victims within a few months, others require longer periods of instruction before they are deemed proficient enough to operate independently.

developing technical scamming capabilities (Lazarus and Soares 2025). In stark contrast, Nigeria's traditional educational institutions, burdened by cost, bureaucracy, and a high unemployment rate among graduates (Ibrahim 2016), fail to meet these needs. The Hustle Kingdom addresses these gaps by providing immediate employment opportunities and requiring trainees to remit a portion of their earnings as tuition under the academy's proprietorship, according to our analysis. This model starkly contrasts with traditional educational systems and is birthed from socio-economic exclusions. Addressing the Hustle Kingdom phenomenon necessitates robust socio-economic reforms and law enforcement strategies, focusing on rehabilitating youth across West African nations such as Nigeria and Ghana. The reliance on innovative tactics by the Hustle Kingdom accentuates the substantial deficiencies in Nigeria's educational system to meet societal goals legally. These insights also necessitate a deeper understanding of the subtle enablers and systemic challenges in prosecuting cybercriminal networks.

Subtle enablers and systemic challenges in cybercrime prosecution

The Hustle Kingdom case highlights not only the direct participants involved in cybercriminal activities but also underscores the role of subtle enablers who contribute to the broader infrastructure that allows such scams to thrive. Insights from the case files and informal officer interviews reveal a complex web of indirect support that sustains these operations. For example, the role of property owners who lease spaces without sufficient oversight aligns with findings from Whittaker, McGuire, and Lazarus (2025), Wang, Su, and Wang (2021), Levi (2022), and Lazarus (2024) on how professionals can inadvertently or intentionally enable illegal activities. For example, Whittaker, McGuire, and Lazarus (2025) show how Cameroonian website developers assist internet fraudsters by creating fake websites to facilitate illicit activities. In parallel, one officer in this empirical treatment of the Hustle Kingdom phenomenon noted:

"Property owners are creating safe havens for cybercriminals… they should be subjected to sanctions where they fail to conduct due diligence."

This observation reflects how legally ambiguous actions by certain actors bolster the resilience of fraud networks.

Additionally, systemic challenges within the Nigerian justice system complicate the prosecution process. With only half of the individuals connected to the Hustle Kingdom facing legal consequences, this case highlights the challenges of prosecuting cybercrime, as noted by Idem et al. (2023). According to one officer:

"Cybercriminals are never really working alone. This case has the potential to assist law enforcement agencies in looking at the important aspects of cybercrime investigation and prosecution."

This need for interagency collaboration and stronger legal frameworks is crucial for effectively dismantling operations like Hustle Kingdom, where gaps in prosecution allow many perpetrators to evade justice. This dynamic mirrors Holt and Lee's (2020) qualitative crime script analysis of 19 vendors on the Open and Dark Web, which shows how these actors enable cybercriminal activity by advertising, facilitating, and delivering counterfeit documents.

The Hustle Kingdom case demonstrates the presence of indirect enablers, such as landlords, who, knowingly or unknowingly, facilitate cybercrime academies by providing operational spaces. Ethnographic field notes indicated that, while the EFCC aimed to have the property forfeited, the current legislation, under Section 3 of the Advance Fee Fraud and Other Fraud-Related Offences Act 2006, was insufficient. Even though the property was implicated due to the owner renting it to the Hustle Kingdom operator, there was no sufficient evidence to demonstrate the landlord's knowledge of the illegal activities. This highlights the need for specific legislation targeting the use of premises for cybercrime operations, extending to hotels and luxury apartments. This reinforces Holt and Lee's (2020) argument for a broader understanding of cybercrime ecosystems, recognising that dismantling these networks requires focusing beyond direct actors. This understanding of indirect enablers in the Hustle Kingdom case lays a foundational context for understanding Hustle Kingdoms' broader implications, both locally and globally, as these operations extend far beyond Nigeria.

Limitations

The sample size of 12 case files from the Hustle Kingdom, with only six leading to prosecution, might be considered small. However, as the first study of its kind based on existing convicted case files related to the Hustle Kingdom phenomenon from the EFCC, the sample size is inherently limited. Since these are the only available records, the researchers could not expand the sample size despite any concerns about its scope. This study adopts an emic approach, incorporating court artefacts, informal conversations with officers, and ethnographic field notes to provide rich qualitative insights. The focus is on depth rather than breadth, offering a distinct interpretive lens into the lived experiences and constructed realities within these criminal networks. While larger samples are typically advantageous for statistical analyses, combining convicted files with conversations and diary notes in this study provides essential context and depth beyond mere numbers. Besides, Lusthaus et al. (2025) conducted their study using two debrief cases, demonstrating that smaller samples yield valuable insights. In this context, the sample size is not a limitation but is instead aligned with the study's goal of providing an in-depth understanding, laying the foundation for future research in this domain.

Conclusion

This study has demonstrated that Hustle Kingdoms function as a structured training ground that inculcates technical expertise, cultural scripts, and patterned strategies for the perpetration of internet fraud. Beneath acts of deviance lie deeper social currents of inequality, disillusionment, and adaptation, revealing how illicit innovation operates as a functional response to systemic economic strain. This study is the first to analyse convicted Hustle Kingdom cases, filling a critical gap in cybercrime scholarship. The case of Mr Akpan and the Hustle Kingdom highlights a growing trend in West Africa, where cybercrime academies are producing a new generation of digital fraudsters. Unlike prior studies focused on specific types of cybercrime, such as cryptocurrency fraud (Garba et al. 2024), this research examines broader organisational structures, recruitment strategies, and operational dynamics. The Hustle Kingdom's decentralised and adaptable model is embedded in Nigeria and Ghana, where poverty and limited opportunities drive youth into cybercrime. As these academies expand, their global influence becomes increasingly significant, necessitating coordinated responses from local and international stakeholders.

Our findings stress the importance of strong law enforcement, international cooperation, and socio economic interventions aimed at addressing the root causes of these activities. By analysing EFCC conviction records and integrating insights from prosecuting officers, this study provides a comprehensive view of the Hustle Kingdom's operations. It also identifies indirect enablers, such as property owners, who may unknowingly provide safe spaces for these networks. The challenges in prosecution reveal systemic inefficiencies, as partial prosecutions allow cybercriminals to avoid full accountability, and gaps in regulatory frameworks enable these networks to persist. Although substantial assets were seized, the limited legal actions highlight the need for stronger frameworks to dismantle such operations. This study not only contributes to cybercrime research but also lays the groundwork for future policies that address both direct participants and those who indirectly support these networks. Despite the small sample size, it provides foundational insights based on available court data on Hustle Kingdom cases.

Countermeasures must go beyond socio-economic interventions. Cultural norms linking masculinity to wealth must be reconsidered when examining the motivations of Yahoo Boys. Addressing structural inequalities and the glorification of wealth will pave the way for more effective strategies, offering young men alternative pathways to achieve respect and status without resorting to crime. These insights are vital for policymakers, law enforcement, and international stakeholders in combating digital fraud. Stronger partnerships between local and international actors, coupled with socio-economic reforms, could limit the reach of entities like the Hustle Kingdom, ultimately strengthening global cybersecurity. A comprehensive response, combining law enforcement, policy reform, and socio-economic interventions, can disrupt these networks and prevent the recruitment of vulnerable youth. The effectiveness of such interventions also depends on the quality of collaboration between researchers and practitioners.

Although this project brought academics and law enforcement together, such collaborations are still uncommon in Africa south of the Sahara. To advance cybercrime prevention, investigation, and policy, these partnerships need to be expanded and formalised. Prior studies (Garba, Lazarus and Button 2024; Lazarus and Okolorie 2019; Soares, Lazarus and Button 2025) illustrate the potential of joint initiatives between academics and law enforcement officers. However, more sustained engagement is required to align scholarly analysis with enforcement practice. Building this bridge would enhance impact, support victims more effectively, and strengthen responses to the realities of cybercrime on the ground. We conclude that the Hustle Kingdom operates as an alternative institution arising from societal structures that restrict legitimate access to success, pushing individuals toward deviant pathways for financial security. This deeper understanding highlights the challenges in developing effective policy and law enforcement strategies in Nigeria and beyond.

Ethics approval statement

Ethics approval for this study was obtained from the Economic and Financial Crimes Commission (EFCC), Nigeria (CB:4000/EFCC/UYO/LEGAL/VOL.1/45).

Corresponding author:

Suleman Lazarus, PhD, Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), Houghton Street, London, WC2A 2AE, United Kingdom.
Email: suleman.lazarus@gmail.com
ORCID: https://orcid.org/0000-0003-1721-8519

Acknowledgements

We thank our Creator for making this collaborative work possible.

References (APA 7th)

Abayomi-Alli, A., Abayomi-Alli, O., Misra, S., & Fernandez-Sanz, L. (2022). Study of the Yahoo-Yahoo hash-tag tweets using sentiment analysis and opinion mining algorithms. *Information, 13*, 152. https://doi.org/10.3390/info13030152

Aborisade, R. A. (2022). Yahoo Boys, Yahoo Parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior, 44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Abubakari, Y. (2025). Forgiveness-seeking behaviors among online romance fraudsters: Insights from Sakawa actors in Ghana. *International Journal of Offender Therapy and Comparative Criminology*. https://doi.org/10.1177/0306624X251322533

Abubakari, Y., & Blaszczyk, M. (2023). Politicization of economic cybercrime: Perceptions among Ghanaian Facebook users. *Deviant Behavior, 45*(4), 483–502. https://doi.org/10.1080/01639625.2023.2253487

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies, 34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Adeniran, A. I. (2008). The Internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Agnew, R. (2013). When criminal coping is likely: An extension of General Strain Theory. *Deviant Behavior, 34*(8), 653–670. https://doi.org/10.1080/01639625.2013.766529

Ajayi, T. M., Adesope, O. A., & Oso, I. O. (2024). Yahooism to ritualism: Ideological motivations for cyber fraud in selected Yoruba films. *Southern African Linguistics and Applied Language Studies, 43*(1), 102–116. https://doi.org/10.2989/16073614.2024.2341708

Akanle, O., Adesina, J. O., & Akarah, E. P. (2016). Towards human dignity and the Internet: The cybercrime (Yahoo Yahoo) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation & Development, 8*(2), 213–220. https://doi.org/10.1080/20421338.2016.1147209

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior and Social Networking, 14*(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Bada, M., Chua, Y. T., Collier, B., & Pete, I. (2021). Exploring masculinities and perceptions of gender in online cybercrime subcultures. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in context. Crime and justice in digital society* (Vol. I). Springer. https://doi.org/10.1007/978-3-030-60527-8_14

Bourdieu, P. (1991). *Language and symbolic power.* Harvard University Press.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

Button, M., Gilmour, P. M., Hock, B., Jain, T., Jesperson, S., Lazarus, S., Pandey, D., & Sabia, J. (2024). *Scoping study on fraud centres: Ghana, India and Nigeria.* ITAD. https://eprints.lse.ac.uk/126338/

Callaghan, E. (2005). What they learn in court: Student observations of legal proceedings. *Teaching Sociology, 33*(2), 213–220. https://doi.org/10.1177/0092055X0503300208

Chism, K. A., & Steinmetz, K. F. (2017). Technocrime and strain theory. In K. F. Steinmetz & M. R. Nobles (Eds.), *Technocrime and criminological theory* (pp. 66–84). Routledge. https://doi.org/10.4324/9781315117249

Cretu-Adatte, C., Azi, J. W., Beaudet-Labrecque, O., Bunning, H., Brunoni, L., & Zbinden, R. (2024). Unravelling the organisation of Ivorian cyberfraudsters: Criminal networks or organised crime? *Journal of Economic Criminology, 3*, 100056. https://doi.org/10.1016/j.jeconc.2024.100056

Cross, C. (2020). “Oh we can’t actually do anything about that”: The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice, 20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Cross, C., & Holt, T. J. (2025). Does age matter? Examining seniors’ experiences of romance fraud. *Security Journal, 38*(46). https://doi.org/10.1057/s41284-025-00486-0

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175. https://doi.org/10.1080/17440572.2012.702523

Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students’ online offending. *Victims & Offenders, 11*(4), 556–577. https://doi.org/10.1080/15564886.2016.1173157

Economic and Financial Crimes Commission. (2024). *Internet fraud academy proprietor bags 10 years jail term.* https://www.efcc.gov.ng/efcc/news-and-information/news-release/9995-internet-fraud-academy-proprietor-bags-10-years-jail-term

Franceschini, I., Li, L., & Bo, M. (2025). *Scam: Inside Southeast Asia's cybercrime compounds.* Verso Books.

Fuh, D. (2021). Chihuahua promises and the notorious economy of fake pets in Cameroon. *Journal of African Cultural Studies, 33*(3), 387–403. https://doi.org/10.1080/13696815.2021.1949967

Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. *Current Issues in Criminal Justice,* 1–17. https://doi.org/10.1080/10345329.2024.2403294

Geertz, C. (2017). *The interpretation of cultures.* Basic Books.

Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review, 48*(6), 781–795. https://doi.org/10.2307/2095325

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity.* Simon & Schuster.

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

Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: The multiscalar production of cybercrime. *Trends in Organized Crime, 24*(2), 282–307. https://doi.org/10.1007/s12117-020-09392-w

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, Southern criminology and diversifying research agendas. *Progress in Human Geography, 48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Hall, T., & Ziemer, U. (2024). Online deviance in post-Soviet space: Victimisation, perceptions and social attitudes amongst young people, an Armenian case study. *Digital Geography and Society, 7*, 100096. https://doi.org/10.1016/j.diggeo.2024.100096

Hay, C., & Ray, K. (2019). General Strain Theory and cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 1–18). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-90307-1_21-1

Hock, B., Park, H., Oh, J., & Button, M. (2025). The profile and detection of bribery in South Korea. *Crime, Law and Social Change, 83*(1), 15. https://doi.org/10.1007/s10611-025-10201-0

Holt, T. J., & Lee, J. R. (2020). A crime script analysis of counterfeit identity document procurement online. *Deviant Behavior, 43*(3), 285–302. https://doi.org/10.1080/01639625.2020.1825915

Ibitoye, O. A., Falana, B. A., Olusegun, I. D., Oyeyipo, E., & Ajiboye, S. K. (2024). Women in the workforce and family-related challenges of married women in Kwara State, Nigeria. *African Identities,* 1–10. https://doi.org/10.1080/14725843.2024.2427191

Ibrahim, S. (2015). A binary model of broken home: Parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana. In S. R. Maxwell & S. L. Blair (Eds.), *Contemporary perspectives in family research* (Vol. 9, pp. 311–340). Emerald. https://doi.org/10.1108/S1530-353520150000009014

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47,* 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2017). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1–9). IEEE. https://doi.org/10.1109/ICCCF.2016.7740439

Ibrahim, S., & Komulainen, S. (2016). Physical punishment in Ghana and Finland: Criminological, sociocultural, human rights and child protection implications. *International Journal of Human Rights and Constitutional Studies, 4*(1), 54–74. https://doi.org/10.1504/IJHRCS.2016.076060

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023). The prosecution of cybercrimes in Nigeria: Challenges and prospects. In *2023 International Conference on Cyber Management and Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/CyMaEn57228.2023.10050896

Lam, I., & Mesch, G. S. (2025). Gender differences in public perceptions of the seriousness of offline and online sexual harassment. *Psychology, Crime & Law,* 1–24. https://doi.org/10.1080/1068316X.2025.2491595

Lazarus, M., & Button, M. (2024). Hustle academies: West Africa's online scammers are training others in fraud and sextortion. *The Conversation.* https://theconversation.com/hustle-academies-west-africas-online-scammers-are-training-others-in-fraud-and-sextortion-238253

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), 63–81.

Lazarus, S. (2019). Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions, 10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "Black Axe" confraternity. *Deviant Behavior, 46*(4), 456–480. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and reactions: Revealing the geographies of cybercrime perpetrators and the North–South divide. *Cyberpsychology, Behavior, and Social Networking, 25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., Button, M., & Adogame, A. (2022). Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). *Heliyon,* e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., Garba, K. H., Soares, A. B., & Hughes, M. (2025). Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. *Journal of Economic Criminology, 7,* 100128. https://doi.org/10.1016/j.jeconc.2025.100128

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice, 61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Chiang, M., & Button, M. (2025). Assessing human trafficking and cybercrime intersections through survivor narratives. *Deviant Behavior,* 1–18. https://doi.org/10.1080/01639625.2025.2470402

Lazarus, S., Hughes, M., Button, M., & Garba, K. H. (2025). Fraud as legitimate retribution for colonial injustice: Neutralization techniques in interviews with police and online romance fraud offenders. *Deviant Behavior,* 1–22. https://doi.org/10.1080/01639625.2024.2446328

Lazarus, S. I., Rush, M., Dibiana, E. T., & Monks, C. P. (2017). Gendered penalties of divorce on remarriage in Nigeria: A qualitative study. *Journal of Comparative Family Studies, 48*(3), 351–366. https://doi.org/10.3138/jcfs.48.3.351

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology, 2,* 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Lazarus, S., & Soares, A. B. (2025). From business centres to Hustle Kingdoms: Historical perspectives on innovative models of deviant education. *International Annals of Criminology,* 1–20. https://doi.org/10.1017/cri.2025.1

Lazarus, S., Tickner, P., & Button, M. (2025). Pulpit, power, and predation: "Yahoo men of God," prosperity theology, and the twin fraud triangles. *Critical Research on Religion,* 1–29. http://eprints.lse.ac.uk/id/eprint/128929

Lazarus, S., Tickner, P., & McGuire, M. R. (2025). Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal, 38,* 42. https://doi.org/10.1057/s41284-025-00482-4

Lee, R. M. (1993). *Doing research on sensitive topics.* Sage.

Leukfeldt, E. R., & Holt, T. J. (2019). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology, 64*(5), 522–538. https://doi.org/10.1177/0306624X19895886

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39–53. https://doi.org/10.1007/s10611-016-9663-1

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21–37. https://doi.org/10.1007/s10611-016-9662-2

Levi, M. (2022). Lawyers as money laundering enablers? An evolving and contentious relationship. *Global Crime, 23*(2), 126–147. https://doi.org/10.1080/17440572.2022.2089122

Lusthaus, J., Holt, T. J., Levi, M., Kleemans, E., & Leukfeldt, E. R. (2025). The evolution of Nigerian cybercrime: Two case studies of UK-based offender networks. *European Journal of Criminology, 22*(4), 557–577. https://doi.org/10.1177/14773708251329695

Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime, 27,* 364–387. https://doi.org/10.1007/s12117-022-09476-9

Martin, J., Whelan, C., & Bright, D. (2024). Ransomware HR: Human resources practices and organizational support in the Conti ransomware group. *Deviant Behavior,* 1–16. https://doi.org/10.1080/01639625.2024.2419905

Matza, D., & Sykes, G. M. (1961). Juvenile delinquency and subterranean values. *American Sociological Review, 26*(5), 712–719. https://doi.org/10.2307/2090200

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672–682. https://doi.org/10.2307/2084686

Mulcahy, L. (2010). *Legal architecture: Justice, due process and the place of law.* Routledge.

Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime & Justice, 44*(4), 419–440. https://doi.org/10.1080/0735648X.2020.1818605

Obioma, I. F., Hentschel, T., & Hernandez Bark, A. S. (2022). Gender stereotypes and self-characterizations in Germany and Nigeria: A cross-cultural comparison. *Journal of Applied Social Psychology, 52*(8), 764–780. https://doi.org/10.1111/jasp.12801

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria. *Cyber Criminology, 13*(2), 309–325.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the Yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology, 6*(2), 1001–1013.

Onanuga, P. A. (2020). When hip-hop meets CMC: Digital discourse in Nigerian hip-hop. *Continuum, 34*(4), 590–600. https://doi.org/10.1080/10304312.2020.1757038

Ononokpono, D. N., Ugwu, N. H., & Odimegwu, O. C. (2025). Household status and socio-economic determinants of divorce among married women in Nigeria: A pooled data analysis. *Cogent Social Sciences, 11*(1). https://doi.org/10.1080/23311886.2025.2536189

Orhero, M. I., & Nwoke, C. (2025). Theorizing the hypeman in Nigerian popular culture: Poetics, performance, and the e-fraud economy. *Canadian Journal of African Studies / Revue canadienne des études africaines,* 1–20. https://doi.org/10.1080/00083968.2025.2462217

Parti, K., & Dearden, T. E. (2024). *Cybercrime and strain theory: An examination of online crime and gender.* https://hdl.handle.net/10919/121133

Parti, K., Tahir, F., & Teaster, P. B. (2025). The wisdom of the scammed: Redefining older fraud victim support by utilizing the ecological systems framework. *Security Journal, 38,* 49. https://doi.org/10.1057/s41284-025-00487-z

Paternoster, C., Nazzari, M., Jofre, M., & Uberti, T. E. (2025). Inside the leak: Exploring the structure of the Conti ransomware group. *Global Crime,* 1–24. https://doi.org/10.1080/17440572.2025.2473350

Platt, J. (1981). Evidence and proof in documentary research: Some specific problems of documentary research. *Sociological Review, 29*(1), 31–52. https://doi.org/10.1111/j.1467-954X.1981.tb03021.x

PM News. (2024, April 20). Proprietor of Uyo Internet fraud school 'Hustle Kingdom' jailed 10 years. https://pmnewsnigeria.com/2024/04/20/proprietor-of-uyo-internet-fraud-school-hustle-kingdom-jailed-10-years

Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: Wherein lies the rule of law? *International Review of Law, Computers & Technology, 35*(2), 131–161. https://doi.org/10.1080/13600869.2021.1885105

Scott, J. (2014). *A matter of record: Documentary sources in social research.* John Wiley & Sons.

Shepherd, D., & Button, M. (2019). Organizational inhibitions to addressing occupational fraud: A theory of differential rationalization. *Deviant Behavior, 40*(8), 971–991. https://doi.org/10.1080/01639625.2018.1453009

Smith, D. J. (2017). *To be a man is not a one-day job: Masculinity, money, and intimacy in Nigeria.* University of Chicago Press.

Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies, 37*(4), 328–351. https://doi.org/10.1080/1478601X.2024.2429088

Soares, A. B., Lazarus, S., & Button, M. (2025). Love, lies, and larceny: One hundred convicted case files of cybercriminals with eighty involving online romance fraud. *Deviant Behavior,* 1–24. https://doi.org/10.1080/01639625.2025.2482824

Steinmetz, K. F., Holt, T. J., & Holt, K. M. (2019). Decoding the binary: Reconsidering the hacker subculture through a gendered lens. *Deviant Behavior, 41*(8), 936–948. https://doi.org/10.1080/01639625.2019.1596460

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of criminology.* Altamira Press.

Udoh, O. D., Folarin, S. F., & Isumonah, V. A. (2020). The influence of religion and culture on women's rights to property in Nigeria. *Cogent Arts & Humanities, 7*(1). https://doi.org/10.1080/23311983.2020.1750244

Ugwudike, P., Lavorgna, A., & Tartari, M. (2023). Sharenting in digital society: Exploring the prospects of an emerging moral panic. *Deviant Behavior, 45*(4), 503–520. https://doi.org/10.1080/01639625.2023.2254446

Uroko, F. C., & Obiorah, M. J. (2025). Fraud and cybercrime against older adults in Christian-dominated Southern Nigeria. *Security Journal, 38,* 45. https://doi.org/10.1057/s41284-025-00481-5

Valimail. (2023). *BEC scams cost companies $50 billion in losses.* https://www.valimail.com/blog/bec-scams-cost-companies-50-billion-in-losses/

Wang, P., Su, M., & 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. https://doi.org/10.1093/bjc/azaa064

West, C., & Zimmerman, D. H. (1987). Doing gender. *Gender & Society, 1*(2), 125–151. https://doi.org/10.1177/0891243287001002002

Whittaker, J. M., McGuire, M. R., & Lazarus, S. (2025). Conversations with deviant website developers: A case study of online shopping fraud enablers. *Journal of Criminology.* https://doi.org/10.1177/26338076251321844

Wilson, N. C., & Seigfried-Spellar, K. C. (2022). Cybervictimization, social, and financial strains influence Internet trolling behaviors: A General Strain Theory perspective. *Social Science Computer Review, 41*(3), 967–982. https://doi.org/10.1177/08944393211065868

Yushawu, A., & Jaishankar, K. (2025). Sakawa in Ghana: The influence of weak ties on economic cybercrime offender networks. *Deviant Behavior,* 1–21. https://doi.org/10.1080/01639625.2025.2459681