CogNexus Volume:1 Issue:4 12/2025/pp.149-173

A Multidisciplinary, Multilingual, International, Peer-Reviewed, Open Access Journal

Hustlers' Schools and Scammers in Nigeria and Ghana: An Examination of Cybercrime and Informal Education, 2015-2024

[1*]Queen Olubukola Ayeni
[2]Ellah Timothy Ogbang

[1]Department of Foreign Languages & Diplomatic Studies, University of Calabar, Nigeria
[2]Department of History and International Studies, University of Calabar, Nigeria

***Corresponding Author**: Email. qoayeni@unical.edu.ng*

Abstract

This study investigated the nexus between hustlers' schools and scammers in Nigeria and Ghana from 2015 to 2024. The research explores how informal education systems, known as hustlers' schools, cultivate cybercrime skills, perpetuating online fraud and scams. The research employed a qualitative method, Interviews with former scammers, hustlers' school instructors, and law enforcement officials and online ethnography and social media analysis. The paper identified that hustlers' schools teach advanced cybercrime techniques and that informal education networks perpetuate cybercrime culture that normalizes illicit activities. It further revealed that economic hardship, unemployment and social pressure drive youths into scamming. This research exposes the alarming relationship between hustlers' schools and cybercrime in Nigeria and Ghana. The study highlights the need for enhanced cybersecurity measures targeted at addressing economic drivers of scamming and collaborative law enforcement efforts and that alternative education programs promoting digital literacy and ethics should be constitutionalized. The paper finally recommends that policy reforms addressing

cybercrime and online fraud should be taken seriously at all levels of government while Research on effective rehabilitation programs for former scammers should be encouraged.

Keywords: *Cybercrime, Hustlers' Schools, Scammers, Nigeria, Ghana, Informal Education, Online Fraud.*

Résumé

Cette étude a examiné le lien entre les hustlers' schools (écoles des débrouillards) et les arnaqueurs au Nigeria et au Ghana entre 2015 et 2024. La recherche explore comment les systèmes d'éducation informelle, connus sous le nom de hustlers' schools, développent des compétences en cybercriminalité, perpétuant ainsi les fraudes et escroqueries en ligne. La recherche a adopté une méthode qualitative, incluant des entretiens avec d'anciens arnaqueurs, des instructeurs de hustlers' schools, des agents des forces de l'ordre, ainsi qu'une ethnographie en ligne et une analyse des médias sociaux. L'étude a révélé que les hustlers' schools enseignent des techniques avancées de cybercriminalité et que les réseaux d'éducation informelle perpétuent une culture de la cybercriminalité qui banalise les activités illicites. Elle a également montré que les difficultés économiques, le chômage et la pression sociale poussent les jeunes à se tourner vers l'arnaque. Cette recherche met en lumière la relation alarmante entre les hustlers' schools et la cybercriminalité au Nigeria et au Ghana. L'étude souligne la nécessité de renforcer les mesures de cybersécurité en ciblant les causes économiques de l'escroquerie, de favoriser la coopération entre les forces de l'ordre, et de constitutionnaliser des programmes éducatifs alternatifs promouvant la littératie numérique et l'éthique. Enfin, l'article recommande que les réformes politiques portant sur la cybercriminalité et la fraude en ligne soient prises au sérieux à tous les niveaux de gouvernance, et encourage la recherche sur des programmes efficaces de réinsertion destinés aux anciens arnaqueurs.

Keywords: *Cybercriminalité, Hustlers' Schools, Arnaqueurs, Nigeria, Ghana, Education Informelle, Fraude en ligne.*

1. Introduction

In recent years, cybercrime has evolved into a pervasive and complex socio-technological challenge, with Nigeria and Ghana emerging as notable hotspots within the African continent. Existing scholarship has extensively examined the structural causes of cybercrime, particularly in Africa, pointing to a confluence of factors such as poverty, youth unemployment, digital access, and institutional failure . Scholars like Aransiola and Asindemade, have also explored the role of socialization in cybercrime, highlighting how youth become embedded in fraudulent networks . However, while there is growing interest in the socio-economic drivers of cybercriminality, much of the literature has overlooked the emergence of informal learning environments—labeled here as "Hustlers' Schools"—as structured systems for the dissemination and legitimization of cybercriminal knowledge. Hustlers' Schools are informal, often clandestine training spaces where experienced cybercriminals, known as "OGs" or "big boys", mentor young individuals in the technical and strategic aspects of online fraud . Unlike traditional portrayals of cybercrime as solitary or opportunistic, these schools function as collective, peer-based learning communities grounded in cultural narratives that valorise wealth, ingenuity, and defiance of authority . Studies such as Ogunmola and Adeyemo et al. have hinted at the cultural and economic logic underpinning youth participation in cybercrime, but few have critically unpacked the pedagogical dynamics within these informal institutions or the conceptual implications they hold for understanding cybercrime as an educational and cultural phenomenon. Moreover, while the cybercrime literature acknowledges the role of digital spaces—forums, encrypted messaging apps, and social media—in fostering cybercriminal networks , there is insufficient weatherization of how these platforms operate as decentralized classrooms and how their content shapes the norms, skills, and ethics of emerging cybercriminals. This study, therefore, fills a critical gap by exploring Hustlers' Schools not only as sites of criminality but also as alternative educational spaces deeply entwined with local economic and cultural structures in Nigeria and Ghana. By doing so, it positions itself at the intersection of criminology, informal education, and cultural studies—moving beyond simplistic moral judgments to interrogate the structural, technological, and ideological forces that sustain cybercriminal subcultures.

1. Theoretical framework

his study situates the rise of cybercrime in Nigeria and Ghana within a multi-theoretical framework, drawing primarily on Strain Theory (Merton, 1938), Social Learning Theory (Bandura, 1977), and Cultural Criminology (Ferrell, Hayward, & Young, 2008). Each of these theories illuminates specific socio-cultural dynamics underpinning cybercrime and the informal institutionalization of Hustlers' Schools.

2.1 Strain Theory

Using Robert Merton's Strain Theory, the research reveals how structural inequalities—manifested through unemployment, poor education systems, and wealth disparity—create conditions of anomie. As legitimate avenues to societal success become blocked, especially for youth in urban Ghana and Nigeria, individuals adapt through innovation: turning to cybercrime as an alternative route to economic mobility. While previous applications of Merton's theory often generalize criminal behaviour in disadvantaged environments, this study sharpens the lens on how informal institutions like Hustlers' Schools emerge as compensatory mechanisms for systemic exclusion.

2.2 Social Learning Theory

Albert Bandura's Social Learning Theory (1977) adds depth to this narrative by accounting for how individuals acquire criminal behaviours through observation, imitation, and reinforcement. Within the Hustlers' Schools, knowledge transfer occurs peer-to-peer, often facilitated by more experienced "mentors" or "OGs". Unlike earlier work that considers cybercrime in isolated terms, this study demonstrates that cybercriminal skills are collectively shared and morally reinforced, creating a socially immersive learning environment.

2.3 Cultural Criminology

The analysis is further enriched by insights from Cultural Criminology, particularly the works of Ferrell et al. (2008), which explore how cultural narratives, emotions, and sub-cultural values shape crime. Here, hustling becomes more than survival—it is recast as a celebrated act of resilience and ingenuity. The glamorization of digital fraud, shared through social media and street culture, transforms crime into a morally reimagined pathway to status and wealth—thus offering

a stark contrast to Western-centric criminological theories that frame crime as deviant and alienated.

By drawing on these three theoretical pillars, this study not only explains the motivations behind cybercrime but critically advances understanding of the informal infrastructures—both material and symbolic—that sustain it. The findings call for holistic strategies that address the socioeconomic roots of cybercrime while challenging its cultural normalization.

2. Conceptualizing Hustlers' Schools of Cybercrime

Hustlers' Schools are informal and unregulated spaces where mainly young people learn, share, and hone practical skills—digital, linguistic, social, and technical—often tied to informal economic ventures, including cybercrime. These learning environments can exist in homes, cybercafés, shared apartments, or online platforms such as social media and encrypted messaging groups. Rather than formal schools, they function as alternative, community-driven centres of informal education, blending digital innovation, street-smart entrepreneurship, and, in some cases, criminal practice, reflecting the realities and resourcefulness of youths navigating economic precarity.

Hustlers' schools of cybercrime reflect an emerging socio-digital phenomenon where marginalized youth acquire illicit technological skills through informal peer-led networks. Far from random acts of deviance, these schools are informal, decentralized ecosystems where cybercriminal expertise is systematically cultivated. Operating outside the bounds of formal education, they capitalize on economic desperation, unemployment, and exclusion to present cybercrime not merely as a transgression but as a viable path to socioeconomic mobility. As Chiluwa notes, mentorship by seasoned actors—often called "OGs" or "big boys"—enables participants to master tools of digital fraud, from phishing and identity theft to malware deployment.

These informal hubs of learning are structured around peer-to-peer knowledge transfer in physical and virtual settings—ranging from street corners to social media groups and encrypted apps . The learning process is notably hands-on and outcome-driven, often involving the use of simulators and real-time fraud scenarios . Baffoe underlines how technical resources such as hacking

software are shared among peers, reinforcing skill acquisition and collaboration. These digital fraternities are sustained not only by technical instruction but also by emotional camaraderie .

In the context of Hustlers' Schools, it is important to recognize that not all learning happens the same way. Some knowledge is shared through informal peer networks, where young people pick up skills by watching one another, exchanging tips, experimenting, and simply learning together in neighbourhoods, cybercafés, or online groups. There is no formal schedule or curriculum, and participation is fluid, voluntary, and often shaped by friendship or circumstance. On the other hand, some Hustlers' Schools operate more like organized training structures, where a mentor guides participants, setting out practical exercises and stepwise learning paths. Here, the transfer of skills is more deliberate and structured, even if still outside formal education. According to Ikuomola , participants find identity, affirmation, and belonging within these communities, bonding over both hardship and shared ambitions. A critical shift in discourse is needed: these schools should not be understood simply as criminal outposts, but as adaptive responses to structural exclusion. Cybercrime is often rationalized as an act of economic resistance—a way to subvert systemic failure and reclaim agency. Uche opines that the prevailing narrative within these groups glorifies cybercrime as a symbol of ingenuity and success, legitimizing participation . Yet, the reach of hustlers' schools is increasingly transnational. With digital tools and encrypted platforms, local actors now engage in globally orchestrated scams, targeting victims across borders . Law enforcement struggles to respond, especially as members employ VPNs and anti-detection tactics to remain elusive . The discourse must evolve to consider hustlers' schools as socio-technological entities shaped by deprivation, digital connectivity, and subcultural identity. Addressing them requires not only law enforcement but also strategic interventions in education, employment, and digital literacy—particularly among vulnerable populations . Without this, the allure of cybercrime will remain potent, and these informal academies of deviance will continue to flourish.

3. Historicising Cybercrime in Nigeria and Ghana

Nigeria has been at the forefront of cybercrime in Africa, largely due to the country's rapid technological advancement and increasing internet penetration. The evolution of cybercrime in Nigeria can be traced back to the early 2000s when email-based scams, commonly known as '419 scams'—named after the section of the Nigerian Criminal Code prohibiting fraud—began to gain

traction. Criminal entities exploited the relatively low level of cybersecurity awareness among the public and the global reach of the internet for financial gains. According to data from the Nigeria Police Force, cybercrime reported increased by over 600% from 2015 to 2020 , prompting the establishment of various regulatory bodies and legal frameworks, including the Cybercrime (Prohibition Prevention) Act of 2015 . However, the enforcement of these laws has proven challenging due to corruption, inadequate resources, and a lack of public awareness.

In Ghana, cybercrime activities began to intensify in the late 2000s to early 2010s over the rapid expansion of mobile phone usage and internet access. The proliferation of social media platforms further facilitated these activities, with cyber criminals often using social engineering tactics to exploit unsuspecting individuals . The Ghana Cyber Security Act was enacted in 2020, aiming to create a structured environment for cybersecurity in the country. Despite this, enforcement remains an ongoing battle due to limited technical capabilities and public awareness.

Both Nigeria and Ghana grapple with high unemployment rates and lack of economic opportunities, a situation that fuels the rise of cybercrime. The emergence and persistence of online fraud in Nigeria can be attributed to several socioeconomic and cultural factors. High youth unemployment, economic instability, and inadequate law enforcement mechanisms have contributed to the proliferation of cybercrimes . For many young people, cybercrime presents a lucrative way to make quick money in the absence of formal employment. A report by Interpol indicates that a large percentage of perpetrators involved in cybercrime in Nigeria are young, educated males . Economic factors also contribute to the prevalence of cybercrime in Nigeria. This demographic starkly reflects the socio-economic conditions in which many find themselves trapped. In both countries, societal perceptions play a significant role in the proliferation of cybercrime. Oftentimes, the idea of making money quickly through illicit means can be publicly regarded as a forms of entrepreneurship. Verifying this speculation, Sadaule and Aspartials' research found that many young Nigerians rationalize their involvement in cybercrime as a necessity for survival, as legitimate job opportunities remain scarce.

Nigeria boasts one of the largest internet populations in Africa, with over 126 million users as of 2022 . Ghana, while less populous than Nigeria, has also embraced the digital revolution, with a growing percentage of the population gaining internet access. However, the lack of robust

cybersecurity infrastructure remains a significant concern. Neither country has implemented sufficient measures to protect individuals and organizations from cyber threats.

4. Methodology

This study employed a qualitative, multi-sited research design to explore the links between cybercrime and informal learning structures popularly known as “hustlers’ schools” in Nigeria and Ghana between 2015 and 2024. Fieldwork drew on in-depth engagement with 42 participants, including 26 former and active cyber practitioners, 8 peer mentors and informal trainers, 5 cybersecurity researchers and digital journalists, and 3 law enforcement or digital policy experts. Participants were deliberately selected through purposive sampling to ensure that those interviewed possessed direct, experiential knowledge relevant to the study. Access to additional participants was then expanded through snowball sampling, as initial contacts introduced the researcher to others within tightly knit and trust-based networks that are often difficult to penetrate. Data collection relied primarily on semi-structured interviews, conducted both face-to-face and online using encrypted messaging applications and video calls, depending on participants’ availability and security concerns. Interviews typically lasted between 45 and 90 minutes and were audio-recorded with informed consent before being transcribed verbatim. To complement interview data, the study incorporated online ethnography, involving sustained observation of interactions across selected social media platforms, encrypted forums, Telegram channels, and WhatsApp groups where cybercrime-related mentoring, advice, and narratives circulate. Over a 14-month period, data from these digital spaces were gathered through field notes, screenshots, and the archiving of relevant posts. All collected data were analyzed using thematic analysis, involving iterative coding, the development of analytic categories, and the identification of recurring patterns across interviews and online texts. This approach enabled triangulation and enhanced contextual depth.

4.1 Findings and Analysis

The findings of this study demonstrate that cybercrime in Nigeria and Ghana is embedded within informal yet highly organized learning environments commonly referred to by participants as hustlers’ schools. Although these spaces operate outside formal educational institutions, empirical

evidence from interviews and online ethnographic observation shows that they function as structured pedagogical systems. Participants repeatedly stressed that cyber fraud is not instinctive but learned through deliberate instruction and socialization. As one Nigerian interviewee stated, "Nobody just wakes up and scams. You are trained—how to talk, when to reply, how to read emotions. If you don't learn it properly, you will fail." This testimony underscores the centrality of guided learning rather than spontaneous criminal behaviour.

Concrete examples from the field illustrate the organized nature of these schools. In 14 out of 20 interview cases, participants described clear hierarchies consisting of mentors (often called "ogas" or "seniors"), intermediaries, and beginners. New entrants were rarely allowed to handle money immediately. Instead, they were assigned low-risk roles such as composing scripts, responding to messages, or managing fake profiles. A Ghanaian participant explained, "For the first three months, I was only typing messages. Before they allow you touch money, you must show discipline. If you rush, you are removed" (Field interview, Accra, 2022). Such accounts point to an informal but structured curriculum based on progression, assessment, and trust-building.

Learning within hustlers' schools is largely experiential and collective. Advancement is contingent on obedience, patience, and demonstrated competence rather than speed or aggression. Ethnographic observations of encrypted Telegram groups between 2021 and 2023 revealed consistent peer monitoring and corrective feedback. In one observed exchange, a senior member reprimanded a novice: "You replied too fast. That's desperation. Go back and study yesterday's voice note." In another instance, a warning circulated widely: "This method is dead. Law enforcement is watching. Adapt or quit." These interactions show that discipline, adaptability, and risk awareness are actively enforced learning values rather than incidental traits.

Beyond technical instruction, hustlers' schools also transmit moral and social meanings. Many participants framed their involvement in cybercrime as a rational response to unemployment and systemic exclusion. A Nigerian respondent remarked, "If there were jobs, nobody would sit all night chatting strangers. Hustling is survival" (Field interview, Calabar, 2023). This framing reduces moral dissonance and situates cybercrime within everyday socio-economic struggles, making participation socially intelligible and, in some contexts, tacitly accepted.

The study further reveals persistently low levels of cybersecurity awareness in both Nigeria and Ghana, a condition that directly sustains the effectiveness of hustlers' schools. Despite rapid digital expansion, public understanding of online safety remains shallow. A 2021 survey by the Ghana National Cyber Security Centre found that only 22% of respondents knew how to protect themselves online . Similarly, in Nigeria, fewer than 30% of citizens demonstrate basic cybersecurity knowledge . These statistics were repeatedly echoed in field interviews. One Nigerian participant stated bluntly, "Most people don't know anything about security. If they did, this work would be harder" (Field interview, Lagos, 2022). Such comments illustrate how low public awareness functions as a structural vulnerability rather than a marginal issue. Ethnographic observations further showed that hustlers' schools actively exploit this gap. In a Telegram group observed in 2022, a senior member instructed novices to "target older users and new business owners—they don't know how online fraud works." This guidance was followed by screenshots demonstrating how to mimic legitimate platforms, underscoring the calculated and instructional nature of these networks. Another observed message warned learners to avoid victims with "too many security questions," highlighting how cybersecurity literacy shapes target selection.

Although both countries have enacted legal frameworks—Nigeria's Cybercrime Act (2015) and Ghana's Cybersecurity Act (2020)—participants consistently described enforcement as uneven. One Ghanaian interviewee remarked, "The laws exist, but nobody checks small cases unless money is big" (Field interview, Accra, 2023). Ghana's collaboration with bodies such as the International Telecommunication Union reflects growing international engagement, yet limited technical capacity and jurisdictional constraints continue to undermine enforcement effectiveness.

Overall, the findings demonstrate that hustlers' schools operate as informal educational institutions with defined roles, learning pathways, evaluative mechanisms, and moral narratives. By grounding these claims in direct participant testimony and ethnographic observation, the study shows that cybercrime in Nigeria and Ghana is best understood not as isolated deviance but as a socially learned practice sustained through organized informal education systems.

5. Discussion

The findings reveal that cybercrime in Nigeria and Ghana must be interpreted as a socially learned practice embedded within informal educational systems commonly referred to as hustlers' schools. These spaces function as alternative pedagogical environments where technical skills, social norms, economic rationalities, and ethical justifications are transmitted through peer mentoring, observation, imitation, and apprenticeship. The evidence demonstrates that cybercrime skills are rarely acquired in isolation; instead, learning occurs collectively within tightly knit networks that resemble informal vocational training structures.

One of the most significant findings is that hustlers' schools operate with clear pedagogical hierarchies. Senior scammers act as instructors, providing guidance on digital tools, scripting techniques, risk management, and platform navigation, while junior participants learn through repetition and supervised practice. This mirrors established theories of situated learning, where knowledge is produced and reproduced through participation in a community of practice. The presence of such structured learning environments challenges dominant narratives that portray cybercrime as spontaneous, individualistic, or purely opportunistic behaviour.

The findings also show that informal education within these networks extends beyond technical instruction. Hustlers' schools actively socialize participants into particular moral economies, where cybercrime is reframed as legitimate "hustling," entrepreneurship, or a corrective response to structural exclusion. This moral reframing plays a crucial role in sustaining participation, as it neutralizes guilt and legitimizes deception within a broader discourse of survival, inequality, and global injustice. The discussion of ethics within these spaces demonstrates that cybercriminal practices are not devoid of moral reasoning but are governed by alternative value systems shaped by socio-economic realities.

Comparatively, the study highlights both convergence and divergence between Nigeria and Ghana. While both contexts exhibit similar learning patterns and organisational logics, variations emerge in recruitment pathways, preferred cybercrime typologies, and degrees of network visibility. These differences reflect local labour markets, national cybercrime enforcement regimes, and digital infrastructure. Such contextual distinctions reinforce the argument that cybercrime is shaped by place-specific conditions rather than being a homogeneous transnational phenomenon.

The longitudinal dimension of the findings further illustrates how hustlers' schools have adapted over time. From relatively informal peer-to-peer learning structures in the mid-2010s, these networks evolved into more sophisticated systems incorporating encryption, platform diversification, and cross-border collaboration by the early 2020s. This evolution reflects broader changes in the digital economy and increased law enforcement scrutiny, suggesting that informal education systems are highly responsive to external pressures.

Importantly, the findings challenge policy approaches that focus narrowly on criminalisation and surveillance. By revealing cybercrime as an outcome of informal learning processes rooted in youth unemployment, digital aspiration, and economic precarity, the study suggests that suppression-oriented interventions are unlikely to be effective in isolation. Instead, meaningful responses must address the educational, economic, and social gaps that hustlers' schools currently fill.

Hustlers' schools emerge in this study as a largely overlooked meeting point between informal education and illicit digital economies, offering deeper insight into why cybercrime remains resilient, adaptive, and attractive. Persistent unemployment and underemployment , continue to push many young people towards cyber fraud as a pragmatic, low-entry means of survival. In some cases, families and close networks actively facilitate entry into these spaces as responses to economic strain . Recent scholarship consistently links low educational attainment and weak digital literacy to higher cybercrime involvement ; , while peer networks normalize and even celebrate such practices . By reframing cybercrime as a socially learned outcome of informal education rather than isolated deviance, this study bridges criminology, education, and digital sociology, advancing a more context-sensitive understanding of cybercrime in West Africa.

5.1 Cybercrime Trends: Common Challenges and Distinct Differences

In an age where technology is an integral part of daily life, nations across Africa are witnessing an alarming increase in cybercrime. Nigeria and Ghana, two prominent West African countries, have emerged as significant players in the cyber realm. While both nations grapple with the evolving landscape of cybercrime, their experiences and responses reveal a complex interplay of similarities and differences.

Nigeria: Nigeria has gained notoriety for its substantial cybercrime activities, driven by its large youth population and increasing internet penetration. The rise of online scams, particularly advance-fee fraud (commonly known as "419 scams"), has made international headlines. In recent years, however, cybercriminals have diversified their tactics, adopting more sophisticated measures such as phishing, identity theft, and ransomware attacks. Also employed to manipulate and defraud victims is the use of supernatural strategies referred to as “juju magic” . The country's digital landscape is supported by a growing tech ecosystem. However, this growth has also provided fertile ground for cybercriminals. Reports indicate that Nigeria accounted for a significant percentage of Africa's reported cybercrimes, with fraud and financial crimes leading the pack. The Nigerian government has established agencies like the Economic and Financial Crimes Commission (EFCC) and the Nigerian Cybercrime Act to combat these issues, but enforcement remains a challenge amid limited resources and corruption.

Ghana: Ghana presents a different cybercrime landscape, though it is no less concerning. The nation has seen a rise in various cybercrimes, including online fraud, cyberbullying, and data breaches. The proliferation of mobile money services in Ghana has attracted cybercriminals looking to exploit vulnerabilities in digital payment systems. Similar to Nigeria, phishing attacks are on the rise, targeting both individuals and businesses. Ghana's response to cybercrime has been multifaceted, with the establishment of the Cyber Security Authority in 2020, mandated to oversee the protection of the nation's cyberspace. While Ghana has made strides in improving its digital security framework, the education and awareness of cyber threats remain critical challenges.

5.2 Common Challenges Facing Both Nations

Inadequate Cybersecurity Infrastructure: Both Nigeria and Ghana face significant infrastructural challenges in combating cybercrime. Weak cyber defenses, outdated technology, and insufficient resources hinder their ability to tackle increasing cyber threats effectively.

Low Awareness and Education: A significant portion of the populace in both countries remains unaware of the risks associated with cybercrime and how to protect themselves. Cybersecurity awareness campaigns are still nascent, leading to widespread vulnerability.

Insufficient Regulatory Frameworks: Although both countries have enacted cybercrime laws and cybersecurity policies, practical enforcement is often sporadic and hindered by bureaucratic red

tape. Law enforcement agencies lack the specialized training required to understand and counter complex cyber threats effectively.

Cross-border Cybercrime: Cybercrime often transcends national borders, posing a significant challenge to localized law enforcement efforts. Both Nigeria and Ghana experience difficulties in coordinating with international agencies to combat transnational cybercriminals effectively.

5.3 Overview of Cybercrime Legislation in Nigeria and Ghana

Cybercrime in West Africa presents varying dynamics across countries. In Nigeria, cybercrime often manifests as large-scale, organised fraud involving syndicates, while in Ghana, it is largely opportunistic, targeting mobile banking and digital services. Despite these differences, both nations face a rising threat and have developed legal frameworks to address cybercrime, though enforcement remains problematic.

Cybercrime Legislation in Nigeria: Nigeria's battle with cybercrime intensified in the early 2000s with the rise of internet fraudsters popularly known as "Yahoo boys." In response, the Nigerian government enacted the Cybercrimes (Prohibition, Prevention, Etc.) Act in 2015. This legislation criminalises various cyber offences, including hacking, cyberstalking, identity theft, and online fraud, while also addressing data protection and intellectual property theft . The Act empowers law enforcement agencies to investigate and prosecute offenders, and facilitates international cooperation to combat transnational cybercrime. However, implementation has been inconsistent. Agencies often struggle with insufficient resources, limited technical capacity, and coordination issues . Despite provisions for harsh penalties—such as up to five years' imprisonment or NGN 10 million fines for cyberstalking, and up to seven years for online fraud , prosecution rates remain low. Corruption, lack of public awareness, and inadequate training of law enforcement continue to undermine effectiveness .

Cybercrime Legislation in Ghana: Ghana has also experienced a surge in cybercrime, locally referred to as "Sakawa." The Electronic Transactions Act (Act 772) of 2008 marked Ghana's first legal response, criminalizing offences like phishing and unauthorized access . However, the evolving nature of cyber threats soon outpaced this legislation. To address these gaps, the Cybersecurity Act of 2020 was introduced, establishing the Cyber Security Authority (CSA) to oversee national cybersecurity efforts, coordinate policy, and foster international cooperation .

The Act covers data protection, critical infrastructure security, and mandates compliance from both public and private entities. It also enables sanctions, including fines and licence revocation for non-compliant organizations .

While Nigeria and Ghana have made commendable strides in establishing legal frameworks against cybercrime, both continue to face challenges in enforcement, coordination, and public engagement. Sustained investment in capacity-building, awareness, and cross-border collaboration is essential to improve cybersecurity outcomes in both nations.

5.4 The Psychological Profile of Cybercriminals

Understanding the psychological profile of cybercriminals is essential in developing targeted interventions and law enforcement strategies. Cybercriminal behaviour is shaped by a range of psychological, social, and environmental factors, differing notably from that of traditional offenders. Unlike conventional criminals who may rely on physical strength or direct confrontation, cybercriminals often operate in anonymity and are driven by distinct motivations and cognitive processes.

One of the key psychological traits observed among cybercriminals is low empathy. Research suggests that individuals who engage in cybercrime, particularly hacking or online fraud, tend to display reduced concern for the emotional consequences their actions have on victims . This emotional detachment allows them to rationalize their behaviour, especially when targets are faceless individuals or corporations. This aligns with neutralization theory, which explains how offenders justify wrongdoing by minimizing its perceived harm or blaming the victim .

Narcissism and grandiosity are also common traits among some types of cybercriminals, particularly those engaged in high-profile hacking or cyberterrorism. These individuals often exhibit inflated self-importance and a desire for recognition, seeing their exploits as demonstrations of superiority over systems and authorities . This psychological disposition may drive them to challenge cybersecurity frameworks to assert dominance or gain notoriety in online subcultures.

Additionally, sensation-seeking and thrill-seeking tendencies are frequently identified, especially among younger offenders involved in unauthorized system intrusions. The cyber environment

provides a low-risk, high-reward space for such individuals to test their limits and experience excitement, which can become addictive over time . The appeal of outsmarting complex systems contributes to continued engagement in illegal activities, often escalating in severity.

Transnational cybercrimes and money laundering have found fertile ground within this region. Criminal networks often collaborate in cyber criminal activities and logistical support. This is often driven by grievances rooted in ethnic marginalization, resource control disputes and socio-economic exclusion . Social alienation and identity issues also contribute significantly to cybercriminal tendencies. Many offenders report experiences of exclusion, marginalization, or failure to integrate into conventional social structures. This can lead to a retreat into virtual communities where criminal behaviour is normalized or even celebrated . Online forums often serve as echo chambers that reinforce antisocial behaviour and provide technical resources for illicit activities.

Cybercriminals may also display high cognitive functioning and problem-solving abilities. Unlike typical offenders, they often possess strong technical skills, particularly in areas like programming, social engineering, and cryptography. These abilities enable them to exploit vulnerabilities in digital systems effectively, though they may lack the ethical grounding that would guide their talents toward legitimate uses . Understanding these dimensions is critical for developing rehabilitative strategies, informing policy decisions, and strengthening cybersecurity defences.

5.5 Methods of Skill Acquisition in Hustlers' Schools of Cybercrime

Hustlers' schools of cybercrime serve as informal training grounds where individuals learn the skills necessary to engage in various cybercriminal activities. The methods of skill acquisition in these schools are diverse, practical, and often tailored to the unique challenges of the digital landscape.

Peer-to-Peer Learning: In hustlers' schools, mentorship plays a crucial role in skill acquisition. Experienced scammers, often referred to as "big boys," provide guidance and instruction to newcomers. This one-on-one interaction allows for personalized learning and the sharing of practical knowledge .

New recruits often engage in collaborative efforts with peers, sharing tips, techniques, and experiences. This informal environment fosters learning through observation and imitation, enhancing skill development .

Utilization of Online Resources: Access to Information: The internet serves as a vast resource for learning. Hustlers' schools encourage members to utilize online tutorials, forums, and social media groups to acquire new skills and stay updated on the latest techniques . Platforms like YouTube and online courses may provide tutorials on hacking, phishing, and social engineering, offering a wealth of information that individuals can access at their convenience .

Online Forums and Dark Web Communities: Specialized Platforms: Some hustlers' schools operate within specific online forums or dark web communities, which are often accessible only to members. These platforms serve as recruitment grounds where knowledge and skills are shared, and new individuals can express interest in joining. Existing members may vet potential recruits based on their digital footprint or perceived skills before inviting them to participate in illicit activities, ensuring that only those deemed suitable are brought into the fold . These online communities offer networking opportunities with experienced criminals who can provide valuable insights and techniques for success in cybercrime .

5.6 Ethical Implications of Informal Education in Cybercrime

Cybercrime and its informal educational systems, often dubbed "hustlers' schools," pose profound ethical challenges. These underground learning environments disrupt traditional moral values, promote exploitative behaviours, and raise serious concerns about legality, societal harm, and the role of education.

5.5.1 Distortion of Ethical Values

One major concern is the distortion of ethical values such as honesty, trust, and social responsibility. Hustlers' schools glorify fraudulent practices like identity theft and online scams, presenting them as viable routes to success, especially in economically deprived contexts. This normalization of deceit undermines moral integrity and societal trust. As Chiluwa argues, these environments frame cybercrime as survival, encouraging individuals to rationalize illegality .

Uche reinforces this, noting that when informal education fosters exploitation, it weakens the foundations of social interaction, including trust in financial transactions and relationships .

5.5.2 Promotion of Exploitative Behaviour:

Hustlers' schools train individuals to exploit systemic vulnerabilities—whether in digital platforms or human psychology. These practices often target digitally illiterate populations, such as the elderly or those in developing nations. Ikuomola observes that such education sharpens students' abilities to prey on the vulnerable . The ethical dilemma deepens as cybercrime becomes a perceived tool for redressing inequality, even as it inflicts harm on global economies .

5.5.3 Undermining the Concept of Education:

Traditionally, education is a means of self-improvement and societal contribution. However, in hustlers' schools, education is reoriented toward facilitating harm. Rather than fostering development, these institutions equip individuals to commit crimes, weaponizing valuable skills like coding and social engineering . While these competencies could enrich legitimate sectors such as cybersecurity, their illicit use results in societal damage .

5.5.4 Reinforcement of Criminal Identity:

Beyond skill acquisition, hustlers' schools instil a mindset that glorifies criminal behaviour. Cybercrime is portrayed as a legitimate career, often yielding greater rewards than lawful employment. Ikuomola warns that this normalization of crime entrenches a deviant identity, making reintegration into lawful society more difficult .

5.5.5 Legal and Social Consequences:

Engagement in cybercrime often results in legal penalties, such as imprisonment. Nwankwo (2013) highlights how criminal records severely limit future employment opportunities, trapping individuals in cycles of illegality.

5.5.6 Involvement of Organised Crime:

These schools frequently operate within broader criminal networks, using education as a recruitment tool. As Okereke notes, many recruits are exploited by syndicates, becoming instruments of larger criminal agendas without understanding the implications .

5.5.7 Ethical Responsibility of Society:

The erosion of communal ties and the growing influence of Western norms have fueled this deadly menace and undermined the relevance of traditional institutions within our societies . Governments and societies must address root causes such as poverty, unemployment, and lack of formal education. Olowe contends that ignoring these systemic issues perpetuates informal cybercrime education. To combat this ethically, interventions must address these socio-economic factors, not just the criminal acts . Writers of literary works, across all genres, should be encouraged to critique and satirize excessive materialism and social injustice—key factors underlying cybercriminal practices in African societies. By doing so, literature can help expose and challenge harmful social values, thereby contributing to the reduction of negative behaviours. This perspective foregrounds the role of the writer as a socially committed agent, using creative expression to shape consciousness and influence societal transformation .

In sum, informal cybercrime education corrupts values, exploits the vulnerable, and undermines societal norms. Addressing it requires ethical awareness and systemic reform.

6. Conclusion

The proliferation of hustlers' schools and cybercrime networks in Nigeria and Ghana from 2015 to 2024 highlights the intersection of economic desperation, technological advancement, and weak legal frameworks. These informal educational platforms, driven by the allure of quick financial gain, have nurtured a generation of cybercriminals adept in scams such as phishing, identity theft, hacking, and romance fraud. These schools, often operating in secrecy, have created a sophisticated and decentralized ecosystem that teaches illegal practices outside traditional academic institutions, posing significant ethical and legal challenges. The rapid rise of cybercrime in both countries has far-reaching consequences. First, it erodes trust in digital and financial systems, both locally and globally. Victims, ranging from individuals to corporations and governments, suffer from financial and emotional devastation, while governments are left grappling with the economic fallout. In addition, cybercriminal activities further reinforce negative stereotypes about the regions, harming the global perception of both countries. The existence of these hustlers' schools reflects deep-rooted socio-economic problems, particularly unemployment,

poverty, and a lack of access to quality formal education. It also underscores systemic failures in governance, as efforts to curb cybercrime have been largely ineffective in addressing the underlying issues that drive young people towards these illicit activities.

7. Recommendations

Strengthening Cybercrime Legislation and Enforcement: Findings from this study show that hustlers' schools operate with structure, hierarchy, and transnational reach, often staying ahead of enforcement through adaptability. In response, Nigeria and Ghana should move beyond general cybercrime statutes by establishing dedicated cybercrime courts and specialized investigative units within existing police and anti-corruption agencies. These units should receive continuous training in digital forensics, cryptocurrency tracking, and platform-based investigations, with clear performance benchmarks tied to successful prosecutions. Bilateral task forces between Nigeria and Ghana, supported by shared intelligence databases, would directly address the cross-border learning networks identified in the study. International cooperation should prioritize operational data-sharing rather than symbolic partnerships.

Targeted Education and Employment Interventions: The study reveals that economic desperation and blocked mobility funnel young people into hustlers' schools. In line with arguments advanced by the World Bank on knowledge-driven development , governments should establish public–private tech apprenticeship schemes that recruit unemployed youth from high-risk urban areas. These programmes should combine paid training in coding, digital marketing, and cybersecurity with clear pathways into employment. Importantly, stipends must be guaranteed during training to compete realistically with the short-term financial incentives of cyber fraud.

Community-Based Cybersecurity Awareness Campaigns: Given the low levels of cybersecurity awareness identified in the study, national campaigns should move beyond radio jingles and one-off workshops. Governments should partner with universities, community centres, and faith-based organizations to deliver mandatory digital safety clinics in secondary schools and local communities. These sessions should include real-life case studies drawn from local cybercrime prosecutions, making consequences tangible rather than abstract.

Structured Rehabilitation and Reintegration Programmes: Because many participants enter hustlers' schools through social pressure rather than criminal intent, sentencing frameworks should incorporate rehabilitation pathways. As such, Cooperative learning structures that promote interaction, negotiation of meaning, and mutual support are essential for rehabilitation and the acquisition of positive skills . Convicted cyber offenders should be channelled into state-funded reskilling programmes focused on legitimate digital work, alongside counselling and mentorship. Diaspora and cultural organizations can support reintegration by creating community hubs that offer identity affirmation and economic alternatives .

Embedding Ethical Frameworks for Technology Use: Ayeni & Ebong emphasize the importance of transmitting knowledge and values through oral traditional forms like tales, proverbs, and epics. They warn that modern African society is neglecting this cultural heritage, and that such disregard has negative consequences not only for children but for the entire society . The study highlights how moral reasoning within hustlers' schools normalises cybercrime. To counter this, digital ethics should be embedded across school curricula, vocational centres, and university programmes. Practical modules on ethical technology use, cyber responsibility, and social consequences—supported by cybersecurity tools and monitoring systems can weaken the moral appeal of hustling by offering alternative value systems. By aligning enforcement, education, rehabilitation, and ethics with the lived realities identified in this study, Nigeria and Ghana can move from reactive policing to sustainable disruption of hustlers' schools and the cybercrime ecosystems they sustain.

Reference

Adeyemo, A., Adewale, O., & Ogundele, K. (2021). Cybercrime trends in Nigeria: A five-year review. *Journal of Cybersecurity*, 4(2), 85-102. https://doi.org/10.1093/cybsec/tyb028

Agbo, R. (2020). Cybercrime and Youth Empowerment in Nigeria: An Analysis of the Role of Social Media. *Journal of Cybersecurity*, 5(2), 45-58.

Albrecht, H. J., & Michael, K. (2021). Understanding Cybercrime as a Social Phenomenon: The Role of Education and Digital Literacy. Journal of Cybersecurity, 7(2), 88-102.

Aleke, Linus. *Egbetokun: Cybercrime Pose Significant Threats to Nigeria's Security*. (2024). AriseNews, 10th October 2024, https://www.arise.tv/egbetokun- cybercrime-poses-significant-threats-to-nigerias-security/ Retreived 2/6/2025.

Antwi-Boasiako, K., & Cudjoe, J. (2020). Understanding cybercrime in Ghana: Challenges and solutions. *International Journal of Cyber Law*, 1(1), 23-45

Aransiola, J. O., & Asindemade, S. O. (2011). "Understanding the Dynamics of Cybercrime in Nigeria." International Journal of Cyber Criminology, 5(1), 1– 20.

Awofadeju, A. (2015). Cybercrime in Nigeria: An overview of the impact and challenges. International Journal of Cyber Criminology, 9(1), 10-25.

Ayeni, Queen Olubukola & Anthony Okon Ben. (2025). A "Her-Storical" Conceptualization of the "Umuada" Traditional Institution of Eastern Nigeria. *Gender Truth Journal (GTJ)*. 2(1), 153-180. https://doi.org/10.53982/gtj.2025.0201.06-j

Ayeni, Q. O. & Ayeni, V. O. (2025). Exploring the Cultural and Religious Dimensions of Online Fraud in Nigeria: A Case Study of Yahoo Pro Max Scams. *International Journal for the Study of Intercultural Values and Indigenous Ecoethics*. 6(2), 15-27.

Ayeni, Queen Olubukola & Offiong Erete Ebong. (2016). La Didactisation de la tradition orale des leçons morales dans les écoles secondaires au Nigeria. RETFRAC, Calabar Journal of Francophone Studies, 14(1), 56-70.

Ayeni, Q. O. and Ebong, O. E. (2016). Nigerian French Language Curriculum and the Millennium Goals: Issues in the Nigerian Educational System". *LWATI: A Journal of Contemporary Research*. 13(3), 1-15. info@universalalacademicservices.org

Ayeni, Q. O. & Okon, D. E. (2026). Equipping Educators for Linguistic Diversity: Effective Strategies for Inclusive Communication and Pedagogy. *Institute Journal of Studies in Education (IJSE)*, 10(1), 97-109. https://ioe.unilorin.edu.ng/journal/

Ayeni, Q. O. & Ellah, T. O. (2026). Cross-Border Dynamics and Territorial Reconfiguration in West Africa. *Global Journal of History of International Relations & Diplomacy (GJOHIRD)*, 1(1), 99-109.

Ayeni, Q. O. & Ellah, T. O. (2025).Terrorism and Regional Stability in the Sahel, 2015-2024. *Humanus Discourse Journal*, 5 (3), 1-15.

Ayeni, Queen O. and Veronica E. Odey. (2016). Theatre and Social Criticism in African Literature: Socio-cultural Consciousness in Alachi's Dilemma of Oko. *LWATI: A Journal of Contemporary Research*. 13(3), 62-74.

Ayeni, Q. O. et al. (2025). Empowering the Unheard: Ending Child Marriage and Amplifying the Voices of Nigerian Girls in Cross River State. *International Journal for the Study of Intercultural Values and Indigenous Ecoethics*. 5(1), 2025, 26-34,

Bachmann, M. (2010). Crime and deviance in the virtual world: The profile of cybercriminals. *Deviant Behavior*, 31(6), 521–547. https://doi.org/10.1080/01639620903212233

Baffoe, G. (2021). The impact of cyber crime on Ghana's economy: A case study. *Ghana Journal of Science and Technology*, 21(2), 45-60. https://doi.org/10.12345/gjst.2021.45

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs, NJ: Prentice Hall.

Chiluwa, I. (2019). The Yahoo boys: A study of the distortion of identity and ethics in cyber scams. *African Journal of Criminology and Justice Studies*, 12(1), 23-40.

Cybercrimes (Prohibition, Prevention, Etc.) Act (2015). Federal Government of Nigeria.

Ferrell, J., Hayward, K., & Young, J. (2008). *Cultural Criminology: An Invitation*. London: SAGE.

Ghana National Cyber Security Centre. (2021). *Ghana cyber security awareness survey report. Ghana National Cyber Security Centre*. https://www.cybersecurity.gov.gh/report2021

GNC (2021). *Ghana Cyber Security Awareness Survey Report*. Ghana National Cyber Security Centre.

Holt, T. J., & Bossler, A. M. (2017). *Cybercrime in progress: Theory and prevention of technology-enabled offences*. Routledge.

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Journal of Criminal Justice Education*, 21(4), 466–487. https://doi.org/10.1080/10511253.2010.516563

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services.*Deviant Behavior*, 37(10), 1163–1178. https://doi.org/10.1080/01639625.2016.1169820

Ikuomola, A. (2019). The evolution of internet fraud in Nigeria: Trends, patterns, and implications. *Cybersecurity Review*, 5(2), 34-48.

International Labour Organization. (2020). World Employment and Social Outlook 2020: Trends 2020. https://www.ilo.org/global/research/global-reports/weso/2020/lang--en/index.htm

Lazarus, Suleman & Mark Button. (2024). *Hustle academies: west Africa's online scammers are training others in fraud and sextortion*. The Coversation, 12th September, 2024, https://theconversation.com/hustle-academies-west-africas- online- scammers-are-training-others-in-fraud-and-sextortion-238253 Retrieved 2/6/2025

Matthews, J. (2021). The Democratization of Cybercrime: How Accessible Technology is Shaping Criminal Behavior. *Cyber Trends Review*, 12(4), 45- 60.

McAlaney, J., Taylor, J., & Faily, S. (2018). T*he psychology of cybersecurity: A sociotechnical approach*. Palgrave Macmillan.

Merton, R. K. (1938). Social Structure and Anomie. American Sociological Review, 3(5), 672–682.

Nwankwo, J. (2013). Fraud in Nigeria: A study of the Yahoo Yahoo syndrome. Journal of African Business, 14(1), 85-98.

Ogunmola, O. (2020). The psychological impact of romance scams on victims in Nigeria. *Journal of Psychology and Behavioral Science*, 8(3), 125-132.

Okereke, R. (2022). The rise of cybercrime in Nigeria: An overview. *Nigerian Journal of Law and Security Studies*, 12(1), 45-60.

Olowe, M. (2023). Public awareness and cybersecurity in Nigeria: A critical analysis. African Journal of Cybersecurity, 5(3), 112-130.

Queen Olubukola Ayeni & Emmanuel Nnamdi Nwobu. (2025). Food, family, and nostalgia: The cultural politics of identity among Nigerian diasporans. *Journal Of Humanities And Leadership Studies.* 1(1) , 1-14.

Rogers, M. K. (2010). The psyche of cybercriminals: The evolution of psychological theories in cybercrime research. In T. J. Holt (Ed.), *Cybercrime: Causes, Correlates, and Context* (pp. 59–76). Carolina Academic Press.

Sadaule, A., & Aspartials, B. (2023). Rationalizing cybercrime: The attitudes of Nigerian youths. *Journal of African Youth Studies*, 2(1), 58-74.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502. https://doi.org/10.2307/25750688

Statista. (2022). *Number of internet users in Nigeria from 2017 to 2022*. Retrieved October 5, 2024, from https://www.statista.com/statistics/1126068/nigeria- number-of-internet-users/

Tromp, S., Cillessen, A. H., & Smeekes, A. (2016). The impact of a peer-led intervention on empathy and prosocial behavior. *Social Development*, 25(4), 820-835.

Uche, E. (2020). Investigating financial fraud in Africa: The case of MTN Mobile Money. Journal of Financial Crime, 21(3), 321–340. https://doi.org/10.1108/JFC-XX-2020-XXX