JOURNAL OF HUMANITIES AND LEADERSHIP STUDIES: JOURNAL OF FACULTY OF ARTS, DENNIS OSADEBAY UNIVERSITY, ASABA, DELTA STATE
Volume 1, Number 1, August, 2025, ISSN: 2971-5741

CULTURAL NARRATIVES AND CYBERCRIME: EXPLORING THE SOCIO-CULTURAL FACTORS INFLUENCING NIGERIAN YOUTH'S INVOLVEMENT IN CYBERCRIME

Ogbemudia Mari JAMES
Department of Mass Communication, Ambrose Alli University, Ekpoma,
Edo State, Nigeria,
marijames2020@aauekpoma.edu.ng

Abstract
Cybercrime, defined as criminal activity conducted through the internet, computers, or other digital platforms, has become a pressing concern in Nigeria. Manifesting in diverse forms such as hacking, fraud, identity theft, phishing, and malicious communication, it poses severe threats to national security, economic growth, and social cohesion. The involvement of Nigerian youths in cybercrime has drawn the attention of policymakers, law enforcement agencies, and other stakeholders. Yet, empirical studies examining the socio-cultural drivers of this menace remain limited. This study explores how cultural norms, values, and beliefs intersect with technological advancements to influence youths' involvement in cybercrime. Guided by Social Learning Theory (SLT) and Cultural Criminology Theory (CCT), the research adopts a mixed-methods approach, combining survey data from Nigerian youths with interviews involving parents and cybercrime experts. The study ultimately aims to generate context-sensitive strategies for preventing and mitigating cybercrime, offering valuable insights for policymakers and stakeholders committed to advancing cybersecurity and digital safety in Nigeria.

Keywords: Nigerian youths, cybercrime, socio-cultural factors, cybersecurity, digital safety.

Introduction

The advent of the internet and digital technologies has reshaped global interaction, communication, and commerce. While this digital revolution has yielded numerous benefits, it has also fostered the rise of cybercrime, a phenomenon now recognized as a major global security and social challenge. Cybercrime, broadly defined as any criminal activity involving the use of the internet, computers, or digital platforms, is increasingly pervasive in Nigeria, with far-reaching consequences for national security, economic progress, and social stability (UNODC, 2021).

In recent years, Nigeria has experienced a troubling surge in cybercrime, ranging from fraud and phishing to identity theft, hacking, and other malicious online practices. Nigerian youths have emerged as the primary perpetrators of these crimes (Ojedokun & Eraye, 2012). Factors such as anonymity, ease of access, and the seeming low risk of detection have made cybercrime an appealing avenue for many young people. The persistence of weak cybersecurity legislation,

limited law enforcement capacity, and widespread digital illiteracy further exacerbates the problem.

Despite the growing attention cybercrime attracts in policy and media discourse, scholarly work has largely centered on its technical and economic dimensions, with comparatively little emphasis on the socio-cultural dynamics shaping its prevalence. Research that interrogates the cultural, moral, and social contexts of cybercrime in Nigeria remains scarce. This study seeks to address this gap by investigating how socio-cultural narratives—including norms, values, and beliefs—interact with technological opportunities to influence Nigerian youths' engagement in cybercrime. By situating the analysis within Social Learning Theory and Cultural Criminology Theory, the research offers a culturally informed perspective that goes beyond technical explanations. Ultimately, this study contributes to a more nuanced understanding of cybercrime in Nigeria and develops culturally responsive strategies for prevention and mitigation. Its findings will be useful to policymakers, law enforcement agencies, and stakeholders committed to strengthening digital safety and fostering social integrity in Nigeria.

Cybercrime Conceptualized

Cybercrime refers to any criminal activity that involves the use of computers, computer networks, or other digital technologies to commit or facilitate a crime (Brenner, 2008). This broad definition encompasses a wide range of activities, including hacking, phishing, identity theft, online fraud, and cyberstalking, among other forms of cybercrimes.

According to Ibikunle and Eweniyi (2013), as cited in Edoghogho & Obiakor (2024), various internet platforms facilitate the commission of cybercrimes, which occur daily in diverse forms. These forms include fraudulent emails, pornography, identity theft, hacking, cyber harassment, ATM spoofing, piracy, phishing, and romantic scams, among other illicit activities.

The concept of cybercrime is multi-faceted and complex. It has been defined and understood in various ways by scholars, policymakers, and law enforcement agencies. One of the earliest and most influential definitions of cybercrime is the one provided by the United States Department of Justice, which defined it as "any illegal activity that involves the use of computers or other digital technologies" (U.S. Department of Justice, 1999). This definition highlights the key role that technology plays in the commission of cybercrimes, emphasizing the importance of considering the technical aspects of cybercrime to prevent or combat it.

The perpetration of cybercrime is a nefarious activity undertaken by individuals or organizations with malicious intent. Cybercrime, according to Ebeleogu, Ojo, Adeh, and Agu (2019), can be conceptualized as a criminal offense that leverages digital technologies to facilitate the commission of a crime, with a primary focus on computing and communication technologies.

This phenomenon is perpetrated mainly by youths who seek to exploit the ease and anonymity of digital platforms to defraud individuals and organizations, thereby facilitating a more convenient means of earning a living.

Explicating cybercrime, Ibikunle and Eweniyi (2013) posit that it constitutes a series of organized crimes that target both cyberspace and cybersecurity, highlighting the complex and multi-faceted nature of this issue. The proliferation of cybercrime has become a pressing concern in Nigeria and worldwide, as many cybercriminal activities are perpetrated from remote locations, making it challenging for security agencies to track and apprehend the perpetrators. The absence of contemporary laws and regulations governing cybercrime in Nigeria further worsened the situation, creating a void in the legal framework that hinders the effective prosecution of these crimes.

Cybercrime, according to Bosser, Adam, Berenblum, and Tamer (2019). It is a computer-oriented crime that involves the use of a computer and a network, where the computer may be utilized as a tool to commit a crime or as a target of the crime itself. This perspective underscores the integral role of technology in the perpetration of cybercrime. Aghatise (2006) provides a more nuanced definition, characterizing cybercrime as a crime committed on the internet using a computer as either a tool or a target victim. He identifies four distinct categories of cybercrime victims, namely the gullible, the desperados, the inexperienced, and the unlucky individuals.

Furthermore, cybercrime can be conceptualized as a type of criminal activity that either targets or utilizes a computer, a computer network, or a networked device. This definition highlights the adaptability and evolution of cybercrime, as perpetrators continually exploit emerging technologies and vulnerabilities to commit crimes. The dynamic nature of cybercrime necessitates a proactive and multi-faceted approach to mitigation, incorporating legislative, technological, and societal measures to combat this menace effectively.

From a criminological perspective, cybercrime can be seen as a type of white-collar crime, characterized by its non-violent and financially motivated nature (Friedrichs, 2009). Cybercrimes often involve the use of sophisticated technologies and techniques to commit crimes such as identity theft, online fraud, and embezzlement. Individuals or groups can commit these crimes, and they can have significant financial and emotional consequences for victims.

The concept of cybercrime has also been influenced by the idea of “cyberspace" as a distinct social and cultural space (Wall, 2007). This perspective highlights the significance of considering the social and cultural contexts in which cybercrimes occur. It also highlights the need to understand how technology is shaping and being shaped by social and cultural forces. From this perspective, cybercrime is not just a technical issue; it is also a social and cultural one, and requires a comprehensive approach that takes into account the complex interplay between technology, society, and culture.

In recent years, the concept of cybercrime has expanded to include a range of new and emerging threats, including cyberterrorism, cyberwarfare, and cyberespionage (Andress & Winterfeld, 2011). These threats involve the use of digital technologies to commit acts of terrorism, warfare, or espionage, posing significant challenges to national security and global stability.

Cybercrime, according to Oumarou (2017), has become so prevalent in Africa that it has been labeled colloquially in different countries. For instance, in Nigeria, it is referred to as "Yahoo Yahoo," with perpetrators being called "Yahoo Boys". Similarly, in Ghana, cybercrime is known as "Sakawa" or "Yahoo Yahoo." At the same time, in Cameroon, it is referred to as "Faymania. Most cybercriminals in Nigeria are youth who are university undergraduates. The term Yahoo Boys" specifically denotes youths engaged in cybercrime through the use of deceptive electronic emails, typically via platforms such as Hotmail, Gmail, and Yahoo Mail. This colloquialism originated from the modus operandi employed by these individuals in perpetrating online fraud.

Socio-Cultural Factors Influencing Nigerian Youth's Involvement in Cybercrime

Efforts to combat cybercrime in Nigeria may be compromised by the country's prevailing socio-cultural norms, prioritizing wealth accumulation and material possessions over integrity and dignity. A pervasive emphasis on materialism has supplanted the cultural values of honesty, morality, and ethics. Consequently, the sources of individuals' wealth are no longer subject to scrutiny, and those who have acquired wealth through illicit means, including cybercrime, are often celebrated and legitimized within society. This phenomenon is evident even within religious institutions, where these individuals are frequently accorded privileged status and treatment. This cultural landscape presents a significant challenge to efforts to curb cybercrime in Nigeria.

The proliferation of cybercrime is encouraged by a convergence of various societal factors, including the erosion of moral standards, the decline of traditional values, and a diminished emphasis on the importance of hard work and formal education. Furthermore, the prevalence of ritual killings and other forms of illicit activities has contributed to a cultural landscape that fosters and enables cybercriminal behaviour. These societal shifts have created an environment in which cybercrime can thrive, underscoring the need for a comprehensive approach that addresses these underlying factors to mitigate the threat of cybercrime effectively.

Nigeria's cultural milieu plays a significant role in the propagation of cybercrime. The country's cultural values and norms profoundly influence individual behaviour, encouraging engagement in cybercrime. Specifically, the cultural emphasis on material prosperity and social standing can motivate some individuals to pursue cybercrime in an attempt to attain these aspirations (Awoyemi, Omotayo, & Mpapalik, 2021). Furthermore, the pervasive "get rich quick" mentality can also contribute to the appeal of cybercrime, as some individuals may perceive it as a quick means to acquire wealth and status.

The ostentatious display of wealth during social ceremonies in Nigeria can have a profound impact on the youth, potentially driving them to engage in cybercrime. The spectacle of extravagant spending can foster a sense of financial insecurity and inadequacy among young individuals, who may feel pressured to acquire wealth and status through illicit means.

Furthermore, peer influence plays a significant role in perpetuating this phenomenon. The visibility of peers driving luxury vehicles can create a sense of competition and aspiration, leading some individuals to feel compelled to acquire similar status symbols. This unnecessary rivalry can result in a sense of relative deprivation, where individuals feel motivated to engage in cybercrime as a means to bridge the perceived economic gap between themselves and their peers.

Additionally, the decline in moral values in society has led to the rising incidence of cybercrime in Nigeria (Okpako, 2020). In this context, the pressure to belong to a specific social class or group can lead to a decline in moral values among young people, as they strive to emulate their peers and achieve a higher socio-economic status. This phenomenon is often characterized by a desire to achieve financial success, regardless of the means, with the notion that "the ends justify the means." The influence of negative role models, coupled with poor parental guidance, can further exacerbate this trend.

Some parents, driven by a desire for financial security, may encourage their children to prioritize wealth accumulation over moral integrity, thereby inadvertently promoting a culture of corruption and cybercrime. The pervasive nature of corruption in Nigerian society has created an environment in which cybercriminals can operate with relative impunity, with some security personnel even serving as accomplices or bodyguards for these individuals.

Also, the intersection of cultural dynamics and globalization has been identified as a contributing factor to the proliferation of cybercrime in Nigeria (Abokwara, 2021). As the country has become increasingly integrated into the global economy, novel forms of criminal activity have emerged, while traditional forms of crime have evolved and adapted to new modalities. Furthermore, the cultural exchange facilitated by globalization can introduce new values and norms that influence an individual's propensity to engage in cybercrime, underscoring the complex interplay between cultural, economic, and technological factors in shaping the trajectory of cybercrime in Nigeria.

As the country's social fabric continues to evolve, it is essential to understand how cultural factors are influencing the rise of cybercrime. These include examining the role of social influence, particularly among young people, in the prevention and perpetuation of cybercrime (Alabi, Bamidele, Abdulrasheed & Bashir: 2023). By recognizing the complex relationship between culture and cybercrime, we can develop more effective strategies to prevent and combat cybercrime in Nigeria.

The socio-cultural life of a country is very important, and once it is eroded, it will have a spill-over effect on other areas. This is why cybercrime is likely to continue thriving in Nigeria, despite the government's efforts to curb it.

It is pertinent to note that many scholars have mainly focused on the economic aspects of the impact of cybercrime, with little emphasis on the socio-cultural factors that promote cybercrime. This study seeks to fill this gap by examining the socio-cultural factors that influence youth involvement in cybercrime.

Cybercrime Categorized

The proliferation of cybercrime has led to a concomitant expansion of its scope and complexity, resulting in a multi-faceted menace that continues to evolve and adapt. A taxonomy of cybercrime reveals three primary categories, each with distinct characteristics and motivations. These categories, according to the National Institute of Justice (2020), are:

1. **Individual-based cybercrime:** This type of cybercrime is mainly perpetrated by solitary hackers or cybercriminals who engage in illicit activities for personal gain or to garner notoriety. This category encompasses a wide range of cybercrimes, including identity theft, phishing, and malware distribution, which are often committed by individuals seeking financial rewards or to satisfy their ego.

2. **Organization-based cybercrime**: This category involves organized groups of cybercriminals who collaborate to commit crimes for financial gain or to further their organization's objectives. These groups often employ sophisticated tactics and techniques to compromise computer systems, steal sensitive information, or disrupt critical infrastructure. Organization-based cybercrime can include activities such as corporate espionage, ransomware attacks, and online fraud.

3. **Nation-state-based cybercrime:** This type of cybercrime is perpetrated by nation-states or governments that engage in cybercrimes for political, economic, or strategic gain. Nation-state-based cybercrime can include activities such as cyber espionage, cyber warfare, and cyberterrorism, which are often designed to compromise national security, disrupt critical infrastructure, or influence political outcomes.

The above categorization of cybercrime can further be subdivided into several distinct categories, including:

i. **Financial Criminals or Fraudsters:** This type of cybercrime encompasses a range of activities, including phishing, scams, and social engineering, which are designed to deceive and defraud victims, often for financial gain. Phishing, in particular, involves the use of malicious emails, attachments, or URLs to gain unauthorized access to a victim's account or computer. This may include links to fake online banking or other websites, which are used to steal private account

information. Scams, on the other hand, typically take the form of ads or spam emails that promise rewards or money but are ultimately designed to deceive and exploit victims.

ii. Internet Scams: These scams often involve enticing offers that appear "too good to be true" and, when clicked on, can cause malware to interfere with and compromise sensitive information. Internet scams can take many forms, including fake online auctions, phishing emails, and social engineering tactics.

iii. **Social Engineering:** This method is used by cybercriminals to trick people into revealing their personal information through lies and manipulation. Social engineering tactics often involve convincing fake stories or scenarios that are designed to lure victims into a trap. This can include pretexting, baiting, quid pro quo, and other tactics that are designed to exploit human psychology and manipulate individuals into divulging sensitive information.

These categories are not mutually exclusive, and cybercrimes can often involve elements of multiple categories. For instance, an individual hacker may be recruited by an organized group or a nation-state to commit a cybercrime. Moreover, a phishing email may use social engineering tactics to trick a victim into revealing their login credentials, which can then be used to commit financial fraud.

Understanding these categories and the tactics used by cybercriminals to commit these crimes is essential to develop effective strategies to prevent, detect, and respond to cybercrimes, as well as to promote international cooperation and information sharing to combat this global menace.

Theoretical Framework

The theories adopted for this study are Social Learning Theory (SLT) and Cultural Criminology Theory (CCT). These theories are discussed below in the context of cybercrime.

The Social Learning Theory (SLT)

The Social Learning Theory (SLT), officially propounded in 1977 by Albert Bandura, posits that individuals learn new behaviors by observing and imitating others, emphasizing the role of social context and cognitive processes in acquiring new behaviours and knowledge. In the context of cybercrime, SLT suggests that Nigerian youths may learn cybercriminal behaviours by observing and imitating their peers or others in their social environment.

This theory posits that social learning occurs through interactions with others within a social context. People develop behaviours by observing and imitating others, particularly when their observations are positively reinforced or rewarded. Through this process of observation,

assimilation, and imitation, people acquire new behaviours, which can ultimately become integrated into their own behavioral repertoire.

Within the realm of cybercrime, social learning theory suggests that individuals acquire deviant behaviours through direct or indirect observation of others who perpetrate such crimes. In the Nigerian context, youths may engage in cybercrime as a result of learning from the behaviours and lifestyles of others, potentially perpetuating a cycle of deviance. This phenomenon underscores the significance of social influence and observational learning in shaping the cybercriminal behaviours of Nigerian youth.

Cultural Criminology Theory (CCT)

Cultural Criminology Theory (CCT), propounded by Jeff Ferrell and Clinton Sanders in 1995, posits that cultural dynamics and meanings play a pivotal role in shaping criminal behaviour. Situated at the nexus of cultural studies and criminology, CCT contends that culture encompasses a collective way of life, replete with symbolism and meaning-making practices that influence individual and collective behaviour.

The theory investigates the intersections of culture, crime, and justice, with a particular focus on the stylized frameworks and experiential dynamics of illicit subcultures. Additionally, CCT examines the symbolic criminalization of popular culture forms, the mediated construction of crime and crime control issues, and the development of situated media and audiences for crime.

Recent expansions of CCT have explored the links between crime, crime control, and cultural space, as well as the collectively embodied emotions that shape the meaning of crime. In the context of cybercrime, cultural Criminology Theory offers a nuanced framework for understanding how Nigerian youths' cultural values, norms, and practices influence their involvement in cybercrime, highlighting the complex interplay between cultural dynamics and criminal behaviour.

Strategies for Curbing Cybercrime

To check the prevalence of cybercrime in Nigeria, one must first tackle the issues of corrupt practices, quick money syndrome, and high unemployment rates in Nigeria. In order to succeed in the fight against cybercrime, the government should embark on proper enlightenment campaigns by organizing regular seminars and workshops to teach citizens how to survive with or without a job, as well as how to use internet security codes to protect themselves from cybercriminals.

Enacting cyber security laws with steady follow-up is also crucial to monitor and prevent cybercrimes. Additionally, job creation is vital, and the government should create more job opportunities and encourage small-scale industries to operate by reducing tax rates and providing grants and loans.

Using firewalls can protect computer systems from unauthorized access, and an address verification system (AVS) can help prevent defrauding individuals by ensuring that the address entered on an order form matches the address where the cardholder's billing statement is mailed from.

Creating more skill acquisition centers in every local government development center can provide youth with the opportunity to learn a skill, which can go a long way in reducing cybercrime in Nigeria. Finally, proper implementation of cyber security laws requires employing experts in the field of cyber security to avoid poor internet working.

To effectively address the cultural factors contributing to cybercrime, it is essential to provide cultural sensitivity training for law enforcement and other stakeholders. This training should aim to educate them on the cultural nuances and values that may discourage individuals from engaging in cybercrime. It is also imperative to shift the cultural discourse and emphasize the importance of education, hard work, and legitimate means of achieving success. This can be achieved through various channels, including community outreach programmes, social media campaigns, and educational initiatives.

Conclusion

The concept of cybercrime is complex and multi-faceted, and it has been defined and understood in various ways by scholars, policymakers, and law enforcement agencies. As digital technology continues to evolve, the concept of cybercrime will likely continue to expand and adapt, and it will require a comprehensive approach that takes into account the technical, social, and cultural aspects of cybercrime.

The ranking of Nigeria as one of the most corrupt countries in the world until 1999, when the Economic and Financial Crime Commission (EFCC) and the Independent Corrupt Practices Commission (ICPC) were established, highlights the depth of corruption in the country. The fact that some security personnel are complicit in protecting cybercriminals rather than arresting and prosecuting them underscores the need for a comprehensive approach to addressing the root causes of cybercrime in Nigeria.

The interplay between poverty, corruption, and poor governance has created a fertile ground for cybercrime to thrive in Nigeria. Addressing these underlying factors is crucial to mitigating the incidences of cybercrime and promoting a culture of integrity and moral responsibility among young people. By providing access to quality education, economic opportunities, and social support, Nigeria can reduce the allure of cybercrime and promote a more secure and prosperous future for its citizens.

Recommendations

To effectively combat cybercrime in Nigeria, a multi-faceted approach is necessary. Firstly, the proper execution of cybersecurity laws by various levels of government is crucial in checking the activities of fraudsters and their agents. This can be achieved through the establishment of a robust legal framework that provides for the prosecution of cybercrimes, as well as the creation of specialized law enforcement units to handle cybercrime cases.

Furthermore, the government should establish seminars and skill acquisition centers to reduce the unemployment rate, which is a major driver of cybercrime. By providing individuals with the skills and knowledge needed to secure legitimate employment, the government can reduce the incentive for individuals to engage in cybercrime. Additionally, the government can provide grants and loans to individuals and small-scale industries to support their economic activities and direct their interests toward legitimate means of earning a living.

Individuals also have a critical role to play in preventing cybercrime. They should be cautious when interacting with suspected fraudsters and avoid responding to fake bank alerts or other suspicious messages. Moreover, individuals should maintain the privacy of their passwords and other sensitive information when using the internet. By taking these precautions, individuals can reduce their risk of falling victim to cybercrime.

Finally, religious leaders, including Christian clergy, Muslim scholars, and practitioners of African Traditional Religion, should consistently discourage their followers from engaging in unlawful means of acquiring wealth. By promoting a culture of honesty and integrity, religious leaders can help to discourage individuals from engaging in cybercrime and other forms of illicit activity. By working together, the government, individuals, and religious leaders can create a society that is less conducive to cybercrime and more supportive of legitimate economic activity.

References:

Abokwara, Edith. (2021). Changing Societal Culture and the Conundrum of Cybercrime in Nigeria. Asian Review of Social Sciences. 10. 10.51983/arss-2021.10.2.2827.

Aghatise, E. (2006). Cybercrime in Nigeria: Causes, effects, and remedies. Journal of Financial Crime, 13(2), 147-155.

Alabi, Abdullahi & Bamidele Ph.D., Abdulrasheed & Abdulrazaq, Bashir. (2023). Cybercrime in Nigeria: Social Influence Affecting the Prevention and Control. Vol 8. 2023.

Andress, J., & Winterfeld, S. (2011). Cyber warfare: Techniques, tactics and tools for security practitioners. Syngress.

Awoyemi, Bosede & Omotayo, Olufunmilola & Mpapalika, Jane. (2021). Forms and Effects of Cyber Crime in Nigeria. 7. 2454 - 6119.

Brenner, S. W. (2008). Cybercrime: Criminal threats in the information age. Praeger.

Bosser, A., Adam, M., Berenblum, T., & Tamer, S. (2019). Cybercrime: A review of the literature. *Journal of Cybersecurity*, 5(1), 1-15.

Ebeleogu, O., Ojo, A., Adeh, E., & Agu, C. (2019). Cybercrime in Nigeria: An examination of the causes and consequences. *Journal of Crime and Justice,* 42(1), 34-47.

Friedrichs, D. O. (2009) Trusted Criminals, 4th Edition. Belmont, CA: Cenage Learning.

Nmeme, E., & Obiakor, N. (2024). Unpacking the Impact of Cybercrimes and Socio-Cultural Dimensional Developments in Nigeria. *Journal of International Economic Relations and Development Economics*, *4*(1), 1-8. Retrieved from *https://www.theinterscholar.org/journals/index.php/jierade/article/view/236*

Ibikunle, F., & Eweniyi, O. (2013). Cybercrime and cybersecurity in Nigeria: An overview. *Journal of Cybersecurity*, 1(1), 1-10.

Oumarou, M. (2007). Brainstorming Advanced Fee Fraud: 'Faymania'—the Cameroonian Experience. In N. Ribadu, I. Lamorde and D. W. Tukura (Eds.). *Current Trends in Advance Fee Fraud in West Africa*, pp. 33–34. Nigeria: EFCC.

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