DEMOGRAPHIC SHIFTS AND CYBERCRIME IN NIGERIA

Anas Kabiru Hamza
Department of Sociology Federal University, Dutsin-Ma, Katsina State
Kanas440@yahoo.com

Bonzena Dauda Cletus
Department of Public Administration Taraba State Polytechnic, Suntai
bonzenadaudacletus@gmail.com

Francis Collins Somorija
Department of Sociology, Taraba State University, Jalingo
Collinsfrancis001@gmail.com

Abstract

Nigeria's demographic shifts, marked by a youthful population, rapid urbanization, and growing digital connectivity, are driving a significant rise in cybercrime, establishing the country as a key hub in sub-Saharan Africa. This systematic review examines the relationship between these demographic trends and cybercrime, focusing on financial fraud, identity theft, and ransomware. With a median age of 18.6 years and high youth unemployment, economic hardship pushes tech-savvy young individuals, often termed "Yahoo Boys," toward cyberfraud. Urban centers like Lagos offer anonymity and robust digital infrastructure, creating fertile ground for cybercriminal activities. Internet penetration, reaching over a third of the population, enhances digital inclusion but also expands opportunities for cyberattacks, worsened by inadequate cybersecurity measures and weak enforcement. Gender dynamics show male dominance in cybercrime, though female involvement, particularly in romance scams, is increasing. Rural-urban migration fuels cybercriminal networks by exploiting economic vulnerabilities and identity issues among migrants. Cybercrime inflicts substantial economic losses, with financial fraud being the most prevalent form. The review identifies a lack of research on victims, particularly vulnerable groups, and proposes targeted interventions, including job creation for youths, strengthened cybersecurity training, improved digital infrastructure, integration of ethics in education, and global cooperation to counter transnational cybercrime networks. Addressing these socio-economic and technological factors is essential to curbing cybercrime's impact on Nigeria's digital economy, national security, and international reputation.

Keywords: Cybercrime, Demographic shifts, Digital connectivity, Urbanization, and Youth bulge,

Introduction

Nigeria, Africa's most populous nation, is undergoing significant demographic shifts characterized by rapid population growth, urbanization, and an expanding youth population. With an estimated population exceeding 205 million and a median age of 18.6 years, the country boasts a vibrant, tech-savvy demographic increasingly integrated into the global digital economy (United Nations, 2023). The proliferation of internet access, with penetration rates reaching 33.6% in recent years, has transformed communication, commerce, and governance, fostering opportunities for innovation and economic growth (Maitanmi et al., 2024). However, this digital transformation has coincided with a surge in cybercrime, positioning Nigeria as a notable hub for cybercriminal activities in sub-Saharan Africa (Odunayo, 2024). Cybercrimes, encompassing phishing, identity theft, online fraud, and business email compromise, exploit

technological vulnerabilities and socio-economic challenges, costing Nigeria an estimated $800 million annually in 2018, with losses likely higher today (Maitanmi et al., 2024). Demographic factors, particularly the youth bulge and socio-economic disparities, are critical drivers of cybercrime in Nigeria. Studies indicate that young Nigerians, often referred to as "Yahoo Boys," engage in cyber fraud due to high unemployment rates, poverty, and peer influence (Bamidele, 2023; Odunayo, 2024). The rapid urbanization and migration to cities, where internet access is more prevalent, further amplify opportunities for cybercriminal activities (Ogunjobi, 2020). Concurrently, the lack of robust cyber security infrastructure and inadequate enforcement of cybercrime laws exacerbate the problem, leaving individuals, businesses, and institutions vulnerable (Tuleun, 2022).

The escalating prevalence of cybercrime in Nigeria poses a significant threat to its digital economy, national security, and international reputation. Despite legislative efforts, such as the Cybercrimes (Prohibition and Prevention) Act of 2015, amended in 2024, cybercrime rates continue to surge, particularly in social, financial, and educational sectors (Maitanmi et al., 2024). The Economic and Financial Crimes Commission (EFCC) reported over 3,000 convictions for cybercrime-related offenses in 2022, underscoring the scale of the issue (Tuleun, 2022). However, the relationship between demographic shifts such as the growing youth population, urbanization, and educational attainment—and cybercrime remains underexplored in contemporary literature. While studies have identified poverty and unemployment as key drivers, few have comprehensively examined how demographic trends, including age, gender, and regional disparities, influence cybercriminal behavior and victimization (Bamidele, 2023).

The problem is compounded by Nigeria's rapid digitalization, which, while fostering economic inclusion, has outpaced the development of cybersecurity measures and public awareness (Odunayo, 2024). Young Nigerians, who constitute the majority of internet users, are both perpetrators and victims of cybercrimes, driven by economic desperation and exposure to cybercriminal subcultures (Ogunjobi, 2020). Moreover, the lack of victim-focused research limits understanding of the human and economic toll of cybercrime, particularly among vulnerable demographics such as the elderly and rural populations (Maitanmi et al., 2024). This gap in knowledge hinders the formulation of targeted interventions to curb cybercrime and mitigate its socio-economic impacts. Therefore, this review aims to synthesize recent studies to elucidate the nexus between demographic shifts and cybercrime in Nigeria, identifying key drivers, impacts, and policy gaps to inform evidence-based strategies for cybersecurity resilience.

Conceptual Clarifications

Cybercrime

Cybercrime refers to illegal activities conducted through digital platforms, exploiting information and communication technologies to perpetrate offenses. In the Nigerian context, cybercrime encompasses a range of activities, including identity theft, financial fraud, and cyberterrorism. Identity theft involves the unauthorized acquisition and use of personal

information, such as names, bank details, or login credentials, to commit fraud or other crimes (Maitanmi et al., 2024). Financial fraud, a prevalent form of cybercrime in Nigeria, includes phishing scams, business email compromise, and online investment schemes, often targeting individuals and organizations for monetary gain (Odunayo, 2024). Cyberterrorism, though less common, involves the use of digital tools to disrupt critical infrastructure, spread propaganda, or incite fear, posing significant threats to national security (Tuleun, 2022). These activities exploit vulnerabilities in Nigeria's rapidly expanding digital ecosystem, driven by widespread internet access and limited cybersecurity infrastructure (Bamidele, 2023). The Economic and Financial Crimes Commission (EFCC) reported that financial fraud alone accounted for over 70% of cybercrime cases in Nigeria in 2022, underscoring its dominance within the cybercrime landscape (Tuleun, 2022).

Demographic Shifts

Demographic shifts refer to significant changes in the composition and characteristics of a population, influencing social, economic, and technological dynamics. In Nigeria, these shifts are characterized by urbanization, youth bulge, population growth, and digital literacy, each contributing to the cybercrime landscape. Urbanization reflects the increasing migration to urban centers, where access to internet infrastructure is more robust, facilitating both digital engagement and cybercriminal opportunities (Ogunjobi, 2020). Nigeria's urban population grew to 52% in 2022, with cities like Lagos and Abuja becoming hubs for cybercrime activities (United Nations, 2023). The youth bulge, defined as a disproportionately large population aged 15–29, constitutes over 60% of Nigeria's population and is a critical driver of cybercrime, as economic hardship and unemployment push young individuals toward illicit online activities (Bamidele, 2023). Population growth, with Nigeria's population projected to reach 263 million by 2030, amplifies pressure on resources and job markets, exacerbating socio-economic conditions conducive to cybercrime (United Nations, 2023). Digital literacy, while enabling participation in the digital economy, also equips individuals with the skills to engage in sophisticated cybercrimes, particularly among tech-savvy youths (Odunayo, 2024). These demographic trends, combined with socio-economic challenges, create a complex interplay that fuels the persistence and evolution of cybercrime in Nigeria.

Methodology

This study adopts a systematic literature review approach to examine the nexus between demographic shifts and cybercrime in Nigeria. Relevant peer-reviewed articles, reports, and statistical data from 2020 to 2025 were sourced from academic databases such as ResearchGate, SSRN, and Google Scholar, alongside reputable institutional publications from the United Nations and the Economic and Financial Crimes Commission (EFCC). The inclusion criteria focused on studies addressing demographic trends (youth bulge, urbanization, digital literacy, migration) and their relationship to cybercrime patterns (financial fraud, identity theft, ransomware) in Nigeria. A thematic analysis was employed to synthesize findings, categorizing data into demographic drivers, cybercrime trends, and socio-economic impacts. To ensure robustness, the review cross-referenced quantitative data, such as internet

penetration rates (33.6% in 2023) and youth unemployment figures (40.6% in 2023), with qualitative insights on cybercriminal motivations and victimization. Limitations include the potential underreporting of cybercrime incidents and the scarcity of victim-focused studies, which may constrain the depth of analysis on vulnerable demographics.

Discussion and Findings

a. **Demographic Shifts in Nigeria**

Nigeria, with a population surpassing 205 million, is experiencing transformative demographic shifts that are reshaping its socio-economic and technological landscapes, with significant implications for challenges such as cybercrime. These shifts, encompassing a youth population explosion, rapid urbanization, educational and unemployment challenges among youths, rising internet penetration, and rural-urban migration, create both opportunities and vulnerabilities in the nation's development trajectory (United Nations, 2023). Understanding these dynamics is essential for addressing their impacts, particularly in the context of Nigeria's growing cybercrime landscape. Nigeria's demographic profile is marked by a pronounced youth bulge, with a median age of 18.6 years, one of the youngest globally, and over 60% of the population aged 15–29 (United Nations, 2023; Bamidele, 2023). This youthful cohort holds immense potential for economic growth and innovation due to its energy and digital proficiency. However, high youth unemployment, estimated at 40.6% in 2023, coupled with widespread poverty, pushes many toward illicit activities, including cyberfraud, with groups like the "Yahoo Boys" exploiting digital platforms for financial gain (Odunayo, 2024; Maitanmi et al., 2024). The youth explosion thus presents a dual challenge, necessitating policies to harness its potential while addressing socio-economic drivers of cybercrime.

Urbanization is another defining trend, with 52% of Nigerians living in urban areas in 2022, a figure projected to reach 65% by 2050 (United Nations, 2023). Cities like Lagos, Abuja, and Port Harcourt are growing rapidly, offering better access to digital connectivity and fueling Nigeria's digital economy through e-commerce and fintech (Ogunjobi, 2020). However, urban centers also serve as hubs for cybercrime, as tech-savvy youths exploit robust digital networks amid economic disparities, highlighting the need for targeted cybersecurity interventions (Maitanmi et al., 2024).

Education, while expanding with over 2 million tertiary students by 2022, faces challenges in quality and employability, with many graduates equipped with digital skills but lacking job opportunities (Tuleun, 2022). This mismatch drives some youths toward cybercrime as an alternative income source, perceiving it as a viable response to unemployment (Bamidele, 2023; Odunayo, 2024). Meanwhile, internet penetration has surged to 33.6% in 2023, with over 70 million users, driven by affordable smartphones and mobile data (Maitanmi et al., 2024). While this fosters economic inclusion, it also exposes users to cyber risks like phishing and malware, exacerbated by limited cybersecurity awareness (Ogunjobi, 2020).

Rural-urban migration further intensifies demographic concentration in cities, with Lagos alone hosting over 15 million residents (United Nations, 2023). Migrants, particularly youths, face economic hardship in urban settings, increasing their vulnerability to cybercriminal networks

promising quick financial rewards (Bamidele, 2023). This migration, combined with enhanced digital access, creates fertile ground for cybercrime in urban hubs (Maitanmi et al., 2024). Collectively, these demographic shifts underscore the need for comprehensive strategies to leverage Nigeria's demographic potential while mitigating the socio-economic and technological vulnerabilities fueling cybercrime.

b. **Patterns and Trends of Cybercrime in Nigeria**

Nigeria has emerged as a significant hub for cybercrime in sub-Saharan Africa, driven by rapid digitalization, socio-economic challenges, and evolving technological landscapes. The patterns and trends of cybercrime in Nigeria reflect a complex interplay of technological advancements, demographic dynamics, and inadequate cybersecurity measures, resulting in substantial economic and social impacts (Maitanmi et al., 2024). Recent studies highlight the escalation of cybercrime incidents, with Nigeria ranked as the fifth most significant source of cybercriminal activity globally in 2024, underscoring the urgency of addressing this growing threat (World Cybercrime Index, 2024). This section examines the dominant forms, evolving trends, and key drivers of cybercrime in Nigeria, drawing on studies from 2020 onward.

i. **Financial fraud**

One of the most prevalent forms of cybercrime in Nigeria is financial fraud, particularly phishing, business email compromise (BEC), and advance-fee fraud, commonly known as "419 scams." Phishing attacks, which involve deceptive emails or messages to steal sensitive information, accounted for 41% of data security incidents in Nigeria in 2023 (Maitanmi et al., 2024). BEC scams, where cybercriminals impersonate executives to authorize fraudulent transactions, have surged, with a 1616% increase in data breaches reported in Q3 2022 (AAG IT Support, 2025). Advance-fee fraud, a long-standing issue, continues to evolve through sophisticated social engineering tactics, targeting both local and international victims (Odunayo, 2024). The Economic and Financial Crimes Commission (EFCC) convicted 2,847 individuals for cyber-related crimes in 2022, with financial fraud constituting over 70% of cases, highlighting its dominance (Tuleun, 2022).

ii. **Identity Theft and Social Engineering**

Another emerging trend is the rise of identity theft and social engineering, particularly among tertiary institution students. Studies indicate that 66% of respondents in Jos City reported negative experiences with cybercrime, with identity theft being a common issue due to low cybersecurity awareness and financial pressures (ResearchGate, 2024). Social media platforms, widely used by Nigeria's youth, have become breeding grounds for cybercriminals, with 39% of internet users aware of fraud-related cybercrimes but less knowledgeable about identity theft or malware (Nzeakor et al., 2022). The use of compromised Gmail accounts and BinBox IPs for targeted phishing campaigns has also increased, reflecting growing sophistication among Nigerian hackers (SpamAuditor, 2025).

iii. **Ransomware and firmware attacks**

Ransomware and firmware attacks are gaining traction, posing significant risks to organizations. Ransomware attacks, which encrypt data and demand payment for release, have

become more prevalent, with Nigeria experiencing a 20% year-on-year increase in cyberattacks targeting businesses in Q1 2024 (StationX, 2024). The healthcare and financial sectors are particularly vulnerable, with small businesses losing an average of $2.5 million per incident due to limited cybersecurity resources (Businessday NG, 2021). Firmware exploits, once limited to nation-state actors, are now being adopted by cybercrime groups, exploiting neglected firmware security in organizations (ThisDayLive, 2022). These trends indicate a shift toward more destructive and persistent attack methods.

iv. **Youth Bulge and Socio-Economic Factors**

The youth bulge and socio-economic factors are critical drivers of these patterns. With a median age of 18.6 years and 40.6% youth unemployment in 2023, many young Nigerians, particularly well-educated undergraduates, engage in cybercrime due to economic desperation and the allure of quick wealth (United Nations, 2023; Bamidele, 2023). The "Yahoo Boys," a term for young cybercriminals, leverage digital skills to perpetrate fraud, often glorified in Nigerian hip-hop culture, further normalizing such activities (Maitanmi et al., 2024). Rapid internet penetration, reaching 33.6% in 2023, and widespread smartphone use have facilitated access to cybercrime tools, with over 70 million internet users exposed to risks like phishing and e-theft (Odunayo, 2024).

Despite efforts by the Nigerian government, including the Cybercrimes Act of 2015 (amended in 2024) and EFCC operations, cybercrime continues to escalate due to inadequate legal enforcement and limited cybersecurity education (Tuleun, 2022). The EFCC's arrest of over 1,000 suspects in 2024, including foreign nationals involved in cryptocurrency and romance fraud, reflects a growing transnational dimension, with non-Nigerians exploiting Nigeria's reputation as a fraud hub (Dark Reading, 2025). These patterns and trends underscore the need for comprehensive strategies, including stronger legal frameworks, enhanced cybersecurity training, and socio-economic interventions to address the root causes of cybercrime in Nigeria.

c. **Relationship between Demographic Shifts and Cybercrime**

Nigeria's demographic shifts, characterized by a burgeoning youth population, rapid urbanization, and increasing digital connectivity, are intricately linked to the rising prevalence of cybercrime. These demographic changes create socio-economic and technological conditions that both enable and exacerbate cybercriminal activities, including online fraud, identity theft, and phishing (Maitanmi et al., 2024). This section explores how specific demographic factors—youth unemployment and underemployment, urban anonymity, education and ICT skills, gender dynamics, and migration—contribute to the proliferation of cybercrime in Nigeria, drawing on studies from 2020 and beyond.

i. **Youth unemployment and underemployment**

Youth unemployment and underemployment are significant drivers of online fraud in Nigeria. With a youth unemployment rate of 40.6% in 2023 and many others underemployed, economic desperation pushes young Nigerians, particularly those aged 15–29, toward cybercrime as a perceived viable income source (United Nations, 2023; Bamidele, 2023). The "Yahoo Boys," a colloquial term for young male cybercriminals, engage in phishing, advance-fee fraud, and

business email compromise, driven by the lack of formal job opportunities and societal pressures for quick wealth (Odunayo, 2024). Studies indicate that unemployed graduates, equipped with digital skills, are increasingly involved in cyberfraud, with 66% of tertiary students in Jos City reporting exposure to cybercriminal activities due to financial pressures (ResearchGate, 2024). This economic vulnerability underscores the nexus between joblessness and the proliferation of online fraud.

ii. **Urban anonymity**

Urban anonymity and the concentration of digital infrastructure in cities facilitate cybercrime. Nigeria's urbanization rate, with 52% of the population in urban areas in 2022, has created densely populated cities like Lagos and Abuja, where anonymity enables cybercriminals to operate with reduced risk of detection (United Nations, 2023). Urban centers offer robust internet connectivity and access to digital devices, fostering an environment conducive to cybercriminal activities (Ogunjobi, 2020). The transient nature of urban populations and the ease of blending into large, diverse communities allow perpetrators to execute scams, such as phishing and identity theft, with relative impunity (Maitanmi et al., 2024). This urban-digital nexus amplifies the scale and sophistication of cybercrime, as cybercriminals exploit the technological advantages of city environments.

iii. **Education and ICT skills**

Education and ICT skills play a dual role in Nigeria's cybercrime landscape, enabling both innovation and criminal entrepreneurship. The expansion of tertiary education, with over 2 million students enrolled by 2022, has equipped many youths with advanced ICT skills, including programming and network management (Tuleun, 2022). While these skills support Nigeria's digital economy, they also empower cybercriminals to develop sophisticated tools, such as malware and phishing kits, to perpetrate fraud (Odunayo, 2024). Research highlights that well-educated undergraduates, facing unemployment, turn to "cybercriminal entrepreneurship," leveraging their technical expertise to orchestrate complex scams like business email compromise, which saw a 1616% increase in data breaches in 2022 (AAG IT Support, 2025). This trend reflects how educational attainment, without corresponding economic opportunities, fuels cybercrime.

iv. **Gender dynamics**

Gender dynamics in cybercrime participation reveal a predominantly male-driven phenomenon, though female involvement is rising. The "Yahoo Boys" culture is heavily male-centric, with young men accounting for the majority of cybercrime convictions reported by the Economic and Financial Crimes Commission (EFCC), which recorded 2,847 convictions in 2022 (Tuleun, 2022). Social norms and economic pressures often push men toward cyberfraud as a means of fulfilling societal expectations of financial success (Bamidele, 2023). However, women are increasingly participating, particularly in romance scams and social engineering, exploiting gender stereotypes to build trust with victims (Odunayo, 2024). The EFCC's 2024 arrests included female suspects involved in cryptocurrency fraud, indicating shifting gender dynamics as digital access equalizes opportunities for cybercrime (Dark Reading, 2025).

v. **Migration, identity issues, and criminal networks**

Migration, identity issues, and criminal networks further link demographic shifts to cybercrime. Rural-urban migration, driven by economic prospects, has led to demographic concentration in cities, with Lagos hosting over 15 million residents (United Nations, 2023). Migrants, often young and economically vulnerable, face identity challenges, such as lack of formal documentation, making them susceptible to recruitment by cybercriminal networks (Bamidele, 2023). These networks exploit migrants' socio-economic precarity, offering training in cyberfraud techniques like phishing and identity theft (Maitanmi et al., 2024). The transnational nature of migration also facilitates cross-border cybercrime, with Nigerian cybercriminals collaborating with foreign nationals, as evidenced by EFCC arrests of non-Nigerians involved in romance and cryptocurrency scams in 2024 (Dark Reading, 2025). Migration thus amplifies the formation of organized cybercriminal networks, leveraging identity vulnerabilities and urban connectivity.

In summary, Nigeria's demographic shifts—youth unemployment, urban anonymity, ICT-driven education, evolving gender roles, and migration—create a fertile environment for cybercrime. These factors converge to enable online fraud, identity theft, and other cybercrimes, driven by socio-economic pressures and technological opportunities. Addressing this linkage requires holistic strategies, including job creation, cybersecurity education, and targeted interventions to disrupt criminal networks, to mitigate the impact of demographic shifts on Nigeria's cybercrime landscape.

Conclusion

The review establishes a clear linkage between Nigeria's demographic shifts—particularly the youth bulge, rapid urbanization, and rising digital connectivity—and the escalation of cybercrime. High youth unemployment (40.6% in 2023), urban anonymity, and advanced ICT skills among educated but jobless youths drive the proliferation of financial fraud, identity theft, and ransomware, costing Nigeria significant economic losses and tarnishing its international reputation. While legislative measures like the Cybercrimes Act (amended 2024) and EFCC operations have yielded convictions, the persistence of cybercrime underscores the need for holistic strategies addressing socio-economic vulnerabilities, enhancing cybersecurity infrastructure, and fostering public awareness to curb this growing threat.

Recommendations

1. The Nigerian government should implement targeted job creation programs for youths, focusing on ICT and digital economy sectors, to reduce economic desperation driving cybercrime.
2. Law enforcement agencies, including the EFCC, should strengthen cybersecurity training and public awareness campaigns to enhance digital literacy and protect vulnerable populations from phishing and identity theft.
3. Policymakers should invest in robust cybersecurity infrastructure, particularly in urban centers, to counter the technological advantages exploited by cybercriminals.

4. Educational institutions should integrate cybersecurity ethics into curricula to deter tech-savvy youths from engaging in cybercriminal entrepreneurship.
5. The government should foster international collaboration to disrupt transnational cybercriminal networks, leveraging partnerships to address cross-border fraud and romance scams.

References

AAG IT Support. (2025). The latest cybercrime statistics (updated April 2025). https://aag-it.com

Bamidele, A. H. (2023). Poverty and youth engagement in cybercrime in Nigeria: An overview of its effect on national security. https://www.researchgate.net/publication/372096345_poverty_and_youth_engagement_in_cybercrime_in_nigeria_an_overview_of_its_effect_on_national_security

Dark Reading. (2025). Nigeria touts cyber success as African cybercrime rises. https://www.darkreading.com

Maitanmi, S. O., & Akinpelu, A. S. (2024). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology, 1*(1), 2579–0617. https://www.researchgate.net/publication/386456789_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging trends in cybercrime awareness in Nigeria. *Virtual Commons, Bridgewater State University*. https://vc.bridgew.edu

Ogunjobi, O. (2020). The impact of cybercrime on Nigerian youths. *ResearchGate*. https://www.researchgate.net/publication/347436728_THE_IMPACT_OF_CYBERCRIME_ON_NIGERIAN_YOUTHS

Odunayo, A. (2024). A literature review on emerging cybercrime in Nigeria. *SSRN*. https://ssrn.com/abstract=4814920

ThisDayLive. (2022). Rising trends of cyberattacks in Nigeria.

Tuleun, C. D. (2022). Impact of cybercrime on national development: A review on Nigeria. *Lapai Journal of Humanities, 13*(1), 2006–2826.

United Nations. (2023). *World population prospects 2022: Summary of results*. Department of Economic and Social Affairs, Population Division. https://www.un.org/development/desa/pd/

World Cybercrime Index. (2024). Mapping the global geography of cybercrime. *PLOS ONE*. https://www.ox.ac.uk