IDEAL INTERNATIONAL JOURNAL of IGBO SCHOLARS FORUM for SOCIO-CULTURAL ADVANCEMENT (INC.) Volume 19, No 2A June, 2026
ISSN: 2476-8421

CYBER SECURITY RISKS AND ITS ASOCIAL EFFECTS: THE WAY FORWARD

BY

Ndukwe, Kalu
Department of PoliticalAbia State University, Uturu

Nwanoruo, Mercy
Department of PoliticalAbia State University, Uturu

Okorocha C. Matthew
Department of PoliticalAbia State University, Uturu

Ikechi Victor C.
Department of PoliticalAbia State University, Uturu

Abstract

Cybersecurity has evolved from a technical concern into a fundamental societal challenge affecting economic stability, national security, and individual well-being. In Nigeria, the rapid digital transformation has been accompanied by an alarming escalation of cyber threats, including phishing, ransomware, cryptocurrency fraud, Al-powered attacks, and the emergence of organized cybercriminal subcultures known as "Hustle Kingdoms."

This paper provides a comprehensive analysis of cybersecurity risks and their profound social effects, drawing on empirical research, legal frameworks, and policy documents from 2024 to 2026. The paper examines the nature and evolution of cyber threats, the structural drivers of cybercrime including youth unemployment and systemic exclusion, and the multifaceted social consequences encompassing financial losses, erosion of public trust, psychological trauma, and moral decay among youth. The paper further analyzes the limitations of current legal and institutional responses, particularly the tension between security imperatives and digital rights, before proposing a comprehensive framework for, action centered on youth empowerment, digital literacy, capacity building, legal enforcement with rights protections, and multi-stakeholder collaboration.

Keywords: Cybersecurity, Social impact, Cyber threat, Information Security.

Introduction

The 21st century has witnessed an unprecedented digital transformation that has reshaped how individuals, businesses, and governments interact, transact, and communicate. Nigeria, as Africa's largest digital economy, has experienced remarkable growth in internet penetration, mobile connectivity, and digital financial

services. According to the Cyber Security Experts Association of Nigeria (CSEAN), the country experienced millions of cyberattacks in the first half of 2025 alone, with a 64 percent increase in data breaches reported nationally.

However, this digital progress has a dark underbelly. The same technologies that enable innovation, efficiency, and connectivity also create new vulnerabilities that cybercriminals are increasingly adept at exploiting. From sophisticated phishing schemes targeting financial institutions to Al-generated deepfakes manipulating public opinion, from the emergence of "Yahoo Academies training jobless youth in digital fraud to the convergence of cybercrime with violent extremism, the threat landscape is evolving at an unprecedented pace.

Cybersecurity as a Societal Challenge

Cybersecurity is not merely a technical issue; it is a fundamental pillar of national security, economic stability, and societal well-being. When citizens lose trust in digital platforms, when young people are drawn into cybercrime as a perceived pathway to wealth, when the state expands surveillance without adequate safeguards, and when victims suffer not only financial losses but profound psychological trauma, the social fabric itself becomes frayed.

This paper addresses three central questions: What are the primary cybersecurity risks facing Nigeria today? What are their social effects on individuals, communities, and institutions? And what comprehensive strategies can be adopted to mitigate these risks while preserving digital rights and fostering a secure digital environment?

Understanding Cybersecurity Risks: Nature, Scope, and Evolution

Cybercrime refers to illegal activities conducted through digital technologies, including attacks on computer systems, data theft, financial fraud, identity theft, and various forms of online exploitation. Cybersecurity, in contrast, encompasses the policies, practices, and technologies designed to protect digital systems, networks, and data from such attacks.

The relationship between cybercrime and cybersecurity is dialectical: as defensive measures improve, offensive tactics evolve in response. This dynamic tension characterizes the contemporary digital landscape and poses ongoing challenges for policymakers, security professionals, and ordinary users.

The Evolution of Cybercrime in Nigeria

What began in the 1990s with rudimentary email scams known as "419 fraud" has evolved into highly

sophisticated schemes involving phishing, identity theft, cryptocurrency fraud, and Business Email Compromise (BEC). This evolution reflects both technological advancement and the development of organized cybercriminal networks.

The 419 Era (1990-2000s): The earliest form of Nigerian cybercrime involved advance-fee fraud, where victims were promised large sums of money in exchange for upfront payments. These scams, while crude by today's standards, established Nigeria's unfortunate reputation in global cybercrime discourse.

The Romance Scam and Phishing Era (2000s-2010s): As social media and dating platforms emerged, cybercriminals developed sophisticated romance scams, building emotional connections with victims before defrauding them. Phishing attacks targeting financial institutions also became prevalent.

The Professionalization Era (2010s-2020): This period saw the emergence of organized cybercriminal networks with hierarchical structures, specialized roles, and formalized training. High-profile cases such as the arrests of Ramon Abbas (Hushpuppi) and ObinwanneOkeke (Invictus Obi) revealed the extent to which cybercrime had become embedded in sophisticated global networks.

The Al and Cryptocurrency Era (2020-Present): The current threat landscape is characterized by Al-powered attacks, deepfake technology, cryptocurrency scams, and the exploitation of emerging technologies. The CSEAN Nigeria Cyber Threat Forecast 2025 projects a surge in cryptocurrency-related scams, driven by rising crypto prices and the influx of inexperienced investors.

Major Cyber Threats

Recent assessments have identified several categories of cyber threats that pose significant risks to Nigerian individuals, businesses, and government institutions.

Cybercriminals exploit the growing interest in cryptocurrency through Ponzi schemes, fake exchanges, and social media scams, leading to substantial financial losses for victims.

The deployment of artificial intelligence by cybercriminals represents a particularly dangerous development. Al-generated deepfakes are being used for sophisticated phishing attacks targeting financial institutions, social engineering tactics to manipulate victims, romance scams and sextortion schemes that exploit personal relationships and trust, and fake news and misinformation campaigns designed to sway public opinion.

Traditional cyber threats remain highly prevalent. Phishing attacks-fraudulent communications designed to trick recipients into revealing sensitive information-continue to target individuals and organizations across sectors. Ransomware attacks, which encrypt data and demand payment for its release, have disrupted businesses, hospitals, and government agencies.

The CSEAN report warns of increasing insider threats, where employees intentionally or unintentionally compromise security, as well as data breaches due to weak security measures in organizations. Advanced Persistent Threats (APTs) targeting critical infrastructure such as banking, telecommunications, and energy sectors pose particular concern.

The "Hustle Kingdom" Phenomenon

Perhaps the most disturbing development is the emergence of organized cybercrime training networks known as "Hustle Kingdoms." A growing underground network operating across Nigeria, the "Hustle Kingdom" represents more than crime; it is a symptom of social breakdown.

According to a joint study by researchers from the London School of Economics, the University of the Western Cape, and Nigeria's Economic and Financial Crimes Commission (EFCC), the "Hustle Kingdom" operates like a formal institution, complete with

hierarchies, "curricula," and even free accommodation for recruits. Students receive free housing, laptops, and training, but are expected to repay their "tuition" with a cut of their criminal earnings.

Dr. Suleman Lazarus from the University of the Western Cape, who has interviewed both active and convicted cybercriminals, explains that entry into these schools is rarely forced. Instead, it is driven by economic desperation and the lack of opportunity in societies where education is expensive and jobs are scarce. The promise of quick wealth makes the "Hustle Kingdom" more attractive than traditional education for many young people seeking survival and independence.

These cybercrime schools have become a deviant response to broken systems, offering young men skills, belonging, and income, but at the cost of ethics and legality.

Structural Drivers of Cybercrime

Understanding the root causes of cybercrime is essential for developing effective prevention strategies. Research consistently identifies interconnected drivers operating at individual, community, and structural levels.

Socioeconomic Factors

Poverty and youth unemployment are widely recognized as primary drivers of cybercrime in Nigeria. Research demonstrates that high rates of youth unemployment, poverty, peer pressure, and easier access to digital technology create a context where cybercrime becomes an attractive, if illicit, pathway to economic survival and social status.

The "youth bulge" phenomenon the relatively large increase in the proportion and number of young people in the population-exacerbates this dynamic. The youth bulge theory postulates that a large youth population can become a "demographic dividend" when their potentials are properly harnessed, and it can also become a "demographic bomb" in the face of systemic socio-economic exclusion, unemployment, hunger, and family poverty.

National Bureau of Statistics data indicates that youth unemployment in Nigeria rose to 7.2 percent in the second quarter of 2023, representing a significant challenge. In the face of socio-economic exclusion, neglect, and widespread corruption, the youth can resort to "get-rich-quick" mindsets through cybercrime.

Governance Failures and Institutional Weaknesses

Weak governance structures and corruption exacerbate digital insecurity. Research has found that corruption is strongly correlated with cybercrime prevalence. Weak

enforcement of Nigeria's Cybercrime Act has been identified as a major barrier to tackling emerging threats. Law enforcement agencies lack the technical capacity, resources, and sometimes the political will to effectively investigate and prosecute cybercriminals.

The absence of transparency in the administration of poverty alleviation interventions and limited opportunities are manifestations of youth exclusion from decision-making processes and are key factors influencing youth participation in cybercrime and violent extremism.

Educational Deficits and Digital Illiteracy

Despite efforts by institutions like the Nigerian Communications Commission (NCC) and the EFCC to promote cybersecurity awareness, substantial gaps in digital literacy remain, especially in rural communities and among young people. Many young people lack the skills to navigate the digital environment safely and responsibly, making them vulnerable both as potential victims and as recruits for cybercriminal networks.

The non-acquisition of cybersecurity skills, lack of digital training and limited access to quality education are among the key factors that drive youth involvement in cybercrime.

Cultural Normalization and Media Glorification

A distinctive feature of Nigeria's cybercrime landscape is the emergence of cultural narratives that normalize and even celebrate cyber malfeasance. Public figures convicted of internet fraud are often simultaneously vilified and idolized, reflecting complex perceptions of success, justice, and opportunity in a society plagued by poverty and systemic corruption.

The glamorization of cybercrime in popular culture, including music videos, social media influencers, and even some Nollywood productions, contributes to this normalization. A 2019 NOIPolls survey indicated that 32 percent of youths knew someone involved in cybercrime, revealing normalization tendencies among vulnerable demographics.

The Convergence of Cybercrime and Violent Extremism

A particularly troubling development is the convergence of cybercrime with violent extremism. Research findings have proven that the "get-rich-quick" mindset through cyber-criminalities influences the performance of human blood and body parts rituals, which translates to violent extremism.

This phenomenon, popularly called "Yahoo Plus" in local parlance, represents a new danger where local epistemologies and worldviews on wealth acquisition give rise to contemporary manifestations of spirituality

in the virtual world. When youths acquire illicit money, the result is excessive clubbing, frivolous spending, promotion of prostitution, and substance abuse, which undermine effective youth engagement in socio-economic development.

Social Effects of Cybersecurity Risks

The consequences of cybercrime extend far beyond immediate financial losses, permeating multiple dimensions of social life. Research demonstrates that cybercrime has become a systemic threat to Nigeria's progress.

Economic Effects

Direct Financial Losses: Individuals and organizations suffer substantial monetary losses from fraud, theft, and ransom payments. The scale of these losses is significant, though precise figures are difficult to obtain due to underreporting and the clandestine nature of much cybercrime.

For businesses and financial institutions, cyberattacks can cause irreparable reputational harm, eroding customer trust and leading to loss of business. For

individuals being associated with cybercrime even as a victim can carry social stigma.

Widespread fear of cybercrime reduces public confidence in digital platforms, inhibiting the growth of e-commerce, online banking, and e-government services. This has downstream effects on economic development and financial inclusion.

Social and Psychological Effects

Trusts Repeated exposure to cybercrime erodes trust in digital institutions, including banks, government online services, and social media platforms. This trust deficit has broader implications for social cohesion and governance.

Victims of cybercrime including those targeted by phishing, romance scams, or identity theft, often experience significant psychological distress, including anxiety, depression, and feelings of violation.

The normalization of cybercrime as a viable career path among young people represents a profound moral crisis. When cybercriminals are celebrated as successful within their communities, the ethical foundations of society are undermined.

National Security Effects

Cybercrime poses direct threats to national security. Attacks on critical infrastructure-including banking, telecommunications, energy, and government systems-can disrupt essential services and undermine state authority. The convergence of cybercrime with other forms of organized crime, including money laundering and terrorism financing, further compounds security challenges.

Cyber-terrorism has emerged as a significant threat to national security, economic stability, and social well-being in Nigeria. The country's increasing reliance on digital technologies has created new vulnerabilities that cyber-terrorists can exploit to disrupt critical infrastructure, steal sensitive information, and spread fear and uncertainty.

Impact on Youth Development

Cybercrime undermines youth empowerment by limiting young people's access to education, gainful employment, and other opportunities. The inability of Nigerian youth to navigate the digital environment safely and responsibly poses grave danger to Nigerians and the Nigerian economy.

The opportunity cost of cybercrime is substantial. Young people who devote their time and energy to cybercrime

are not developing legitimate skills, pursuing education, or contributing productively to the economy. This represents a significant loss of human capital for the nation.

Digital Rights and Civil Liberties Concerns

As the state responds to cyber threats, there is a significant risk that security measures may infringe upon citizens' digital rights. The Nigeria Cybercrimes Prohibition, Prevention, etc. (Amendment Act 2024) has expanded state surveillance powers, raising serious concerns about privacy and freedom of expression.

Key provisions of concern include:

Expanded Surveillance Powers: Security agencies can now intercept communications without a court order in "urgent" cases. Telecom companies must retain user data for longer periods, raising concerns about mass surveillance.

Stricter Online Speech Controls: The law criminalizes "false" or "misleading" posts-critics say this could be used to silence journalists and activists. Social media companies could be fined or blocked if they fail to take down "offensive" content quickly.

Weaponization Concerns: Human rights organizations, including the Socio-Economic Rights and Accountability

Project (SERAP), have accused Nigerian authorities of weaponizing the Cybercrimes Act to stifle dissent, criminalize journalism, and target critics of the government. Section 24 of the Act, despite its 2024 amendment, has been described as a legal bludgeon routinely used against journalists, bloggers, activists, and even ordinary citizens for expressing opinions online.

The Nigerian Guild of Editors (NGE) and SERAP have called for the suspension of the implementation of the Cybercrimes Act, decrying a sharp rise in attacks on press freedom and civil liberties. The ECOWAS Court of Justice ruled Section 24 of the original law as vague, arbitrary, and in violation of international human rights treaties, yet the amended version retains ambiguous terms that create room for arbitrary interpretation and misuse.

Current Legal and Institutional Responses

Nigeria's primary legal framework for combating cybercrime is the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, signed into law on February 28, 2024. The amendment aims to strengthen the legal framework, particularly in response to evolving threats, and addresses gaps in the original 2015 act.

Key changes in the amended Act include:

The amendment broadens the scope of offenses and imposes stricter penalties. Hacking, identity theft, and online fraud now carry longer jail terms (up to 10 years). Financial institutions must report suspicious transactions within 24 hours.

Section 24 of the Act makes it an offense to intercept or access electronic communication without authorization, including recording a conversation without the consent of all parties involved. Violations can lead to fines up to N7 million and imprisonment of up to three years.

The Act grants security agencies expanded surveillance powers, including the authority to intercept communications in urgent situations without a court order. While this may enhance law enforcement capabilities, it raises concerns about privacy rights and the potential for misuse.

Institutional Framework

Multiple government agencies have responsibilities for cybersecurity, including the National Information Technology Development Agency (NITDA), the Economic and Financial Crimes Commission (EFCC), the Nigerian Communications Commission (NCC), the National Security Adviser's office, and various law enforcement units.

The EFCC has recognized the need for multi-stakeholder collaboration, recently partnering with journalists and civil society organizations to enhance awareness and enforcement. As the EFCC Chairman stated, "the landscape of crime in the world is rapidly evolving, with a dramatic shift from traditional schemes to sophisticated cyber-enabled fraud, which makes it difficult for the anti-graft commission alone to defeat".

Private Sector and Civil Society Initiatives

Private sector organizations and civil society have made important contributions to cybersecurity. The Cyber Security Experts Association of Nigeria (CSEAN) provides research, training, and advocacy. The Information Security Society of Africa Nigeria (ISSAN) convenes annual conferences and calls for national awareness campaigns.

Yet these efforts remain fragmented and under-resourced relative to the scale of the challenge. A coordinated, national approach is lacking, and many initiatives operate in silos without adequate integration or reach.

The Capacity and Implementation Gap

A persistent gap exists between legal frameworks and practical implementation. The absence of adequate enforcement mechanisms, insufficient technical capacity

within law enforcement, and corruption has undermined the effectiveness of legal responses.

Research has found that the relationship between cybersecurity and factors such as capacity building, enhanced funding and resources, modernization of IT systems, and public awareness campaigns is significant and positive. Continuous staff training recruitment of skilled personnel in collaboration with cybersecurity experts and stricter sanctions for cybercriminals is essential for effective cybercrime control.

Recommendations and suggestions

Addressing cybersecurity risks and their social effects requires a multi-faceted, coordinated approach that addresses root causes, strengthens institutional capacity, and protects digital rights.

Youth Empowerment and Economic Inclusion

Sustainable reduction in cybercrime requires addressing its socioeconomic drivers. Youth unemployment, poverty, and lack of opportunity must be tackled through job creation, skills development, and entrepreneurship support.

Research recommends the need to address root causes through the empowerment of young people with the necessary skills and knowledge needed to succeed in the

digital landscape, thus mitigating the risks of cybercrime and unlocking new opportunities for innovation, entrepreneurship, and socio-economic development.

Young people should be provided with legitimate pathways to participate in and benefit from the digital economy. Training in ethical hacking, cybersecurity, software development, digital marketing, and other tech fields can redirect skills that might otherwise be used for cybercrime toward productive ends.

Targeted Poverty Alleviation: As socioeconomic inequality significantly drives cybercrime, targeted poverty alleviation initiatives, including conditional cash transfers, microcredit programs, and social protection schemes, can reduce the desperation that fuels cybercriminal activity.

Public Awareness and Digital Literacy

A comprehensive national awareness campaign is needed to tackle rising cyber threats, including community engagement and strategic public-private partnerships. Such a campaign should use multiple channels radio, television, social media, and community events-to reach diverse audiences with messages about safe online practices, common threats, and reporting mechanisms.

Cybersecurity education should be integrated into school curricula at all levels, from primary through tertiary institutions. This includes basic digital literacy, critical thinking about online information, and awareness of the risks and consequences of cybercrime. Beyond basic ICT, students should learn cybersecurity essentials such as safe browsing, password protection, and online privacy. Teaching these skills early will prepare young people to engage safely and confidently in the digital world.

Given the cultural dimensions of cybercrime, community-based approaches are essential. Religious leaders, traditional rulers, and community elders should be engaged in messaging that counters the normalization of cybercrime and promotes ethical digital citizenship.

Strengthening Legal and Institutional Frameworks

The Cybercrime Act must be enforced more effectively. This requires allocating adequate resources to law enforcement agencies. Providing specialized training for investigators and prosecutors, and establishing dedicated cybercrime units.

Cybersecurity policies must be developed and implemented in accordance with international human rights norms. Aligning national policy with international human-rights norms, establishing independent oversight,

enhancing transparency, and investing in infrastructure to reconcile security with rights are essential.

Research advocates for stricter sanctions for cybercriminals to create meaningful deterrence, balanced with proportionate responses that distinguish between minor offenders and serious criminals.

Cybercrime is inherently transnational. Nigerian authorities must collaborate with international partners, including INTERPOL, the FBI, and other national agencies to investigate and prosecute offenders who operate across borders.

Capacity Building and Talent Development

Cybersecurity Education and Training: Significant investment is needed in cybersecurity education and training to nurture a new generation of experts equipped to protect digital infrastructure. This requires collaboration between government, academia, and the private sector to create comprehensive training programs and career pathways.

Public-Private Partnerships: Collaboration between government agencies and private sector organizations is essential for sharing threat intelligence, developing best practices, and building collective capacity.

Retention Incentives: To address the "Japa" migration phenomenon-the emigration of skilled workers seeking better opportunities abroad, Nigeria must create incentives to retain talent, including competitive salaries, career advancement opportunities, and supportive working environments.

Multi-Stakeholder Collaboration

As ISSAN emphasizes, "cybersecurity is a shared responsibility." No single actor-government, private sector, or civil society can address the challenge alone.

Nigeria requires a truly national, multi-stakeholder cybersecurity strategy that integrates the efforts of all relevant actors, allocates resources effectively, and establishes clear lines of accountability.

Given the rapid evolution of cyber threats, strategies and responses must be continuously reviewed and adapted. Regular threat assessments, policy reviews, and stakeholder consultations are essential.

Conclusion

Cybersecurity risks in Nigeria have evolved from a technical concern to a fundamental challenge affecting economic development, social stability, and national security. The social effects of cybercrime financial losses, reputational damage, and erosion of trust,

psychological trauma, and moral decay among youth are profound and demand urgent, comprehensive response.

The structural drivers of cybercrime are well understood: poverty, unemployment, weak governance, inadequate enforcement, educational deficits, cultural normalization, and the emergence of cybercriminal subcultures that normalize and celebrate online fraud. Addressing these root causes is as important as strengthening technical defenses.

The way forward requires a holistic framework that integrates youth empowerment, public awareness and digital literacy, legal and institutional strengthening, capacity building and talent development, protection of digital rights, and multi-stakeholder collaboration.

Critically, this framework must recognize that the "Hustle Kingdom" phenomenon is a symptom, not the disease. Young people join these criminal networks not because they are inherently criminal but because they see no viable alternatives. Providing legitimate pathways to economic participation, digital skills, and social belonging is therefore not merely a crime prevention strategy but a fundamental investment in Nigeria's future.

The tension between security and rights must also be carefully managed. While effective cybercrime enforcement is essential, it must not come at the cost of

fundamental freedoms. The weaponization of cybercrime legislation against journalists and activists undermines democracy and creates a climate of fear that is itself a form of social harm.

This is not a task for government alone, nor for any single sector. It requires a national commitment-from policymakers, educators, business leaders, civil society, and ordinary citizens to build a secure, resilient, and rights-respecting digital future.

The cost of inaction is unacceptable: continued financial losses, deepening social divisions, erosion of trust in digital institutions, and the wasted potential of young people drawn into cybercrime. The cost of action, while significant, is far less than the cost of continued crisis. The question is not whether Nigeria can afford to address its cybersecurity challenges but whether it can afford not to.

References

Ainabor, A. E, &Akuza, B. O. (2025), Cyber-crimes and youth empowerment for socio-economic development in Nigeria. *International Journal of Research and Innovation in Social Science,* 9(7), 1558-1569.

Bemgba, P. T. (2025). Evaluating public perception and awareness of internet fraud among residents in Nigeria. *African Journal of Stability and*

Development (AJSD), 17(2), 903-933. https://doi.org/10.53982/ajsd 2025. 1702.06-

Etinagbedia, G. (2025). The role of public awareness and digital literacy in preventing cybercrime in Nigeria. CEEOL, Issue 2/2025.

EWN. https://www.ewn.co.za/2025/10/13/inside-the-hustle-kingdom-the- Nigerian-Cybercrime-schools-tuning-jobless-youth-into-digital-fraudsters.

Ginikachukwu, C. I. (2025). Cyber-terrorism in Nigeria: An analysis of threats, vulnerabilities, and mitigation strategies. FUNAI Law Projects https://www.nigerianjournalsonline.org/index.php/FUN AILAWPROJECTS/article /view/2046

Martin, C. (2025, October 13). Inside the 'Hustle Kingdom': The Nigerian cybercrime schools turning jobless youth into digital fraudsters.

NGE, SERAP demand reform of Cybercrimes Act, media freedom, (2025, May 2).

Nigerian Tribune. https://tribuneonlineng.com/nge-serap- demand-reform-of-cybercrimes-act-media-freedom/.

Nigeria's Cybercrime Reform. (2025, May 21). National Anti-Terrorism Law Framework. https://naltf.gov.ng/nigerias-cybercrime-reform/.

Review of the impact of cyber-crime on socio-economic development in Nigeria.(2025). Zenodo. https://zenodo.org/records/16945723.

The impact of cyber-crime and violent extremism on socio-economic development in Nigeria. (2025). Discover Global Society, 3, Article 72. https://doi.org/10.1007/s44282-025-00195-4.

Umar, A., & Manaf, H. A. (2024). Cybercrime and cybersecurity in the era of e-government: Interrogating the Nigerian state. *Journal of Tianjin University Science and Technology.* https://doi.org/10.5281/zenodo 13740477