Strengthening Nigeria's Response to Cybercrime

Policy Recommendations for a Safer Digital Economy

EXECUTIVE SUMMARY

Nigeria stands at a critical juncture in its digital evolution. As the nation's digital economy expands, valued at over $13 billion in 2022, it faces mounting challenges from cybercrime that threaten both its economic growth and international standing. This policy paper examines the complex intersection of Nigeria's digital transformation, cybersecurity challenges, and institutional responses, while proposing actionable solutions to combat the rising tide of cyber threats.

The scale of cybercrime in Nigeria has reached alarming proportions, with annual losses exceeding $800 million. Beyond immediate financial impacts, these activities severely damage Nigeria's global reputation and impede legitimate businesses' access to international markets. Traditional "419" scams have evolved into sophisticated digital operations, while new forms of cybercrime continue to emerge, exploiting the country's growing internet penetration and relatively low mobile data costs.

This challenge is compounded by significant structural factors, including a youth unemployment rate of 55.4% and inadequate legislative frameworks. The current Cybercrimes Act of 2015, while foundational, has proven insufficient in addressing contemporary cyber threats such as cryptocurrency fraud and cyberterrorism. Furthermore, enforcement agencies suffer from fragmented coordination and resource constraints, limiting their effectiveness in combating cybercrime.

This paper presents a comprehensive analysis of Nigeria's cybercrime landscape and proposes targeted policy interventions focused on four key areas: legislative reform, inter-agency coordination, infrastructure development, and public awareness. By implementing these recommendations, Nigeria can better protect its digital economy while fostering sustainable growth and international trust in its digital ecosystem.

POLICY PROBLEM

1. Nigeria's Expanding Digital Economy and Cybercrime

Nigeria's digital economy is expanding at an unprecedented rate. With over 83 million Internet users and increasing mobile penetration, the country is quickly becoming a regional tech hub. The digital economy was valued at over $13 billion in 2022 and is expected to continue growing. However, this rapid growth has created a fertile ground for cybercrime (Statista, 2023).

Cybercrime in Nigeria manifests primarily in financial fraud, phishing, and identity theft. The "419" scams, historically rooted in advance-fee fraud, have evolved into sophisticated digital schemes. The most notorious perpetrators are the Yahoo Boys, young Nigerians often motivated by unemployment and poverty, who exploit the internet to commit scams (Shola, 2021). Nigeria's internet penetration and relatively low mobile data costs ($0.39 per GB) make cybercrime accessible for both perpetrators and victims (Sule, Yusuf, & Sambo, 2022).

Cybercrime has major socio-economic implications. In 2020, Nigeria lost $800 million to cybercrime (Bruce, Lusthaus, Kashyap, Phair, & Varese, 2024). Financial institutions and consumers are the primary victims, but the broader economy suffers from reduced foreign direct investment and a tarnished global reputation. Legitimate Nigerian businesses face discrimination when engaging with international markets, further impeding economic growth (Obiefuna, Adibe, & Osuagwu, 2023).

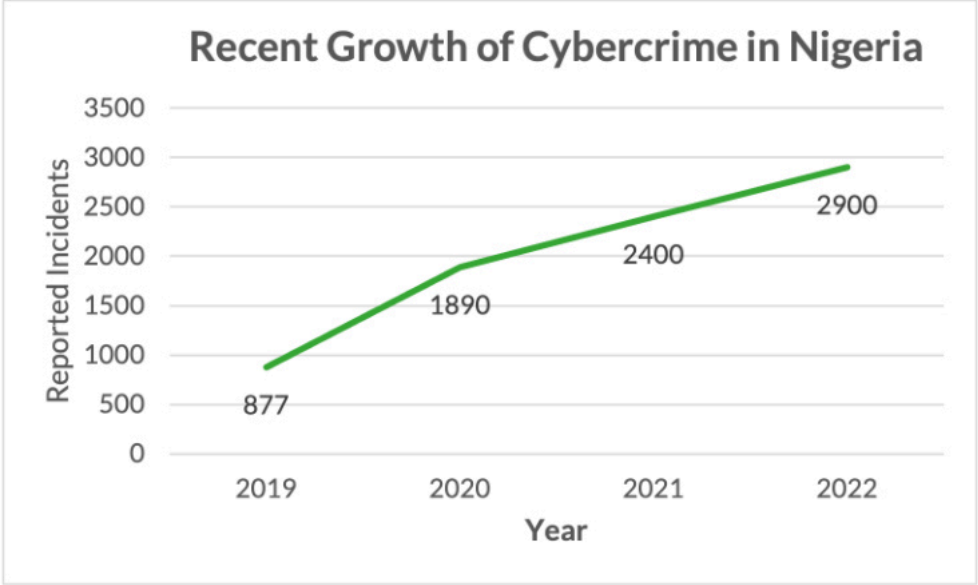

Figure 1 – Growth of reported incidents of cybercrime in Nigeria (210 Participants. Source: (Atoyebi, Omokhabi, & Omokhabi, 2024, pp. 218-219)

2. The Drivers of Cybercrime in Nigeria

The high rate of youth unemployment, standing at 55.4% in 2021, is a significant driver of cybercrime in Nigeria (Akinyentun, 2021). Cybercrime provides a seemingly easy way for young Nigerians to achieve financial stability. Relative Deprivation Theory explains this behaviour: i.e., when individuals perceive a gap between their aspirations and reality, they may resort to crime as a means of closing that gap (Stouffer, 1949).

Additionally, cybercrime has become embedded in parts of Nigerian culture. Among the youth, it is often glamorised in music, media, and peer networks, contributing to its normalisation (Shola, 2021). This societal tolerance, combined with weak law enforcement, exacerbates the problem.

3. Weaknesses in Nigeria's Cybercrime Legislation

The Cybercrimes (Prohibition, Prevention, etc) Act, (2015) is the cornerstone of Nigeria's legal response to cybercrime. While it addresses many forms of cybercrime and prescribes penalties, the law has several shortcomings. It lacks provisions for emerging threats such as cyberterrorism, social engineering, and cryptocurrency fraud (Eboibi & Mac-Barango, 2020). Furthermore, the Act's enforcement has been inconsistent due to the lack of coordination among Nigeria's multiple law enforcement agencies, including the Economic and Financial Crimes Commission (EFCC) and the Nigerian Financial Intelligence Unit (NFIU).

A significant barrier to effective enforcement is the lack of specialised skills and resources. Nigeria's cybercrime agencies are underfunded and under-equipped to handle the sophisticated tactics used by modern cybercriminals. Additionally, the lack of a central cybersecurity command structure, as seen in countries like Kenya and Singapore, contributes to inefficiency (Tsado, Raufu, Ben-Edet, & Krakrafaa-Bestman, 2023).

A recent survey of 1,104 participants (Emerging Trends in Cybercrime Awareness in Nigeria) revealed that while 68% of respondents are aware of cybercrime, a concerning 32% are still unaware of the various forms of cybercrime. This lack of awareness exposes a significant portion of the population to heightened risks of victimisation. Without adequate knowledge of how cybercriminals operate, these individuals are more likely to fall victim to scams, identity theft, and other cyber-related crimes. As such, this data reinforces the need for comprehensive public awareness campaigns that target the 32% who remain unaware of cyber threats.

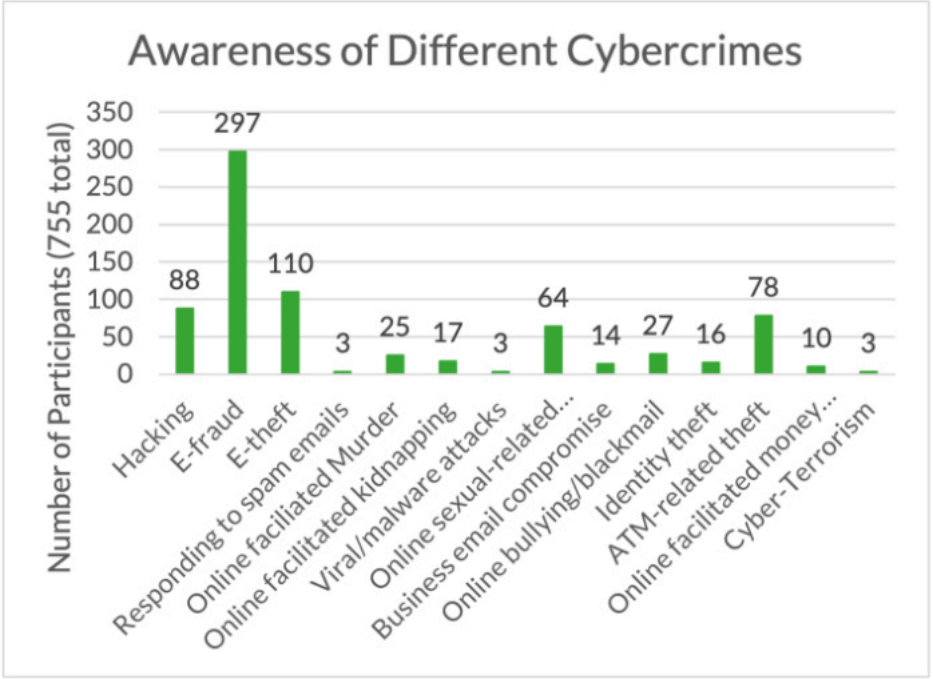

Figure 2 – Emerging trends in cybercrime awareness in Nigeria (1,111 participants). Source: (Nzeakor, Nwokeoma, Hassan, Ajah, & Okpa, 2022, p. 49)

POLICY RECOMMENDATIONS

1. Strengthen Legislative Frameworks

1.1. Expand the Cybercrimes Act of 2015

The current legislation must be revised to include protections against emerging threats such as cyberterrorism and cryptocurrency fraud. These additions will ensure that the law remains relevant in an increasingly complex digital world.

1.2. Introduce Specialised Cybercrime Courts

Cybercrime cases are often delayed due to backlogs in the general court system. The establishment of specialised cybercrime courts would expedite the legal process, ensure cases are handled by judges with digital expertise, and increase conviction rates.

1.3 Enhance Policy-Driven Identification Initiatives

Nigeria's recent SIM-NIN (National Identification Number) linkage policy illustrates how identification mandates can bolster security and reduce digital risks. This policy led to a 30% drop in active mobile subscribers, from 219.3 million in March 2024 to 153.32 million in September 2024, as unlinked SIMs were deactivated.

Achieving a 96% compliance rate, the mandate significantly reduced unverified users in Nigeria's mobile network, showing how targeted policies can limit entry points for cybercriminals. Integrating similar identification requirements into Nigeria's cybercrime legislation could strengthen monitoring and control capabilities, helping to safeguard Nigeria's digital economy.

2. Enhance Inter-Agency Coordination

2.1. Establish a National Cybersecurity Task Force

A centralised body that coordinates cybersecurity efforts across agencies, such as the Nigerian Police Force, EFCC, and NFIU, is critical for efficient law enforcement. This task force would facilitate real-time information sharing and coordinate investigations, leading to more effective responses to cyber threats.

2.2. Invest in Digital Forensics and Cybersecurity Training

To improve the capacity of law enforcement agencies, the government must invest in digital forensics training for investigators and prosecutors. Establishing cybercrime training academies in collaboration with international cybersecurity organisations would ensure that law enforcement officers are equipped with the necessary skills to combat cybercrime effectively.

3. Develop Infrastructure and Human Capital

3.1. Increase Funding for Cybercrime Prevention

Nigeria's cybersecurity infrastructure is currently underdeveloped, making the country vulnerable to cyber-attacks. Increasing funding for cybersecurity initiatives would enable the government to invest in digital forensic tools, secure data storage systems, and improved monitoring technologies for tracking suspicious transactions.

3.2. Partner with the Private Sector for Cybersecurity Development

Collaboration with private technology firms and financial institutions is crucial to building a more secure digital environment. These partnerships can help develop advanced cybersecurity measures, such as multi-factor authentication and blockchain technology, to safeguard financial transactions.

4. Increase Public Awareness and Digital Literacy

4.1. Launch Nationwide Cybersecurity Awareness Campaigns

Public awareness campaigns that educate citizens on the risks of cybercrime and the importance of digital hygiene are essential. By promoting practices such as strong password usage and phishing detection, the government can empower individuals and businesses to protect themselves. With the youth so heavily involved in cybercrime, and 65.2% of respondents believing that celebrity culture influences cybercrime (Atoyebi, Omokhabi, & Omokhabi, 2024, p. 227), employing popular stars for advertising could perhaps go a long way.

4.2. Implement Digital Literacy Programs in Schools

Introducing digital literacy programs in secondary and tertiary institutions will ensure that young Nigerians understand the dangers of cybercrime and are equipped with the skills needed to navigate the digital economy safely. These programs should include training on cybersecurity best practices, data protection, and ethical online behaviour.

CONCLUSION

The challenges posed by cybercrime to Nigeria's digital economy require immediate and decisive action. The evidence presented in this paper demonstrates that cybercrime is not merely a law enforcement issue but a complex socio-economic challenge that demands a multifaceted response. With losses of $800 million annually and a concerning 32% of the population still unaware of cyber threats, the stakes could not be higher.

The proposed policy recommendations – from strengthening legislative frameworks to enhancing digital literacy – offer a practical roadmap for reform. The success of recent initiatives like the SIM-NIN linkage policy, which achieved a 96% compliance rate and significantly reduced unverified users, demonstrates that targeted policy interventions can yield concrete results. However, implementation will require sustained political will, adequate funding, and coordination across multiple stakeholders.

As Nigeria continues its trajectory as a regional tech hub, the effectiveness of its cybercrime response will largely determine its digital future. By adopting a comprehensive approach that combines robust legislation, enhanced law enforcement capabilities, and public awareness, Nigeria can create a more secure digital environment that supports economic growth while protecting its citizens and businesses from cyber threats.

Prepared for Cenerva by:

Gana N. Nwana, BSc (Hons) (King's College London)

Gana Nwana is an Honours graduate in European Politics from Kings College, the University of London, UK. He can be reached at gana.nwana@atlantic-tm.co.uk. He is currently a Policy Research Analyst at Atlantic Telecoms & Media (Atlantic-TM) – www.atlantic-tm.com.

References

Atoyebi, V. O., Omokhabi, A. A., & Omokhabi, U. S. (2024, June). An Analysis of Young Adults Engagement in Cyber-Criminal Activities in Nigeria. *Journal of Criminology and Security Studies*, *3*(1), 213-233.

Auwal, A. M. (2023). *The Overview of Cybercrime and Cyber Security in Nigeria and Its Future Trends.* University of Jos. Jos: Research Square. doi:https://doi.org/10.21203/rs.3.rs-3307532/v2

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024, April 10). Mappingtheglobal geography of cybercrime with the World Cybercrime Index. *PLoS ONE*, *19*(4). Retrieved from https://doi.org/10.1371/journal.pone.0297312

Cybercrimes (Prohibition, Prevention, etc) Act. (2015).

Eboibi, F., & Mac-Barango, I. (2020). A Critical Examination of Cybercrime Investigation Agency under the Nigerian Cybercrimes Act 2015. In *Cybercrime: New threats, New Responses* (pp. 66-84). Universitat Oberta de Catalunya(UOC), HUYGENS EDITORIAL.

Masele, J. J., & Mwita, D. (2024). Online Television Subscription in Tanzania: Examination of the Influence of Information Quality, Video quality and technology ease of use. *ORSEA JOURNAL*, *13*(2).

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022, January 11). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(3), 41-67. doi: https://doi.org/10.52306/2578-3289.1098

Obiefuna, O. C., Adibe, E., & Osuagwu, A. (2023). Nigeria's Cybercrime (Prohibition, Prevention etc) Act 2015 at Eight: Class Act or the New Normal. *International Review of Law and Jurisprudence*, *5*(1), 1-8.

Shola, A. T. (2021). Poverty, Cybercrime and National Security in Nigeria. *Contemporary Sociological Issues*, 86-109. doi:10.19184/csi.v1i2.24188

Statista. (2023, December 21st). *Internet usage in Nigeria - statistics & facts.* Retrieved from Statista: https://www.statista.com/topics/7199/internet-usage-in-nigeria/#topicOverview

Stouffer, S. A. (1949). *The American Soldier.* Princeton University Press.

Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, *30*(6), 1557-1574. Retrieved from https://www.emerald.com/insight/1359-0790.htm

Sule, B., Yusuf, M., & Sambo, U. (2022, October 10). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, *30*(1). doi:10.1108/JFC-07-2022-0157

Tsado, L., Raufu, A., Ben-Edet, E., & Krakrafaa-Bestman, D. (2023, December). Combatting the Threat of Cybercrime in Nigeria: Examining Current Laws and Policies. *Journal of Applied and Theoretical Social Sciences*, *5*(4), 413-430. doi:10.37241/jatss.2023.100