British Journal of Interdisciplinary Research **August 2026, Volume 3, Number 13, pp. 1-13**
ISSN 3049-8899

IMPLICATIONS OF CYBERCRIMES ON GLOBAL SECURITY: A NIGERIAN PERSPECTIVE

Abdulrasheed BAWA,

Department of Political Science and International Relations, Nile University of Nigeria, Abuja, Nigeria, abdulrasheedbawa@yahoo.com

&

Bello UMAR,

Special Duties, Office of the Executive Chairman, Economic and Financial Crimes Commission, Abuja, Nigeria, muhdbello01@yahoo.co.uk

Abstract

The study analysed the implications of cybercrime in Nigeria for global security. The paper also examined the issues identified as cybercrimes in Nigeria in relation to global security, and proffered recommendations to address the challenges of cybercrimes in Nigeria from a global security perspective. The qualitative approach utilised content analysis of heterogeneous sources. It was revealed that the implications of cybercrime in Nigeria for global security are significant, and that cybersecurity is interconnected and requires coordinated efforts to address cyber threats at both the national and international levels. Combatting cybercrime requires a combination of technical measures, cybersecurity best practices, user awareness, law enforcement investigations and prosecutions, and international cooperation to mitigate risks, prevent cyber threats originating in Nigeria, and safeguard global security. It was recommended that implementing these strategies and fostering collaboration among stakeholders will make Nigeria and other countries enhance their cybersecurity posture, combat cybercrimes effectively, and contribute to global security efforts in this digital age. This study is among the recent research examining the implications of cybercrimes for global security.

Keywords: *Cyber, Cybercrime, Cybersecurity, Security, Global Security, Nigeria.*

DOI: 10.31039/bjir.v3i13.147

1. INTRODUCTION

Ransomware, phishing, online scams, and computer intrusion (i.e. hacking) are the cybercrime trends which countries most frequently perceive as posing ‘high’ or ‘very high’ threats globally (INTERPOL Global Crime Trend Summary Report, 2022).

Global security refers to the collective measures, policies, and strategies of all nations that aim to maintain peace, prevent conflict, and promote the prosperity of all individuals wherever they may be. While any activity that is being perpetuated anywhere in the globe against the peace, well-being of individuals, and stability of nations is an act of insecurity, cybercrime is one such activity.

In this age of globalisation, the entire world is operating as a single system. Nwafor (2022) stated that the internet, which is in many ways the driving force of globalisation, helps to achieve global integration in all facets of life. Thanks to the internet, in no small measure, what is happening or will happen in any part of the globe is affecting the globe directly or indirectly. Thus, crime on the internet (cybercrime) anywhere in the world can affect global security.

In Nigeria, the regulatory agency, the Nigerian Communications Commission (NCC), reported that as of March 2024, there were 219,304,281 mobile phone subscribers, of whom 164,368,292 had active internet subscriptions. The report further stated that 753,388.77 terabytes of data were used in March 2024 alone. The teledensity, assuming a Nigerian population of 190,000,000, is 101.16%. This indicates the availability of the internet in Nigeria, everywhere and for almost everyone.

In 2020, Lewis et al., in their report for the Centre for Strategic and International Affairs (CSIS) titled The Hidden Costs of cybercrime, stated that "the global losses from cybercrime approach $1trillion. How can the world's security not be affected by $ 1 trillion in criminals' hands? Jack and Ene 2016 reported that Nigeria is losing US$80 million to piracy alone, and in quoting Sesan et al. (2013), they further stated "that in 2012 alone, an estimated customer loss of N2,146,666,345,014.75 (US$13,547,910,034.80) was incurred to cybercrime in Nigeria.

As of 2024, the World Cybercrime Index (WCI) ranked Nigeria 5th globally as a cybercrime hotspot. Russia tops the chart, followed by Ukraine, China, and the United States. Nigeria is the only African Country in the top 10. Together with Ghana and South Africa, they are the only African countries in the top 20. While Ghana and South Africa have WCI scores of only 3.38 and 2.58, respectively, Nigeria scored 21.28.

Since the early 2000s, Nigeria has witnessed a significant increase in cybercrime, which poses and continues to pose a significant threat to individuals, businesses, and various levels of government not only in Nigeria but also beyond. The cyber-criminal activities have not only targeted individuals but have also impacted businesses and government institutions, leading to

financial losses, collapse of businesses, and reputational damage caused by data breaches and cyber incidents, which have lasting negative consequences for individuals, businesses, and Government (Jack and Ene, 2016; Nwafor, 2022; Pantami, 2022). The anonymity of the perpetrators and the borderless nature of the internet worldwide have made it easier for cybercriminals to operate with impunity, transcending geographical boundaries and evading traditional law enforcement measures.

The rapid advancement of technology has provided cybercriminals with new opportunities to carry out their illicit activities, ranging from financial fraud and identity theft to cyberterrorism and espionage. This surge in cybercrime not only undermines Nigeria's digital economy but also the global digital economy (Pantami,2022). The primary objective of this paper is to analyse the implications of cybercrime in Nigeria for global security. The paper also examined the issues identified as cybercrimes in Nigeria and proffered solutions to the challenges of cybercrime in the context of global security. Hence, the Research Question: What are the implications of Cybercrimes in Nigeria on Global security? The other sections are the conceptualisation, methodology, implications, conclusion and recommendations of the study.

2. CONCEPTUALISATION

2.1 Global Security

Currently, global politics faces many security challenges, including terrorism, cyber threats, epidemics, and climate change, which require different approaches to resolve; hence, the need for global mechanisms or arrangements to promote cooperative security (Adesanmi & Adeleke, 2025). Global security is a state of relations among states at the global level through the achievement of peace, security and cooperation, along with proactive prevention of risks, dangers and threats under conditions of high predictability, clarity and understanding; if at all risks and threats are to materialise, they can easily be overcome or reduced to a low degree (Stefanov, 2025).

Thus, security in this paper is defined as the protection and safety of individuals, organisations, nations, and their environments against threats that render them insecure. These threats can come from nature, individuals, organisations, or nations in the form of crimes (of any kind), conflicts, sabotage, and espionage, etc.

In view of the above, Global Security can be defined as the collective individual, organisational and national measures that aim to secure the Globe. The primary motive of which is to maintain peace, stability, and prosperity of all individuals, organisations, and the nation as a whole. Global security covers a comprehensive scope of matters, including military, economic, political, and environmental security.

The global security environment is now more volatile, complex, and uncertain, and is continually dominated by transnational threats posed not by states but by non-state actors. However, the competition between China, the United States and Russia are forcing nations to 'realign their security relationships' (Niblett, 2024; and Yusuf, 2018). Further understanding of Global Security can be achieved by examining key aspects, including Military Security, Political Stability, Human Security, Economic Prosperity and Sustainability, Nuclear Non-proliferation, Environmental Security, and Cybersecurity.

Cybersecurity is the protection of computers, networks, and data from malicious attacks. The internet has presented many advantages to its users. However, it still has risks that need to be assessed and addressed (Alabi, 2024). Cybersecurity is primarily related to this study. Cybersecurity is an increasingly important aspect of global security, as cybercrimes and other cyber threats and attacks have pervasive and destructive consequences for individuals, organisations, and governments. Global security is about protecting data and infrastructure from cyber threats of any kind.

2.2 Cybercrime

There is no one single agreed-upon definition of Cybercrime (Adesina, 2017; Nwafor, 2022). However, various institutions and individuals have given different definitions based on their institutional or individual understanding, but it can simply be referred to as any crime committed using cyberspace (Pantami, 2022). Cybercrime is an offence enabled by or dependent on computer systems, computer networks, digital systems or any other information technology platforms (Zeng &_Buil-Gil, 2023).

Cybercrime is any criminal activity carried out through a computer, computer networks, or other related devices, with the aim of accessing, transmitting, or manipulating data for financial gain, disrupting networks, stealing data, or causing harm to data.

Cybercrime encompasses a wide range of activities, including Bots, Cyber Espionage, Cyberbullying, Data Breaches, Denial-of-Service (DoS) Attacks, Hacking, Identity Theft, Malware, Online Scams, Phishing, and Ransomware.

World Cybercrime Index scholars at Oxford University identified five major categories of cybercrime:

1. Technical products/services (e.g., malware coding, botnet access, access to compromised systems, tool production).
2. Attacks and extortion (e.g., denial-of-service attacks, Ransomware).
3. Data/identity theft (e.g., hacking, phishing, account compromises, credit card compromises).
4. Scams (e.g., advance fee fraud, business email compromise, online auction fraud).
5. Cashing out/money laundering (e.g., credit card fraud, money mules, illicit virtual currency platforms).

2.3 Issues identified as cybercrime in Nigeria.

In Nigeria, Nwafor (2022), Identified several institutional and legal framework governing cybercrimes in Nigeria to include Economic and Financial Crimes (Establishment) Act, 2004, Nigerian Communications Act, 2003, Advance Fee Fraud and other related offences Act, 2006, Money Laundering (prevention and prohibition) Act, 2022, Criminal Code Act, Penal Code Act, Independent Corrupt Practices and other related Offences Act, 2000, National Information Technology Development Agency Act, 2007, Nigerian Financial Intelligence Act, 2018, Nigerian Cybercrime Working Group, Nigerian National Policy for information Technology, and the National Information and Communication Technology Policy. However, in 2015, Nigeria enacted the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. The Act, in its Part Three titled Offences and penalties, has twenty-seven (27) different offences to include the following:

1. Offences against critical national information infrastructure
2. Unlawful access to a computer
3. Registration of cybercafe

4. System interference
5. Intercepting electronic messages, emails, and electronic money transfer
6. Tampering with critical infrastructure
7. Wilful misdirection of electronic messages
8. Unlawful interceptions
9. Computer-related forgery
10. Computer-related fraud
11. Theft of electronic devices
12. Unauthorised modification of computer systems, networks, data and system interference
13. Cyber terrorism
14. Fraudulent issuance of E-instructions
15. Identity theft and impersonation
16. Child pornography and related offences
17. Cyberstalking
18. Cybersquatting
19. Racist and xenophobic offences
20. Attempt, conspiracy, aiding and abetting.
21. Importation and fabrication of E-tools
22. Breach of confidence by service providers
23. Manipulations of ATM/POS terminals
24. Phishing, spamming, and spreading computer viruses.
25. Electronic cards related to fraud.
26. Dealing with the cards of another
27. Use of fraudulent devices or attached emails and websites.

3. METHODOLOGY

Qualitative research takes an interpretative, naturalistic approach to its subject by seeking to comprehend phenomena from the perspective of the people involved. The choice is a qualitative approach due to the research problem analysis, the research question, the objective, and the study's proposition. The study primarily seeks to provide a detailed assessment of the implications of cybercrime in Nigeria for global security. Qualitative research is appropriate

for this study because it underscores processes over outcomes and interpersonal contact. Hancock (2002) believed that qualitative research methods offer crucial insight into the character of individual actors and events in the study and help explain political and social phenomena.

The Data collection methods adopted are documentary (content) analysis. In the documentary analysis, the variety of written documents, including textbooks, journals, conference proceedings, online materials, and case studies, among others, form part of the data source for this study. The study applied the principles of authenticity, credibility, reliability, and significance in analysing the information used in this investigation to address concerns about the negativity associated with the data source.

The qualitative research analysis is characterised by its descriptive nature and emphasises interpreting meanings rather than quantification. This study adopted this approach in answering the research question while working to achieve the research objective.

4. IMPLICATIONS OF CYBERCRIMES IN NIGERIA ON GLOBAL SECURITY

The implications of cybercrimes in Nigeria on global security as a unit of the international system are significant and multidimensional, and they include:

1. International cyber threat: Cybercrime activities from Nigeria, particularly Advanced fee fraud (aka 419, named after section 419 of Nigeria's Criminal Code), business email compromise (BEC) schemes, hacking and ransomware attacks are contributing significantly to the global cyber threat. WCI ranked Nigeria as the 5th-most-cyber-threat hotspot in the world, behind only Russia, Ukraine, China, and the United States of America. In Africa, Ghana and South Africa are the only African representatives in the top 20 of the WCI. Nigeria scored 21.28 in the WCI, while Russia, in first place, scored 58.39, as against 3.58 and 2.58 for Ghana and South Africa, in 13th and 14th place, respectively. These threats also pose a threat to national security, as they target individuals, businesses, and organisations around the globe, leading to financial losses, data breaches, and disruptions to critical services. Nigerian cybercriminals' tactics, techniques, and procedures are constantly evolving, challenging cybersecurity professionals and law enforcement agencies to stay ahead of the threats they pose.

2. Economic and financial implications: Nigerian cybercriminals perpetrate various forms of cybercrimes with several consequences across the globe. Financial gains for cybercriminals cause financial losses, undermining economic stability, trust in e-commerce, and the integrity of international financial systems. On the other side of the coin, the Economic implications of cybercrimes are significant for individuals, organisations, and nations. Financial losses due to data breaches, ransomware attacks, and intellectual property theft are huge; furthermore, the costs associated with detecting, investigating, prosecuting and mitigating cybercrimes are substantial. Goodman (2016) stated that Global spending on security software was almost $ 20 billion in 2012 and may reach up to $ 94 billion in 2017.

3. Implications on international businesses: Nigerian cybercriminals often target multinational corporations with sophisticated attacks, such as BEC scams and ransomware. These attacks can disrupt business operations, cause financial losses, and damage the reputations of affected companies, thereby impacting global commerce and supply chains.

4. Reputation and trust damage: The prevalence of cybercrimes originating from Nigeria has tarnished the country's reputation and eroded trust in its businesses and institutions (Nwafor, 2022). This can have diplomatic implications and affect Nigeria's relationships with other countries, potentially leading to strained international ties. Nigeria’s international reputation and trustworthiness are diminishing. We are known as the capital of the world for Advance Fee Fraud (Jack and Ene, 2016; Nwafor, 2022).

5. Technological innovation: Cybercriminal activities in Nigeria can hinder technological innovation and global digital transformation efforts. The resources and efforts spent on combating cybercrimes could otherwise be directed towards research, development, and advancement of technologies that benefit society.

6. International cooperation: Investigating and preventing Cybercrimes originating in Nigeria requires collaboration among global law enforcement agencies and governments. Partnerships and information-sharing, trust-building mechanisms must be strengthened to combat this international crime.

7. Critical infrastructure vulnerabilities: Nigerian cybercriminals may target critical infrastructure systems in Nigeria and other countries, including communication

networks, power grids, transportation systems, healthcare facilities, and educational institutions. Any success in cybercrime activities targeting critical infrastructure has severe consequences for global security, stability, and public safety; e.g., an attack on Microsoft led to flight cancellations.

8. Skills development: Nigeria's efforts to combat cybercrime have led to the development of skilled cybersecurity professionals and cybercrime investigators who contribute to global cybersecurity initiatives. The Economic and Financial Crimes Commission, for instance, has investigated and convicted thousands of suspects of cybercrime-related offences. These investigations led to further arrests of other suspects in Nigeria and beyond.

9. Intellectual property theft: The theft of intellectual property, trade secrets, and proprietary information is a type of Cybercrime with long-term implications for Nigeria's economic competitiveness and innovation capabilities in the global economy.

10. Data breaches and identity theft: Cybercriminal activities originating from Nigeria have led to data breaches, identity theft, and other forms of personal information compromise on a global scale. This can have far-reaching consequences for individuals, businesses, and governments, leading to financial losses and reputational damage (Falcon and Rosenbach, 2022).

11. Political instability: Cybercrimes are being used daily as tools for espionage and sabotage and influence operations, leading to political instability and undermining trust in democratic institutions. Manipulation of elections, dissemination of disinformation, and hacking of political organisations can have far-reaching consequences.

12. Personal privacy: Cybercrimes compromise the personal, organisational, and national privacy and security.

5. CONCLUSION

Cybercrime is a crime committed through computers and/or computer networks, or on computer(s) and computer networks; it poses significant challenges to global security, which is defined simply as protection in all ramifications for individuals, organisations, and governments across the globe.

The implications of cybercrime in Nigeria for global security are significant, highlighting the interconnected nature of cybersecurity and the need for coordinated efforts to address cyber threats at both the national and international levels. Combatting cybercrime requires a combination of technical measures, cybersecurity best practices, user awareness, law enforcement investigations and prosecution efforts, and international cooperation to safeguard global security.

Implementing these strategies and fostering collaboration among stakeholders will help Nigeria and other countries enhance their cybersecurity posture, combat cybercrime effectively, and contribute to global security efforts in this digital age. Future studies may adopt a quantitative approach to assess the implications of cybercrime for global security, with an emphasis on financial cybercrime. This study highlighted some implications of cybercrime for global security from a Nigerian perspective.

Recommendations

Navigating the challenges of cybercrime in Nigeria and its implications for global security requires a multifaceted, collaborative approach involving all stakeholders. The following are the recommendations to address these challenges:

1. Enhancement of cybersecurity measures: Countries worldwide must acquire and implement robust cybersecurity measures across their computers, networks, and related systems, including strong encryption, multi-factor authentication, software updates, network monitoring, and security awareness training. The international community must raise awareness among individuals, businesses, and government agencies about cybersecurity best practices, common cyber threats, and ways to protect against cybercrimes. Promote a culture of cybersecurity and data privacy across all sectors of their society.

2. Human capacity building: The international community must build the technical and institutional capacity of government agencies, regulatory bodies, and cybersecurity organisations to effectively mitigate cybersecurity risks, respond to cyber incidents, investigate and prosecute cybercrimes. Countries around the world must invest in cybersecurity/Cybercrime education, training, and skills development.

3. Effective law enforcement: International community enforcement of cybercrime laws, regulations, and policies to deter cybercrime activities and prosecute offenders. Where cybercrime laws do not exist, countries must work as soon as possible to enact and implement them effectively.

4. International cooperation: Countries around the world must strengthen collaboration and information sharing with international partners, law enforcement agencies, and cybersecurity organisations to address transnational cyber threats and promote global cybersecurity efforts. Enhance collaboration between law enforcement agencies, government institutions, and international partners to combat cybercrimes effectively.

5. Public-private partnerships: The international community must promote partnerships among all stakeholders to include the government, private sector, academia, and civil society to share threat intelligence, best practices, and resources for combating cybercrimes and enhancing cybersecurity resilience. Public-private collaboration will foster collaboration between the public and private sectors to share threat information, develop joint cybersecurity initiatives, and collectively address cyber threats that impact both sectors.

6. Promote ethical hacking: Countries worldwide should encourage the development of ethical hacking skills and the establishment of bug bounty programs to identify vulnerabilities in systems and applications before cybercriminals can exploit them.

7. Continuous monitoring and incident response: Implement continuous monitoring of networks and systems to detect cyber threats early. Establish effective incident response plans to promptly contain and mitigate cyber incidents.

8. Anti-money laundering measures, Financial Technology (FINTECH) regulations, and digital asset regulations should be taken more seriously globally.

REFERENCES

Adesanmi, F. O., & Adeleke, A. (2025). Global governance, security, and development. *Public Administration and Regional Studies*, *18*(1), 79 - 91.

Adesina, O.S. (2017). Cybercrime and poverty in Nigeria*. Canadian social science 13*(4), 19-29.

Alabi, M. (2024). Literature review on cybersecurity in Nigeria. Available at SSRN 4818514.

Cybercrimes Act. (2015). *Prohibition and prevention*. Federal Government of Nigeria, Abuja.

Falcon, G., & Rosenbach, E. (2002). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cyber Security.* Oxford: Oxford University Press

Goodman, M. (2016). *Future Crimes: Inside the digital underground and the battle for our connected world.* New York: Penguin Random House.

Hancock, B. (2002). *An Introduction to Qualitative Research*. London: University of Nottingham.

International Criminal Police Organisation. (2022). *INTERPOL Global Crime Trend Summary Report*. INTERPOL, Lyon

Jack, J.T., & Ene, R. (2016). *Cybercrime and the challenges of socio-economic development in Nigeria*. https://www.researchgate.net/publication/313361300

Lewis, J. A. (2020). *The hidden costs of cybercrime*. https://www.csis.org/analysis/hidden-costs-cybercrime. viewed at 16:54 on Tuesday 25th June 2024.

Ncc.gov.ng/statistics-reports/industry-overview#GSM

Ncc.gov.ng/statistics-reports/subscriber-data

Ncc.gov.ng/statistics-reports/subscriber-data-#internet-service-operator-data

Niblett, R. (2024). *The new cold war: How the contest between the US and China will shape our century*, Atlantic Books.

Nwafor, I. E. (2022). *Cybercrime and the law: Issues and Development.* Lagos: CLDS publishing

Pantami, I. A. (2022). *Cybersecurity initiatives for securing a country*. Ibadan: University of Ibadan Press.

Sesan, G., Soremi, B., & Oluwafemi, B. (2013). *Economic cost of cybercrime in Nigeria*. Cyber Steward Network Project of the Citizen Lab. University of Toronto.

Stefanov, N. (2025). Globalization and global security. *Environment Technology Resources. Proceedings of the International Scientific and Practical Conference 5*, 285-289.

World-first "Cybercrime index" ranks countries by cybercrime threat level. https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.

Yusuf, R. O. (2018). Higher defence organisation and management in defence and national security management in Nigeria. National Defence, College, Nigeria publication (Strategic Lenses Series 2 2018).

Zeng, Y., & Buil-Gil, D. (2023). Organizational and organized cybercrime. *CrimRxiv.*