British Journal of Interdisciplinary Research **August 2025, Volume 2, Number 7, pp. 182-196**
ISSN 3049-8899

CYBERCRIME AND NATIONAL SECURITY IN NIGERIA

Umearokwu Uchenna CHUKWUEMEKA,

Ph.D, Political Science Department, Faculty of Social Sciences, University of Abuja, Nigeria

Uchenna.umearokwu@uniabuja.edu.ng

&

Nwaobilo Ikechukwu ERNEST,

Political Science Department, Faculty of Social Sciences, University of Abuja, Nigeria

inwaobilo@yahoo.com

Abstract

This study examined Cybercrime and national security in Nigeria. The rise of technology online has made Nigeria one of the very connected nations, which enable communication, trade, and international relation. Nevertheless, greater connectivity has also incremented chances of hacking which present serious threat to national security. Nigeria has gained an international reputation as a source of several types of cybercrime, especially the so-called advanced fee fraud or 419 activities, as well as hacking, phishing, identity theft, and ATM fraud. Such cases have thrived in an enabling environment that has seen high unemployment in the country, poverty level, and lack of effective implementation of laws governing cyber activities. Unemployment levels are highly among the youth with the rate at 55.4 percent and a large percentage of the population struggling to live below the poverty line, which is why many see cybercrime as a good economic option. This state of affairs undermines the confidence of the masses, deters foreign investment and causes weaknesses that can be used by the criminal and terrorist networks. Adopting the Marxist theoretical framework, the analysis provided an academic interpretation of cyber-crime as an outcome of structural social-economic disparities and structural exclusion in Nigeria. It reckons that such countermeasures should not only encompass a policing approach; it should also touch on socio-economic changes based on which digital criminality has its origins. The study recommends that National Information Technology Development Agency (NITDA) should formulate and deploy a national cyber-awareness campaign that would target schools, companies, and government institutions, Economic and Financial Crimes Commission (EFCC) should strengthen and modernise its Cybercrime departments by introducing superior Cybercrime digital forensic equipment and more human resources.

Keywords: *Cybercrime, National Security, Computer-Related Crime, Digital Crime, Information Technology Crime.*

DOI: 10.31039/bjir.v2i7.63

1. INTRODUCTION

The proliferation of technology has disturbed global communication networks. Citizens are now permitted to engage freely, conduct commerce, and participate in cross-border trade. In 2020, 58 percent (4.5 billion individuals) of the global population (7.8 billion individuals) had internet access, while social media users represented 49 percent (3.8 billion individuals) of the global population. The globe has evolved into a global civilization characterized by heightened connectivity, impacting all facets of human existence (Ahmed, 2019). The increased utilization of technology can enhance communication, promote technological progress, and initiate paradigm shifts in the creation, distribution, and regulation of information. Conversely, technology has precipitated a notable rise in unlawful activities, facilitated illicit enterprises, and augmented cyberterrorism and cybercrime (Farber, 2025).
The United States, Russia, and Hong Kong are claimed to have the greatest rates of cybercrime globally. In 2013, cybercrime in Hong Kong escalated by 70 percent, resulting in financial losses of US$118 million, quadrupling the amount from 2012. Cybercrime in the United Kingdom results in an annual loss over £27 billion (US$43 billion). Nigeria is allegedly one of the nations globally associated with the origins of cybercrime. Five The primary type of cybercrime in Nigeria is "advanced fee fraud 419" (often known as yahoo-yahoo); however, other forms also occur, such as hacking, phishing, spamming, identity theft, piracy, credit card fraud (ATM), and scamming. The escalation of cybercrime in Nigeria is largely ascribed to widespread unemployment and poverty (Priyandita, Hogeveen, & Stevens, 2022). Nigeria, sometimes termed the giant of Africa, has a developing economy that falls short on various socioeconomic indicators, including health, income, life expectancy, education, employment, and crime investigations (Sede & Ohemeng, 2015). The unemployment rate in Nigeria stands at 23.1%, with youth unemployment accounting for 55.4% of this total. At the national level, 40.1 percent, or 82.9 million Nigerians, are categorized as living in poverty. Moreover, 40% of Nigeria's population has an annual per capita spending that falls below N137,430 (about $355). Disregarding cybercrime can profoundly damage a nation's reputation. The proliferation of cybercrime in Nigeria has undermined national security initiatives and engendered negative sentiments (Akinyetun, 2021).

2. LITERATURE REVIEW

A central challenge in the study of cybercrime is the absence of a universally agreed definition of what constitutes the offense. Tsakalidis and Vergidis (2017) argue that this definitional

inconsistency complicates research, while Smith (2024) highlights that the concept itself is riddled with ambiguity. Over the years, a wide array of definitions has been proposed, and the term is often used interchangeably with related expressions such as computer crime, computer-related crime, digital crime, and information technology crime. Other terms in circulation include internet crime, virtual crime, e-crime, and net crime (Rakhmanova & Pinkevich, 2020). Regardless of the terminology, cybercrime is broadly understood to involve a variety of unlawful activities carried out in the digital environment. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, deliberations on computer network offenses produced two categories of cybercrime. The first was defined as unlawful conduct performed through electronic means that threatens the security of computer systems and the information they process. The second encompassed illegal activities committed through or in relation to computer systems or networks, such as unauthorized access, unlawful distribution, or transmission of information across different platforms.

The Council of Europe's Convention on Cybercrime (2001) provides one of the most comprehensive attempts at classification. It views cybercrime as an umbrella term covering offenses against computer data and systems, crimes committed using computers, offenses related to illegal content, and violations of copyright and related rights. According to this framework, cybercrime can be grouped into four main categories. The first covers breaches of the confidentiality, integrity, and availability of data and systems, including unauthorized access, interception, alteration of data, and use of illegal devices. The second relates to crimes such as computer forgery and fraud. The third addresses offenses linked to content, for instance child pornography, while the fourth focuses on copyright and intellectual property infringements. Other scholars and institutions have also advanced definitions. Protrka (2021) describes cybercrime as "computer-mediated activities that are either illegal or considered illicit by specific actors and carried out via global electronic networks." Similarly, the Canadian Police College defines it as criminal conduct where the computer is either the target or a significant tool, a perspective widely adopted by Canadian law enforcement (Statistics Canada, 2002). Zomba (2014) emphasizes that cybercrime refers to illegal acts targeting computers, information networks, or data, including crimes carried out through these systems. What unites these views is the recognition that, despite numerous efforts, no single legal definition adequately captures the full scope of cybercrime.

Cybersecurity, on the other hand, is concerned with protecting cyberspace from risks, particularly malicious cyber activities. The concept of "cyber-threat" remains vague but is generally used to describe the harmful use of information and communication technology (ICT) as either a target or an instrument of attack by hostile actors. The National Cybersecurity Working Group (NCWG) coordinator has noted that cybersecurity often overlaps with issues of national security. Adisa (2023) also underscores that the focus of cybersecurity is the defense of networks, systems, and devices from unauthorized use. Key issues identified in cybersecurity include ensuring information confidentiality, maintaining system integrity, and strengthening the resilience of networks (CIS). The ultimate goal is to shield systems from illegal access, protect data from internal manipulation, and prevent external cyber intrusions.

The term "cybersecurity" is commonly understood in three interconnected ways. First, it refers to the set of practices, policies, and strategies—both technical and organizational—designed to protect networks, hardware, software, and data, as well as other components of cyberspace, from a broad range of threats, including those that affect national security. Second, it refers to the actual level of protection or security achieved through the adoption of such measures. Third, it is regarded as a specialized professional field that encompasses research, innovation, and the practical application of methods aimed at improving the protection of digital systems.

Cybersecurity is thus broader than simple data protection because of its close relationship with information security, which constitutes its core. Information security deals with safeguarding data in all its forms. Its objectives are generally categorized into confidentiality, integrity, and availability. Confidentiality ensures that sensitive data remains protected from unauthorized access; integrity guarantees that information is not altered unlawfully; and availability ensures that authorized users have timely access to the information when needed. In some contexts, accountability is also included, meaning that actions in cyberspace must be traceable to responsible entities. Contemporary information security strategies are focused on building systems that are resilient against a variety of threats, particularly denial-of-service attacks. Moreover, the structure and frequency of network topologies play an important role in shaping protection strategies, influencing the design of policies, objectives, techniques, and tools that can be applied to address emerging cyber risks effectively.

Cybersecurity is often viewed through multiple lenses, reflecting its multifaceted nature. One perspective is cybersecurity as an information technology issue. From this standpoint, it is considered a branch of IT security or information assurance with a strong emphasis on

safeguarding the internet and related infrastructures. Policies in this domain are aimed at reducing vulnerabilities in digital systems, often through the use of technological defenses such as antivirus programs, firewalls, and intrusion detection mechanisms. The major risks in this context arise from system failures, software bugs, human errors, and deliberate cyberattacks.

A second perspective emphasizes cybersecurity as an economic necessity. In the modern digital economy, uninterrupted access to ICT infrastructures is indispensable for business survival. E-commerce, in particular, requires constant availability of networks and secure data flows to ensure efficiency and competitiveness. Within this frame, the private sector becomes the primary actor, and the main dangers include malware, hacking attempts, insider errors, and organized cybercrime that target businesses. Ensuring robust cybersecurity is therefore essential to maintaining organizational continuity and competitiveness in global markets.

Thirdly, cybersecurity is often understood as a law enforcement challenge. In this sense, it is closely connected to the growing incidence of cybercrime. Law enforcement agencies are tasked with responding to a wide spectrum of technology-enabled offenses, from hacking to cyberterrorism. Cybersecurity measures are therefore necessary to both prevent and investigate such crimes. The threats in this context revolve around criminal exploitation of digital systems and networks for theft, fraud, disruption, or extremist purposes.

Finally, cybersecurity is also framed as a matter of national security. Societies increasingly rely on ICT for essential services, and any disruption has the potential to threaten national stability and public safety. Addressing these vulnerabilities requires comprehensive countermeasures that combine technical, legal, regulatory, organizational, and international approaches. Here, national security agencies and cybersecurity experts are the primary actors. The risks at this level include cyberterrorism, state-sponsored attacks, and information warfare waged by rival nations. Such threats make cybersecurity an indispensable element of modern defense and security policies, requiring constant adaptation to evolving technological and geopolitical challenges.

Forms of Cybercrime

a	Hacking	Unauthorized access to an individual's computer to compromise information. This is often performed remotely and takes use of weaknesses in the victim's software. Hackers can monitor the victim's computer activities and retrieve files, including passwords, credit card information, corporate data, and business strategy.
b	Cyber-theft	The use of a computer to unlawfully obtain electronic information falls within this category. Cybercriminals breach banking systems and redirect funds to an external account. Cyber-theft represents a predominant category of cybercrime, providing significant financial incentives for skilled hackers. Cybercriminals compromise a victim's banking information to misappropriate funds or acquire high-value items in the victim's name.
c	Cyberstalking	This refers to the subjection of an individual to harassment over the internet. It often involves sending life-threatening messages to the victim.
d	Software, viruses, and worms	Cybercriminals create and distribute malicious software known as viruses and worms to compromise a victim's computer network, obtain confidential information, or damage the system. Viruses and worms can jeopardize systems and are often integrated with other programs or documents, enabling their infiltration into the computer.
e	Cyberterrorism	This is a pervasive disruption of computer networks by the deployment of viruses, intended to induce fear and panic or to dismantle networks for political or ideological purposes.
f	Cyber espionage	This concerns the unlawful use of a computer to seize state secrets, engage in espionage against another government, or obtain intelligence about a government's clandestine activities.
g	Child soliciting and abuse	Cybercriminals solicit and exploit minors in chat rooms for the creation of child pornography.
h	Intellectual theft	This occurs when a person violates copyrights or obtains unlicensed intellectual properties, such as films, music, video games, and software, through the internet. Disturbingly, some websites advocate for software piracy.
i	Phishing, website cloning, and spamming	Cybercriminals are infamous for distributing spam emails to promote and advertise deceptive products and websites. To promote these services or products, criminals may duplicate a legitimate website to deceive victims, who often input

		their credit card information and other personal details, which the perpetrators then exploit for credit card fraud. Moreover, fraudsters often imitate esteemed authorities or celebrities to lure their victims into financial transactions. This is a common form of cybercrime in Nigeria.
j	Business Email Compromise [BEC] and romance fraud	Business Email Compromise (BEC) is a widespread cybercrime in Nigeria that entails sending emails from a fraudulent or compromised account to the target company's financial institution, requesting a wire transfer. At the commencement of the transfer, the payment information is compromised and modified by criminals. Fraudulent activities are sometimes conducted by syndicates based in Nigeria, which may target enterprises in the United States and later remit unlawful gains to Mexico, Ireland, or China. Business Email Compromise (BEC) and romantic fraud

Source: African Cyber Security (2019); Chigozie et al. (2017); Makeri, et al (2017)

National Security

National security pertains to the capacity for self-defense. Ogbuleke (2020) asserts that national security cannot be understood solely in military terms. The socio-economic and cultural aspects of development, modernization, and national integration are inherently linked to national security. Okoli and Ochim (2016) assert that national security entails the protection of a political entity from various threats, including political, social, economic, military, psychological, and technological dimensions. Akinyetun (2021) posits that national security includes political resilience, human capital, economic structures, technological expertise, industrial capability, resource availability, and military power. Holmes (1964) defines national security as the comprehensive protection of the state. The fundamental principle of national security is the protection of the state against hostility. It involves the mobilization of military forces to protect the state from external threats and to safeguard state secrets.

National security include national defense and the protection of various interests, including economic and geopolitical factors. This study characterizes national security as a state's provision of essential conditions that guarantee economic success and protect human and state security from both internal and external dangers. Threats appear in several forms of attacks, including economic, political, religious, and technological aspects, such as cybercrime. An overt attack on individuals and entities, whether governmental or private, intended to

undermine their capacity to achieve economic success potentially provided by the state, is a national security concern.

The Relationship between Cybercrime National Securities in Nigeria

The increasing activities of Nigerian fraudsters in high-profile frauds have put into question, the international profile of the country. The young entrepreneurs are now experiencing diminishing opportunities as visa requirements of Nigerian citizens are becoming more stringent after being distrusted by foreign governments (Ardhianti & Yulianto, 2020). The reputation of Nigeria as a cybercrime centre negatively affects the economic environment of the country, especially those of small and medium-sized businesses (SMEs) and start-ups who are reliant on foreign collaborations. This also does not favor potential investors adding insult to the inability of Nigeria in attracting foreign direct investment. This crime increased or became more threatening after the arrest of Ramon Abass (popularly known as Hushpuppi), six Nigerians, Alex Ogunshakin, Richard Uzuh, Abiola Kayode, Micheal Olorunyomi, Nnamdi Benson and Felix Okpoh were some of the names on the most wanted list by the FBI, with Business Email Compromise and romance scams defrauding people in the United States a total of 6.3 million dollars. In addition to reputation loss, cybercrime poses direct risks to people subjecting them to the risk of financial losses and identity theft, intellectual property infringement. The scams are common in the vulnerable groups such as the elderly since they do not possess the technical expertise to identify the scams. More than 62,000 Americans age 60 and older lost more than 649 million in 2018 (Apeloko, Chukwudi, Atobatele, & Chiamaka, 2024). In Nigeria, Olawe (2023) points out that the representatives of older generations of citizens make up a significant percentage of victims of scams, which is an indication of the human impact of cybercrime.

According to Umaru, Aguda, and Davies (2018), poverty is one of the primary causes of cybercrime since economic deprivation is forcing most youth to engage in fraudulent online activities. Yet, these initiatives deeply hurt the interests of Nigeria internationally and deter tourism, drive away investments, and this lowers macroeconomic stability and financial inclusion. The other implication of cybercrimes on national interest is its involvement in the economic advancement and welfare of its people. The continuous fraudulent Internet practices are painting Nigeria as insecure when it comes to doing business destroying the confidence in its financial system and also posing obstacle to international cooperation. This fear of online fraud has made a lot of business people resist online transactions and this has acted as the major

barrier to ICT adoption and innovation. The pressure to demonstrate legitimacy is also becoming an increasing burden to the Nigerians connecting with foreigners online and erodes the element of trust which are vital to social and business interactions across borders. As result of this rising mistrust, as Ogunseye notes, the country risks losing its ability to be an active participant in the global economy thus making the country an economic outcast.

Threats of cyber-crime are not only restricted to the economy but in issues of security and governance too. The Boko Haram insurgency hacked the servers of state department security on August 30, 2013 and stole sensitive information about over 60 officials of the department including their personal information of the loved ones. This instance indicated the vulnerability of lives and unstable national security that can be directly impaired by the possibility of cyberattack. The price of cybercrime has been increasing in the financial world, prompting companies and banks to invest extremely huge resources towards enhancing online security. Umaru points out that such incremental security costs add to operations, cutting down profitability and decreasing growth. Cybercrime has drastically destabilized the financial sector of the whole of Africa, as in Nigeria, the proportion of cyber-related fraud has steadily increased as overall fraud activity. The outcome has been a profound loss of trust by the population in finance institutions and an attitude that is even more resistant to the capacity of the state to guarantee its citizens against cyber threats.

3. THEORETICAL FRAMEWORK

Routine Activity Theory (RAT)

This paper adopted Marxist Theory as the theoretical framework. The theory, one of the first historical materials of the 1848 Communist Manifesto by Karl Marx and Friedrich Engels in the middle of the 19th century, is the social, economic and political framework, analyzing the society and its use as the mean of struggle among the classes, economic inequality and exploitation of the working people by the ruler elite. According to Marxism, the capitalist society is such that it possesses an inherent property distribution of wealth, power and opportunities that creates a basis of social tensions and hereditary aberrant practices. According to a Marxist approach, crime is frequently part of the reaction to forms of systemic injustices and financial exploitation. Marxist theory applied in understanding cybercrime and national security in Nigeria enables one to derive the idea of socio-economic deprivation that promotes criminal behaviour in a global world driven by capitalism. High unemployment rate in Nigeria,

poverty, and low social mobility in the country form an environment where a significant portion of the population especially the young population is locked outside official channels of the enrichment process.

The birth of the digital divide, and the rapid use of technologies has brought another issue of classes in cyberspace: the population that is considered to be able to use technologies, but is subjected to economic uncertainty takes advantage of the world economy system using cybercrime means. Here, the associated crimes such as advanced fee fraud (419 scams), hacks, and identity theft can be considered as forms of crimes generated by structural differences where the people with less economic advantage use criminal styles to counteract their alienation. The dominance of the ruling class (in form of political elites and business owners who possess large wealth) to control resources and opportunities, creates limited legitimate prospects to large segments of the population. There are no good social buffers and wealth distribution made fight income to further create the elements of economic viability or success through the cybercrime industry.

4. GOVERNMENT RESPONSE AND SOLUTION TO CYBERCRIME IN NIGERIA

A preliminary assessment of the trend analysis of cybercrime in Nigeria suggests that it is deeply rooted and requires state involvement. According to Omodunbi, Odiase, Olaniyan, and Esan (2016), the cyber crime in Nigeria has a long history and assumes various forms of crime such as BVN scams, banking fraud, sales scam, forgery, data and airtime theft/sales, software piracy, Nigerian prince, charity fund scams, and social hijacking. Consequently, the government of Nigeria has established several regulations that will prevent cybercrime in the country. The key piece of legislation that is currently employed by Nigeria in order to combat cybercrime is the Cybercrime Act of 2015, although it is not possible to exclude other laws that preceded it. Awhefeada and Bernice (2020) argue that before the enactment of the Cybercrime Act of 2015, the relevant laws in Nigeria were: the Economic and Financial Crimes Commission (Establishment) Act, 2004; the Advanced Fee Fraud and Other Related Offences Act, 2006; the National Identity Management Commission Act, 2007; the Money Laundering (Prohibition) Act, 2011; the Nigerian Evidence Act; the Criminal Code Act; the Penal According to Awhefeada and Bernice (2020), the regulation mentioned above could not cope with the complexity of events related to cybercrime and lacked appropriate enforcement mechanisms. The first action taken in Nigeria concerning cybercrime is the Cybercrime Act of

2015. The National Assembly of the Federal Republic of Nigeria passed it in order to prevent, penalize, and prevent cybercrime and issues associated with it. The aims are:

The objectives are:

(a) to create a complete legal, regulatory, and institutional framework for stopping, finding, prosecuting, and punishing cybercrimes in Nigeria;

(b) to protect important national information infrastructure; and

(c) to improve cybersecurity and protect computer systems and networks, electronic communications, data, computer programs, intellectual property, and privacy rights.

Part II of the Act says that the President can name certain computer systems, networks, and information infrastructures as Critical National Information Infrastructure if the National Security Adviser suggests it. These systems, networks, and infrastructures are important to Nigeria's national security or the economic and social well-being of its people. This shows that the Act sees computer infrastructure as an important part of national security and a necessary step to protect the economic well-being of Nigerians.

Part III of the Act lists cybercrimes in Nigeria, such as breaking into critical national information infrastructure; accessing computers without permission; intercepting communications without permission; changing computer programs or data without permission; disrupting systems; misusing devices; forging documents related to computers; committing fraud related to computers; stealing someone's identity and impersonating them; making and distributing child pornography; stalking someone online; squatting on someone else's domain; committing cyberterrorism; committing racially and xenophobically motivated crimes; attempting, conspiring, aiding, and abetting; and corporate liability. Depending on the crime, the punishments can include jail time, the death penalty, and/or fines of between 5,000,000 ($12,904) and 25,000,000 ($64,523).

Since the Cybercrime Act went into effect, there hasn't been much progress in fighting cybercrime in Nigeria. The Act set up a Cybercrime Advisory Council to give advice on how to stop and deal with computer-related crimes, cybercrimes, threats to national cyberspace, and other cybersecurity issues. However, it does not include any particular cybersecurity measures

for fighting cybercrime. The rise in cybercrime has not stopped. The goal of this project right now is to look at the future of cybersecurity. The Global Cybersecurity Index (GCI) puts Nigeria 57th out of 175 countries in the fight against cybercrime around the world.

Nigeria's commitment to fighting cybercrime is rated as "medium," along with South Africa, Uganda, Tunisia, Pakistan, Mexico, the UAE, Kuwait, Iran, Greece, and 45 other countries. People in Kenya, Egypt, the US, the UK, Korea, Japan, and France, on the other hand, are thought to be quite devoted. So, it's clear that the Nigerian government needs to work more to make cybersecurity better.

To make the cybersecurity environment better, Nigeria needs to do more to build capacity and develop its people. Awareness and cybersecurity education should be at the top of the list for the government and other important groups. Cybersecurity should be considered a fundamental element of the educational framework and integrated at all educational levels (Technical College, College of Education, Polytechnic, and University) within relevant disciplines (political sciences, economics, business, engineering, social sciences, and law). Education is an important part in improving human capital. Education improves competitiveness, job prospects, and social cohesion. Ghernaouti-Hélie, Simms, and Tashi (2011) assert that education is an essential factor in enhancing confidence and security in the use of ICT and cybersecurity.

5. CONCLUSION

Cybercrime in Nigeria is one of the top national security issues which is driven by the above factors of unemployment, poverty and poor applications of the cyber laws. It can destroy trust in the population, scare away foreign investment, and give criminal and terrorist networks a channel to which they can be active. Otherwise, it will negatively affect the world image of Nigeria even more and undermine its economical and safety networks. The digital space in Nigeria requires a concerted effort by the government body, security agencies, and the private sector to achieve security and cyber resilience of the country with technology advancement becoming an engine of growth and not a means of committing crimes.

Recommendations

1. National Information Technology Development Agency (NITDA) should formulate and deploy a national cyber-awareness campaign that would target schools, companies, and government institutions.

2. Economic and Financial Crimes Commission (EFCC) should strengthen and modernise its Cybercrime departments by introducing superior Cybercrime digital forensic equipment and more human resources.

3. Courses on cyber-safety and digital ethics should be made compulsory by Federal Ministry of Education as part of secondary and tertiary education curriculum.

4. High level youth digital skills and entrepreneurship programmes offered nationwide should be instituted by Federal Ministry of Labour and Employment in collaboration with the private tech companies to give them options instead of cybercrime.

REFERENCES

Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.

Ahmed, U. (2019). The Importance of cross-border regulatory cooperation in an era of digital trade. *World Trade Review*, *18*(S1), S99-S120.

Akinyetun, T. S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2), 86-109.

Apeloko, O. D., Chukwudi, C. E., Atobatele, A. J., & Chiamaka, C. S. (2024). Impacts of Cyber Crimes on the Image of Nigeria in the International Community: A Case of the Perceptions of Ghanaians. *Journal of African Film & Diaspora Studies (JAFDIS)*, *7*(4).

Ardhianti, M., & Yulianto, B. (2020, March). Sign on Cybercrime Text in Java. In *4th International Conference on Arts Language and Culture (ICALC 2019)* (pp. 603-608). Atlantis Press.

Awhefeada, U. V., & Bernice, O. O. (2020). Appraising the laws governing the control of cybercrime in Nigeria. *Journal of Law and Criminal Justice*, *8*(1), 30-49.

Chigozie, M. P., AGA, C. C., & Onyia, E. (2018). Effect of human capital development in organizational performance in manufacturing industries in South-East Nigeria. *International Journal of Academic Research in Economics and Management Sciences*, *7*(3), 60-78.

Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal*, *38*(1), 29.

Ghernaouti-Hélie, S., Simms, D., & Tashi, I. (2011, September). Protecting information in a connected world: A question of security and of confidence in security. In *2011 14th International Conference on Network-Based Information Systems* (pp. 208-212). IEEE

Holmes, J. W. (1964). The Political and Philosophical Aspects of UN Security Forces. *International Journal*, *19*(3), 292-307.

Makeri, H. K., Ayo, J. O., Aluwong, T., & Minka, N. S. (2017). Daily rhythms of blood parameters in broiler chickens reared under tropical climate conditions. *Journal of circadian rhythms*, *15*, 5.

Ogbuleke, L. E. (2020). Leadership, strategic communication and national security in Nigeria. *Mediterranean Journal of Basic and Applied Sciences (MJBAS)*, *4*(2), 41-53.

Okoli, A. C., & Ochim, F. (2016). Forestlands and national security in Nigeria: A threat-import analysis. *IIARD International Journal of Political and Administrative Studies*, *2*(2), 43-53.

Olawe, O. E. (2023). Representation of Nigerian Internet scamsters in selected Nigerian and International news reports. *British Journal of Multidisciplinary and Advanced Studies*, *4*(2), 21-41.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology*, *1*(1), 37-42.

Priyandita, G., Hogeveen, B., & Stevens, B. (2022). State-sponsored economic cyber-espionage for commercial purposes.

Protrka, N. (2021). Cybercrime. In *Modern Police Leadership: Operational Effectiveness at Every Level* (pp. 143-155). Cham: Springer International Publishing.

Rakhmanova, E. N., & Pinkevich, T. V. (2020, May). Digital crime concept. In *2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth"(MTDE 2020)* (pp. 193-196). Atlantis Press.

Sede, P. I., & Ohemeng, W. (2015). Socio-economic determinants of life expectancy in Nigeria (1980–2011). *Health economics review*, *5*(1), 2.

Smith PhD, T. (2024). Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimization in the Digital Realm. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2), 4.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710-729.

Umaru, H., Aguda, N. A., & Davies, N. O. (2018). The effects of exchange rate volatility on economic growth of West African English-speaking countries. *International journal of academic research in accounting, finance and management sciences*, *8*(4), 131-143.

Zomba, L. B. (2014). *Computer related crimes: a comparative analysis of Tanzanian and South African frameworks* (Doctoral dissertation).