UAR Journal of Arts, Humanities & Social Sciences (UARJAHSS)
Vol. 1, Issue. 6, August 2025
ISSN: 3049-4362
DOI: 10.5281/zenodo.16945723

REVIEW OF THE IMPACT OF CYBER-CRIME ON SOCIO-ECONOMIC DEVELOPMENT IN NIGERIA

Oluwatoyin Adewale SHEYINDEMI[1] and Thomas Imoudu GOMMENT, Ph.D.[2]

[1,] Department of Sociology, Faculty of the Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State Nigeria
[2.] Department of Sociology, Faculty of the Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State Nigeria

Article Info

Article historys:

Received: 09/08/2025
Accepted: 15/08/2025
Published: 26/08/2025

Keywords:

Cybercrime, Socio-economic Development, Youth, Digital Access, Nigeria

ABSTRACT

Nigeria has seen a notable increase in cybercrime, particularly among young people, as a result of the growing integration of digital technology into daily life. The impact of cyber-economic crime on Nigeria's socioeconomic development is reviewed in this paper. Examining Nigeria's cybercrime rate, determining the reasons behind youth cybercrime, and examining the effects of cybercrime on the nation's socioeconomic development are among the paper's goals. The study is based on the theories of routine activity and social disorganisation, and it uses the secondary method of data collection. The paper's analysis of the literature shows that high rates of youth unemployment, poverty, peer pressure, a lack of cyber-regulatory enforcement, and easier access to digital technology are the main causes of cybercrime in Nigeria. According to the report, cybercrime has far-reaching effects, such as financial losses, harm to one's reputation, a decline in national security, a decline in public confidence in digital platforms, and moral decline in young people. The paper's conclusion asserts that cybercrime has evolved into a systemic threat to Nigeria's progress and suggests a multifaceted strategy that includes enhanced cybercrime enforcement, policy reform, youth empowerment, and public awareness.

Corresponding Author:

Oluwatoyin Adewale SHEYINDEMI
Department of Sociology, Faculty of the Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State Nigeria

Introduction

Internet use is now commonplace and a necessary part of everyday life in the modern world (Ch et al., 2020; Viraja & Purandare, 2021). People use the internet for a variety of purposes, from online shopping and communication to managing the home and office. With instant information, quicker communication, and increased efficiency, this digital access has drastically decreased human labour, which results in cost savings and increased productivity for individuals, families, and society as a whole (Yasin et al., 2021). Internet access was mostly limited to desktop computers in cities in the early 2000s, but with the advent of smartphones, almost everyone now has easy access to the internet (Singh, 2018).

Kaur (2015) asserts that the many advantages associated with internet use have fuelled its explosive growth. However, there are now more chances for criminal exploitation due to the widespread adoption of internet technologies, especially in the form of cybercrime. Because cybercriminals misuse information and communication technologies (ICT), the growing incidence of cybercrime poses major risks to both individuals and organisations. Data system attacks, identity theft, child pornography, fraudulent online transactions, online scams, and malicious software like worms, viruses, phishing, and email fraud are some examples of these crimes. Khudhair (2021) points out that since cybercrime typically entails using computers, networks, and digital data to extort money from victims, the likelihood of becoming a victim of such crimes increases as more people acquire internet access.

In a similar vein, Aghatise (2016) highlights that cybercrime frequently targets computers in order to distribute malware, steal private information, or obtain unauthorised access to sensitive data. Furthermore, according to Ajah and Chukuemeka (2019), cybercrime includes more conventional offences like fraud, impersonation, and forgery, but they are now committed online. According to Olarewaju et al. (2020), cybercrime is one of the most prevalent types of crime in Nigeria, particularly among young people. Often referred to as "yahoo-yahoo," "419 stars," or "yahoo plus," these cybercriminals take advantage of online platforms and social media to commit fraud and identity theft.

Many display lavish lifestyles that are financed by online fraud, and some even use ritualistic techniques to control their victims, like incisions or charms. Nigerian cybercrime is well-organised and aided by insiders, such as bank workers who divulge private client data or enable illegal transactions using credit cards, foreign accounts, and money transfers (Olarewaju et al., 2020).

According to Oumarou (2007), even small-scale cyberattacks can have serious repercussions for companies. Hackers' misuse of cyberspace damages digital infrastructure, erodes customer trust in online services, and negates the potential advantages of ICT adoption (Folashade & Abimbola, 2013; Hassan et al., 2012; Ibrahim, 2016). According to research, the majority of Nigerian cybercriminals are young adults, especially students, recent graduates without jobs, and school dropouts (Hassan, Lass & Makinde, 2012). They take advantage of cyberspace's anonymity to perpetrate theft, fraud, and other offences that jeopardise Nigeria's economic stability. Olayemi (2014) noted that over 80% of Nigerian e-commerce platforms are vulnerable to hacking because of inadequate security measures, which was brought on by the growing prevalence of cybercrime. Attacks can target even delicate organisations like the Stock Exchange, banks, online payment systems, and the Central Bank of Nigeria.

Cybercrime has significant financial costs on a global scale. According to estimates from the Council of Economic Advisers (2018), malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016. While cybercriminals have attacked ATMs in South Africa, resulting in large financial losses, hackers have breached government websites in Kenya,

endangering the data and revenue systems of citizens (Tobiko, 2014). The costs of cybercrime in Nigeria are equally concerning; according to Senator Iroegbu, the nation loses roughly 127 billion Naira a year, or 0.08% of its GDP (Ewepu, 2016).

In six countries (the United States, Japan, Germany, the United Kingdom, Brazil, and Australia), the annual cost of cybercrime ranged from USD 4.3 million to USD 17.3 million across 237 companies, according to the Ponemon Institute (2016). Through decreased profits, increased operating costs, interrupted operations, and welfare losses, these losses have a detrimental impact on people, companies, and governments. Stricter regulation and monitoring of cybercrime have become crucial due to the increasing interconnectedness of global economies and the dependence on digital technologies for financial and trade activities. Nigeria's socioeconomic advancement depends on lowering cybercrime since crime impedes development. In light of this, the current study looks at how cybercrime affects Nigeria's socioeconomic development in an effort to find ways to stop its spread and guarantee long-term, sustainable growth.

Aim and Objectives

The aim of the study is to examine the impacts of cybercrime on socio economic development in Nigeria. Specific objectives included to;

1. Examine the rate of cybercrime in Nigeria
2. Investigate the causes of cybercrime among youths in Nigeria
3. Explore the impacts of cybercrime on socio-economic development in Nigeria

Methodology

This study was conducted using a secondary source of data collection methodology, which included books, articles, and journals published by renowned criminology authors and scholars. Documentaries and abstracts, whether digital or physical, were also used as secondary sources of information for this paper.

Conceptual Review

Cyber-crime

In order to differentiate computer programs (and linked sets of programs) that are specifically made to enable financial crimes from other types of malicious software, Peter Cassidy, Secretary General of the Anti-Phishing Working Group, coined the term "cybercrime" (Shehu, 2019). Cybercrime is the term used to describe illegal actions taken against people, groups, or organisations via digital networks and technologies. The victims may suffer direct or indirect psychological, financial, or social harm as a result of these activities, which frequently involve internet-enabled devices like computers, smartphones, and tablets (Chaudhary, 2019; Kashyap & Chand, 2020). Cybercrime also includes intentional damage to digital devices or data, theft or alteration of stored data, and illegal access to databases or computer systems (Ompal et al., 2017).

Researchers have broadly divided cybercrime into three categories: crimes against organisations, governments, and individuals (Tiwari et al., 2016; Singh, 2018; Singh et al., 2019; Zahoor & Razi, 2020). Forgery, document falsification, web jacking, virus distribution, and typo-squatting, in which hackers fabricate phoney websites in order to obtain private data, including passwords—are among the crimes that frequently target individuals (Singh et al., 2019). Hacking, illegal access to classified data, cyberwarfare, cyberterrorism, and the dissemination of pirated software are examples of crimes against governments.

According to Tiwari et al. (2016), crimes against organisations include corporate data theft, email bombing, Trojan horse malware for illegal access, denial-of-service (DDoS) attacks to disrupt services, and "salami attacks" to steal money from credit cards and bank accounts.

Financial institution cyberattacks have increased in frequency, sophistication, and scope. Smaller organisations like regional banks, credit unions, payment processors, and money transfer services have also seen numerous breach attempts, even though large-scale DDoS attacks on major banks and financial systems garner a lot of media attention. Software piracy, online pornography, spam-related activities (like phishing, malware distribution, and cyberstalking), cyber hate speech, cyber espionage, cyberbullying, revenge pornography, and cyber terrorism are additional prevalent types of cybercrime. Notably, cyber fraud has been closely linked to Nigeria (Zahoor & Razi, 2020).

Lewis (2002) distinguished four essential elements for evaluating the risks of cybercrime. The first target is infrastructure, where cyberterrorism and cyberwarfare are viewed in the larger framework of past assaults on vital systems. The second is separating intentional cyberattacks from normal infrastructure failures. The idea of "weapons of mass annoyance," which refers to the reliance of contemporary infrastructure on computer networks and their inherent redundancies, comes in third. The fourth is the connection between hacking and terrorism, which investigates whether cyberweapons can accomplish desired results and how they are used to further political agendas.

According to Broadhurst (2016), there are various types of computer-related crime, such as traditional crimes that are made possible by computers (like child pornography and intellectual property theft), direct network attacks, and traditional crimes that are backed up by digital evidence. Similar to this, Hassan et al. (2012) divided cybercrimes into the following categories: malware, stalking, spam, wiretapping, password sniffing, cyberterrorism, cyberfraud, and logic bombs. This classification was further broadened by Wada and Odulaja (2012), who added phishing and counterfeit websites as extra types of cybercrime.

Socio-Economic Development

The systematic and comprehensive advancement of economic, social, cultural, and political facets with the goal of enhancing a population's general well-being is known as socio-economic development. It places a strong emphasis on a society's ongoing social and economic development. Addressing people's social needs as the primary goals of development and implementing people-centered and participatory strategies that guarantee inclusivity and equity are the two main components of social development, which in particular reflects the intricate interplay of social structures, processes, and relationships (Morris, 2022). Fundamentally, social development encourages equality of participation, social justice, and group welfare.

Indicators of social development are often used to evaluate progress in areas such as income levels, poverty reduction, security and job prospects, healthcare, education, preventing crime, and public participation. In certain instances, these indicators also take environmental factors into account (Fritz, 2004, cited in Iyabo et al., 2020). Similarly, Madan (2022) contends that fair access to resources, healthcare, education, and income distribution are all components of socioeconomic development. Essentially, the degree of socio-economic development in a community or country can be used to gauge the general quality of life there.

Additionally, by giving marginalised groups the ability to take control of their own development, improve their living conditions, and assert their legitimate position in society, socioeconomic advancement promotes sustainability (Bilance, 2022). The World Bank and Mynt (2020) support this viewpoint, arguing that poverty should be considered in relation to vulnerability, discrimination, lack of accountability, and exposure to violence rather than just low income. When combined, these perspectives imply that socio-economic development is about giving people the autonomy to make significant decisions about their lives without compromising the rights and dignity of others.

Empirical Review

There are numerous impacts as it relates to cybercrime across the globe. However, this section of the paper concentrated on reviewing previous studies on the impacts of cybercrime on socio-economic development in Nigeria.

According to Nwosu et al. (2017) investigating the intention to commit cybercrime among 1,200 computer science undergraduates from six private universities in Ogun State. Their findings revealed that, 68% of respondents had a high propensity toward cybercrime, with statistically significant associations between cybercrime intent and both age and gender. This suggests that cybercrime is not only prevalent but deeply rooted in demographic and social factors among Nigerian youth.

Similarly, Balogun et al. (2024), in a study involving 400 undergraduates at the University of Ilorin, reported that 54% of respondents had witnessed or participated in online fraud schemes, including phishing, spoofing, and financial impersonation. Notably, 61% cited access to unrestricted internet services on campus and peer pressure as factors facilitating their engagement. Furthermore, 82% of the respondents admitted that Nigerians are widely perceived as key perpetrators of cybercrime globally, and 71% reported a negative impact on their individual reputations as a result of this stereotype.

Also, Adegbola and Fadara (2022) surveyed 150 NCE students of Oyo State College of Education on their exposure to cybercrime. The study revealed that 72% of the students were aware of cybercrime techniques, while 45% admitted either having committed or considered committing such acts. The findings also highlighted a general perception that cybercrime was an acceptable means of survival amidst poor economic conditions.

In Lagos-based public universities, Okeke and Onyekachukwu (2024), found that, 58% of their respondents had witnessed cybercrime among their peers. Furthermore, 34% had experienced direct pressure or invitations to engage in cybercrime activities such as hacking, phishing, or online extortion. The study emphasized how peer networks, digital access, and lack of effective deterrence encourage cyber-offending behaviour in academic settings. Also, at the University of Nigeria, Nsukka, Uche and Uche (2023), conducted a focus group discussion with 54 undergraduates, all of whom acknowledged the high prevalence of cybercrime in their university environment. 30% of participants stated that engagement or association with cybercrime had negatively impacted their academic performance through disciplinary sanctions, stress, or anxiety linked to illegal digital activity.

Moreover, Molokwu (2022), analyzing a sample of 150 young people aged 18–35 in Ibadan, reported that internet accessibility was the most significant predictor of cybercrime involvement ($F(1,148)=9.617$; $p<.002$), followed respectively by peer influence ($F(1,148)=1.768$; $p<.186$) and unemployment ($F(1,148)=1.829$; $p<.176$). Economic hardship, however, did not reach statistical significance ($F(1,148)=0.66$; $p<.79$) (Molokwu, 2022).

Consequently, Hassan et al. (2012), identified a suite of socioeconomic factors through a nationwide survey: urbanization, high unemployment, poverty, quest for wealth, weak cybercrime enforcement, ill-equipped law enforcement agencies, and negative role models fostered youth cybercrime. Likewise, Akwara et al. (2013) confirmed a causal relationship linking unemployment poverty insecurity, with corruption and the low barrier to internet entry further exacerbating youth criminality.

Furthermore, Adesina (2017), emphasizes that approximately 35% of Nigerians live in extreme poverty, with over 50% categorized as poor creating fertile conditions for cybercrime amid severe unemployment and limited legitimate opportunities. With cybercafés widespread and minimally regulated, many youths without internet access at home resort to these venues for illicit activity. Also, Daily Trust (2022) and Punch (opinion piece, Sesan Ajibike) confirm the significance of unemployment: youth unemployment stood at 53.4% in 2022 (NBS), and this economic desperation is frequently cited alongside poverty and peer/parental pressure as primary catalysts for cybercrime.

Finally, Ukwuoma (2021) surveyed 66 respondents and reported that 100% affirmed the existence of an insecure cyberspace hindering digital trust. A substantial proportion indicated that cyber threats discourage Nigerians from engaging in electronic transactions, thus undermining digital economic growth.

Theoretical Framework

Any research project's structure, direction, and interpretation are influenced by the theory selected. Thus, two theoretical frameworks, Social Disorganisation Theory and Routine Activity Theory, were used in order to investigate the impact of cybercrime on Nigeria's socioeconomic development.

Social Disorganization Theory

Social Disorganization Theory was developed by Clifford Shaw and Henry McKay in 1929 and later formalized in their 1942 publication *Juvenile Delinquency and Urban Areas* (Vito, 2017). The central argument of the theory is that crime is significantly influenced by one's location or environment. According to Shaw and McKay, neighborhoods with persistent high crime rates share three common characteristics: physical dilapidation, poverty, and ethnic heterogeneity.

The theory assumes that communities with high levels of unemployment, frequent population turnover, and weakened social institutions lack the informal social control necessary to prevent deviant behavior. As social bonds weaken, criminal values become culturally transmitted and normalized, thereby perpetuating criminal behavior across generations regardless of who resides in the area. The theory also emphasizes that the breakdown of institutions such as the family, schools, and religious bodies leads to an increase in youth delinquency and criminality.

This theory is relevant to the current study as it provides a foundational explanation for the environmental and structural factors that drive cybercrime among Nigerian youths. In many urban slums and transitional communities, poverty, unemployment, and lack of functional education systems serve as fertile grounds for criminal behavior, including internet fraud. Madubuike and Dimnajiego (2023) affirmed that social disorganization is a key predictor of youth criminality, as it explains how dysfunctional neighborhoods erode positive social norms and reinforce deviant subcultures.

Furthermore, studies by Vito et al. (2022) argue that once criminal behavior becomes entrenched in a community, it becomes part of the cognitive framework of residents, especially youths. Hochstetler and Copes (2018) support this claim, observing that early exposure to neighborhood crime rationalizes criminal behavior and makes it appear as a legitimate means of survival.

Social Disorganization Theory is applied in this study to highlight the structural realities and disintegrated social conditions in Nigerian cities that nurture cybercriminal subcultures. It explains how youths who grow up in such disorganized environments are

more likely to adopt cybercrime as a lifestyle due to the absence of positive role models, limited opportunities, and the normalization of criminal activity.

Routine Activity Theory

Routine Activity Theory (RAT), introduced by Lawrence Cohen and Marcus Felson in 1979, explains the conditions that make crime more likely to occur. The theory suggests that criminal activity takes place when three factors intersect in the same time and space: the presence of a motivated offender, the availability of a suitable target, and the lack of an effective guardian.

Unlike Social Disorganization Theory, which focuses on environmental and structural factors, Routine Activity Theory examines situational factors—specifically, how everyday patterns of behavior and routine interactions can increase or reduce opportunities for crime. The theory argues that as more individuals gain access to digital technology, particularly without oversight or control, the likelihood of cybercrime increases.

Routine Activity Theory complements Social Disorganization Theory by providing a micro-level understanding of how cybercrime occurs among Nigerian youths. In contexts where social disorganization has already diminished collective efficacy and informal guardianship, Routine Activity Theory explains how cybercrime is facilitated by digital exposure, lack of online surveillance, and ease of target access.

For example, youths in Nigerian tertiary institutions or urban centers often have unrestricted access to the internet, unsupervised use of smartphones, and exposure to fraudulent peer groups. The lack of capable guardians such as parents, school administrators, or cyber-security policies creates opportunities for youths to exploit vulnerable online users and systems.

This theory also explains why not all youths in disorganized communities engage in cybercrime. While the environment may be permissive, actual involvement depends on routine behaviour that provide the opportunity. Thus, RAT helps bridge the gap left by Social Disorganization Theory by explaining the "how" and "when" of criminal acts, especially those conducted in virtual spaces.

Routine Activity Theory is applied in this study to demonstrate how everyday digital behaviors and weak monitoring systems create the enabling environment for cybercrime, particularly among youths who are already predisposed by structural disadvantages.

Discussion of Findings

The findings from this study have revealed critical insights into the increasing rate, causes, and impacts of cybercrime on Nigeria's socio-economic development. The study established that cybercrime is significantly prevalent among Nigerian youths, particularly those in tertiary institutions and urban centres. The review by Nwosu et al. (2017) demonstrated that 68% of undergraduates from private universities in Ogun State had a high propensity toward cybercrime. This finding aligns with that of Balogun et al. (2024), who found that 54% of students at the University of Ilorin had either participated in or witnessed cyber-related fraud schemes. These findings collectively indicate that youth involvement in cybercrime has moved from isolated deviance to a normalized subculture within academic environments.

Furthermore, the findings revealed that access to unrestricted internet, peer influence, unemployment, and a weakened legal framework are among the major drivers of cybercrime. For instance, Molokwu (2022) empirically showed that internet accessibility ($F(1,148)=9.617$; $p<0.002$) was the most significant predictor of cybercrime involvement among youths in Ibadan. Peer influence and unemployment, although slightly less significant statistically, also featured prominently in facilitating deviant behaviour. These findings reinforce the theoretical assumptions of both the **Social Disorganization Theory** and the **Routine Activity Theory** used in the study. The disintegration of social institutions such as family, school, and religion has weakened informal social control, while the daily unsupervised digital activities of youths have created the opportunities necessary for cybercrime to thrive.

The study also discovered that societal attitudes toward wealth and materialism have made cybercrime appear to be a viable and even acceptable route to success. As noted by Adegbola and Fadara (2022), 45% of surveyed NCE students admitted to having engaged in or considered engaging in cybercrime, with many viewing it as a survival strategy amid economic hardship. Similarly, Okeke and Onyekachukwu (2024) reported that 34% of university students had received invitations to participate in cybercrime, with 58% witnessing it among their peers. These results suggest that cybercrime is no longer viewed purely as criminal but has become culturally and economically rationalized within certain youth circles.

More importantly, the study revealed that cybercrime has had dire consequences on Nigeria's socio-economic development. These include loss of business assets, defamation of the nation's image, reduced investor confidence, and erosion of trust in digital transactions. Ukwuoma (2021), for example, found that 100% of surveyed respondents affirmed that the presence of cyber threats discouraged their participation in online financial activities. This loss of digital trust undermines the growth of Nigeria's digital economy and its global economic integration. Similarly, John-Williams (2025) noted that youth engagement in cybercrime not only diverts attention from productive ventures but also contributes to the rise of unproductive consumerism fueled by illicit wealth.

Additionally, the estimated economic losses linked to cybercrime are substantial. According to reports cited in the study, Nigeria loses up to ₦127 billion annually to cybercrime, which constitutes approximately 0.08% of its GDP (Ewepu, 2016). This not only affects government revenue and business operations but also diminishes the nation's global economic credibility.

In terms of social impact, the normalization of cybercrime among youths contributes to a breakdown of societal values and promotes a culture of impunity. Uche and Uche (2023) reported that students involved in cybercrime experienced academic decline due to stress, sanctions, and guilt associated with their actions. The integration of traditional spiritual practices into cybercriminal activities as documented by Olarewaju et al. (2020), further illustrates how deep-seated and ritualized cybercrime has become in Nigeria's socio-cultural landscape.

Conclusion

This paper provided insight into the impact of cybercrime on socio-economic in Nigeria. The multifaceted nature of cybercrime among Nigerian youths must be taken into consideration in any attempt to understand and address this complex issue. A comprehensive strategy that accounts for the environmental, economic, technological, social, and cultural dimensions of youth cybercriminal behavior must be adopted. Structural factors such as poverty, unemployment, and community disorganization interact with situational opportunities such as internet accessibility and

weak digital oversight to foster a conducive environment for cybercrime. The consequences, ranging from reputational damage and economic loss to weakened national security and eroded digital trust, highlight the urgency for coordinated efforts in prevention, education, and policy reform.

Recommendations

Based on the findings of this study, the following recommendations are made to address the causes and mitigate the impacts of cybercrime on Nigeria's socio-economic development:

1. The government should ensure the full enforcement of existing cybercrime laws and provide adequate support to law enforcement agencies in terms of training, tools, and technological infrastructure. In addition, there is a need to incorporate cybersecurity awareness and ethical digital practices into educational curricula at all levels. This will empower youths to understand the legal and moral consequences of cybercrime and promote responsible digital citizenship.
2. As unemployment and poverty are key drivers of cybercrime, government and private sector stakeholders must prioritize youth empowerment through job creation, digital entrepreneurship programs, and vocational training. Interventions that provide alternative, legitimate means of income will reduce the appeal of cybercrime as a survival strategy among young Nigerians.
3. Parents, educational institutions, and community leaders have a crucial role to play in monitoring and mentoring the youth. Strengthening moral education, promoting positive peer influence, and increasing parental oversight of online activities will help create an environment that discourages cyber-offending. Community-based initiatives aimed at restoring social values and fostering discipline should also be encouraged.

REFERENCES

1. *Adegbola, E. A., & Fadara, J. A. (2022). Influence of ICT on students' involvement in cybercrime in Oyo State College of Education. Journal of Digital Learning and Development in Education, 1(2), 20–35.*
2. *Adesina, F. O. (2017). Cybercrime and economic deprivation in Nigeria: A sociological analysis. Journal of Nigerian Studies, 9(1), 25–40.*
3. *Aghatise, E. J. (2016). Cybercrime and internet fraud in Nigeria: Emerging trends and challenges. Journal of African Criminology and Justice Studies, 10(1), 45–61.*
4. *Ajah, B. O., & Chukuemeka, G. E. (2019). The use of technology in modern crime: A study of cybercrime among Nigerian youths. Nigerian Journal of Criminology, 13(2), 88–101.*
5. *Akwara, A. F., Udaw, J. E., & Ajene, D. I. (2013). Unemployment and poverty: Implication for national security. Global Journal of Management and Business Research, 13(10), 1–11.*
6. *Balogun, A. R., Abdulrahman, T. M., & Aka, C. O. (2024). Perceptions and involvement of undergraduates in cybercrime activities in Kwara State. Nigerian Journal of Social Studies and Humanities, 8(1), 88–102.*
7. *Bilance. (2022). Socio-economic development and sustainability: A people-centered approach. International Development Review, 15(4), 44–58.*
8. *Broadhurst, R. (2016). Cybercrime: A criminological overview. In M. McGuire & T. Holt (Eds.), The Routledge Handbook of Technology, Crime and Justice (pp. 77–99). Routledge.*
9. *Ch, I. M., Hussain, A., & Khan, R. (2020). Internet usage and its implications on youth behavior. International Journal of Cyber Behavior, 9(1), 22–34.*
10. *Chaudhary, D. (2019). Understanding cybercrime in the digital age. Cybersecurity Review, 6(3), 35–45.*
11. *Daily Trust. (2022). Nigeria's unemployment crisis and cybercrime surge. Daily Trust Newspaper, March 14.*
12. *Ewepu, F. (2016, December 6). Nigeria loses N127bn annually to cybercrime – FG. Vanguard Newspaper. https://www.vanguardngr.com/2016/12/nigeria-loses-n127bn-annually-cybercrime-fg/*
13. *Folashade, T., & Abimbola, F. (2013). Cyber fraud and its impact on economic growth in Nigeria. African Journal of Economic Policy, 20(2), 66–80.*
14. *Fritz, T. M. (2004). Social development indicators: A review. United Nations Development Report. [Cited in Iyabo et al., 2020]*
15. *Hassan, R., Lass, R., & Makinde, A. (2012). Youth unemployment and cybercrime in Nigeria. Journal of Applied Sociology, 15(1), 33–48.*
16. *Hochstetler, A., & Copes, H. (2018). The learning and rationalization of violence in criminal settings. Deviant Behavior, 39(8), 950–965.*
17. *Ibrahim, A. M. (2016). Cybercrime and economic implications in Nigeria: A case study. International Journal of Cyber Security and Digital Forensics, 5(2), 18–27.*
18. *Iyabo, A. A., Salisu, S. M., & Gambo, L. A. (2020). Social policy indicators and development in Africa. African Social Development Review, 14(1), 71–84.*
19. *John-Williams, A. T. (2025). Youth deviance and the economics of cybercrime in Nigeria. African Journal of Sociology and Behavioral Science, 13(1), 54–68.*
20. *Kashyap, R., & Chand, R. (2020). Social media and the rise of cybercrime. International Journal of Law and Society, 2(2), 50–61.*
21. *Kaur, R. (2015). Cybercrime in the digital age: Issues and challenges. International Journal of Computer Science and Mobile Computing, 4(6), 25–30.*
22. *Khudhair, A. A. (2021). Cybercrime and digital vulnerabilities: The Nigerian experience. Journal of Information Technology and Social Science, 9(3), 118–130.*
23. *Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic and International Studies (CSIS). https://csis.org*
24. *Madan, P. (2022). Indicators of socio-economic development. Development Economics Quarterly, 3(2), 20–33.*
25. *Madubuike, C. C., & Dimnajiego, C. I. (2023). Environmental influences and youth criminality in Nigeria: An application of social disorganization theory. Nigerian Journal of Social Sciences and Criminology, 11(2), 45–60.*
26. *Molokwu, A. N. (2022). Socioeconomic predictors of cybercrime among Nigerian youths in Ibadan metropolis. Turkish International Journal of Special Education and Guidance & Counselling, 11(1), 61–68.*
27. *Morris, D. J. (2022). Dimensions of social development. Social Indicators Review, 19(4), 99–115.*

28. *Mynt, T. (2020). Redefining poverty: The multidimensional lens. World Bank Policy Paper Series, No. 217.*
29. *Nwosu, H. E., Dike, B. C., & Ogedebe, P. M. (2017). Predictors of cybercrime intent among computer science students in Ogun State private universities. International Journal of Computer Trends and Technology, 51(2), 105–110.*
30. *Okeke, F. C., & Onyekachukwu, U. (2024). Digital crime and peer influence: A study of university students in Lagos metropolis. Journal of Research in Social Sciences and Humanities, 12(3), 57–72.*
31. *Olarewaju, I. R., Omotayo, A. O., & Adeyinka, S. K. (2020). Ritualistic motivations and cyber-fraud practices in Nigeria: A social lens. Journal of Contemporary African Studies, 38(4), 553–570. https://doi.org/10.1080/02589001.2020.1755926*
32. *Olayemi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology Research, 1(1), 9–18.*
33. *Ompal, G., Ashish, K., & Deepak, G. (2017). Types and prevention of cybercrime. International Journal of Advanced Research in Computer Science, 8(5), 371–375.*
34. *Oumarou, I. (2007). Cybersecurity threat and economic implications. African Business and Technology Review, 5(3), 42–55.*
35. *Ponemon Institute. (2016). 2016 Cost of Cybercrime Study: Insights from the Global Survey. Ponemon Research Reports. https://www.ponemon.org*
36. *Shehu, S. (2019). Defining cybercrime: An overview. African Journal of Criminology, 8(2), 90–98.*
37. *Singh, A. (2018). Internet accessibility and cyber threats. Asian Journal of Information Technology, 17(4), 81–89.*
38. *Singh, V., Srivastava, S., & Chauhan, M. (2019). Cybercrime and its impact on social development. International Journal of Scientific Research and Management, 7(2), 203–210.*
39. *Tiwari, R., Bhardwaj, N., & Yadav, R. (2016). Cybercrime and preventive measures. International Journal of Engineering Sciences and Research Technology, 5(3), 204–209.*
40. *Tobiko, M. (2014). Cybercrime in East Africa: Kenya's experience. African Law Review, 4(1), 33–44.*
41. *Uche, I. P., & Uche, A. A. (2023). Cybercrime and academic performance of undergraduates at University of Nigeria, Nsukka. International Journal of Social Sciences and Humanities Invention, 10(2), 1305–1312.*
42. *Ukwuoma, S. C. (2021). Cybercrime: Implications for digital financial transactions in Nigeria. International Journal of Cyber Behavior, Psychology and Learning, 11(3), 45–59. https://doi.org/10.4018/IJCBPL.2021070104*
43. *Viraja, P., & Purandare, M. (2021). Internet usage and productivity in developing economies. Journal of Information and Communication Studies, 13(2), 44–58.*
44. *Vito, G. F., Maahs, J. R., & Holmes, R. M. (2022). Criminology: Theory, research, and policy (5th ed.). Jones & Bartlett Learning.*
45. *Wada, F., & Odulaja, O. (2012). An appraisal of cybercrime in Nigeria. Nigerian Journal of Criminology and Justice Studies, 6(1), 35–48.*
46. *Yasin, M., Usman, R., & Kamran, H. (2021). Internet in everyday life: A behavioral study. Journal of Digital Culture and Media, 9(1), 70–85.*
47. *Zahoor, M., & Razi, W. (2020). Cybercrime and its socio-economic impact in Nigeria. International Journal of Law and Cybercrime Studies, 4(1), 11–25.*