Journal of Economic Development and Village Building, Vol. 3 No. 1 March 2025, pp. (88-97). E-ISSN: 2986-4666
DOI: https://doi.org/10.59261/jedvb.v3i1.108

JOURNAL OF ECONOMIC DEVELOPMENT & VILLAGE BUILDING
Journal Homepage : http://jedvb.politeksci.ac.id/index.php/jedvb/

Effect Of Cyber Crime On The Economy: A Comparative Study India And Nigeria

Idris Muhammed Ango[1*], Salihu Ahmed[2], Bala Aliyu[3], Muhammad Sani Umar[4], Maimuna Muhammad Harande[5]
National Institute of Medical Sciences University Rajasthan, India[1,2,3,4]
Shehu Idris Institute of Health Sciences and Technology, Nigeria[5]
*Corresponding Author: idrisangomakarfi1@gmail.com

Article Info

Article history :
Received on:
January 19, 2025
Revised on:
January 29, 2025
Accepted on:
February 26, 2025
Available Online :
March 25, 2025

Keywords :
effect of cyber of crime; youths; India and Nigeria

Abstract

Background: The astounding and alarming rate of crime by young adult at global level have attracted attention, while cybercrime has become a material economic concern for both advanced and emerging economies.
Objective: This study examines the causes of cybercrime among young adults in India and Nigeria, identifies the effects of cybercrime on the economies of India and Nigeria, and proposes appropriate solutions to the menace of cybercrime in the study countries.
Method: This study uses a descriptive comparative desk-review design based on secondary data. The units of comparison are India and Nigeria, and the sources consist of documented scholarly written materials, legislation and other publications cited in the article. The analysis was conducted by organizing the available secondary evidence into common themes that permit comparison between India and Nigeria.
Result: The findings indicate that cybercrime has increased in India and remains a major cause of concern in Nigeria, with economic consequences for individuals, businesses, and public institutions. Youth involvement, online fraud, limited investigative capacity, legal challenges, and cyber-security skills remain important concerns.
Conclusion: The findings also have implications for cybercrime legislation, investigative capacity building, public awareness campaigns and youth employment policy, while serious action is needed to protect cyber space as a national security requirement.

This is an open access article under the CC BY-SA license.

Copyright © 2025 by Author. Published by Politeknik Siber Cerdika Internasional

INTRODUCTION

The commercial diffusion of the internet in the mid-1990s transformed the way business is conducted, allowing firms of every size to sell goods and services across long distances and national borders with a single keystroke or click. The same infrastructure, however, opened new opportunities for fraud, since offenders tend to follow financial flows and continually adapt their schemes to new technologies (Lazarus, 2025). Early commentators had already anticipated that the internet would reshape social behaviour, including deviant behaviour, as it entered the new millennium (Cooper, 1997). In the terms of the functionalist tradition, cybercrime can be understood as an unintended consequence of an otherwise beneficial technological change (Elster, 1990). More than two decades after

the beginning of the internet revolutio, cyber fraud and other forms of cybercrime have not only persisted but have expanded considerably in scale and sophistication (Okosun & Ilo, 2023).

Recent evidence confirms that the problem has intensified. The Internet Crime Complaint Center (IC3) of the United States received 859,532 complaints in 2024, with reported losses of US$16.6 billion, a 33% increase over 2023. In India, the National Crime Records Bureau registered 65,893 cybercrime cases in 2022, an increase of 24.4% from 52,974 cases in 2021, with fraud being the motive in 64.8% of cases. In Nigeria, the Nigerian Communications Commission has estimated that cybercrime costs the country about US$500 million annually. These figures indicate that cybercrime is no longer a peripheral technical issue but a material economic concern for both advanced and emerging economies (Aborisade et al., 2024).

Earlier industry data had already revealed the geographic distribution of online fraud. In February 2013, the fraud-prevention firm iovation published an analysis of billions of on line transactions showing that credit card fraud, identity theft, and account takeover or hija cking attempts were the leading cybercrime schemes in 2012. Such patterns are relevant fo r organisations engaged in cross-border business because they indicate where threats are m ost likely to originate. Although these data are now dated, they provide a useful historical b aseline, as they identify India and Nigeria among the leading sources of online fraud in their respective regions.

According to that analysis, Africa recorded the highest proportion of fraudulent transa ctions (7%), with Nigeria and Ghana contributing the highest percentages; most fraudulent transactions from the continent targeted online dating and retail websites and involved cre dit card fraud, identity theft, profile misrepresentation and online scams. Asia ranked secon d (5%), with above-average rates in Bangladesh, Vietnam and India; nearly half of these tra nsactions targeted retail websites, while online dating and multiplayer online gaming accou nted for about one-third, including shipping fraud, gold farming, chargebacks and the theft of virtual goods through account hijacking.

South America followed (4%), led by Chile and Brazil, with most fraudulent transactio ns directed at retail websites. Europe (2%), led by Poland, Romania and Portugal, and Nort h America (1%), led by Mexico, showed fraud spread more evenly across retail, gaming, ga mbling, financial services, travel, logistics and telecommunications.

Individual cases illustrate the transnational reach of such schemes. The Federal Bureau of Investigation (n.d.) lists Shaileshkumar P. Jain and his co-conspirator, Bjorn Daniel Sundi n, as wanted for their alleged involvement in an international scareware operation. Betwee n December 2006 and October 2008, fake advertisements placed on legitimate companies' websites allegedly misled internet users in more than 60 countries into believing that their computers were infected with malware, inducing them to purchase more than one million b ogus software products and causing consumer losses of more than US$100 million.

It would be hard to guess at a number to represent cyber- crime and computer fraud lo sses on a global scale. Eugene Kaspersky, the Russian co-founder of anti-virus software mak er Kaspersky Labs, told an audience at a Dublin technology conference last month that he b elieves such a number ranges in the hundreds of billions of dollars. As reported by The Gua rdian, Kaspersky believes that a previous, widely cited estimate of $100 billion is far too lo w, and the truth is likely "many times more" than that amount. Kaspersky's projection is pr obably more accurate and may even be conservative, considering that the latest ACFE Repo rt to the Nations estimate of fraud (all fraud, not just online) points to more than a trillion d ollars in global loss.

Even more serious to consider is the fact that Kaspersky believes the security lapses af fecting organizations, and the sophisticated methods of exploiting them, create an environ ment where fraud might be the lesser of two major concerns. It is actually the threat of a cy ber terrorist attack one affecting infrastructure, financial centers or military targets that Ka spersky says is most troubling of all. For fraud examiners, the fight against online fraud mig

ht feel like an uphill battle. With every new and changing facet of technology, those who co mmit fraud through the Internet tend to innovate and remain ahead of investigators trying to catch them. On the road ahead, increased training and knowledge for anti-fraud professi onals will be critical mixed with a healthy dose of innovation of their own.

Dr. Wells noted that one technical innovation, biometric technology (which includes co ncepts such as face and voice recognition) could be a key to stemming the tide of online fra ud. “This science (of biometrics) is already quite well developed but currently under-utilize d,” Wells said. “I can envision a day in the not-too-distant future where, in order to claim m oney or other resources, you’ll have to prove scientifically that you are who you say you are . “That system, had it been employed, would have prevented billions of dollars in recent tax refund scams,” Wells added. “And that’s just one example.

Credit card and benefit frauds could be greatly reduced, too. As a matter of fact, nearly any fraud employing identity theft could all but be wiped out through the proper applicatio n of biometric resources. But using this technology must be balanced to protect the privacy of citizens.” No method of prevention is foolproof and fraudsters will be no doubt look for m ethods to overcome biometrics or other key controls that can hinder their efforts. But in the race to curb cyber- crime, any efforts that can slow the criminals down is a valuable and ne cessary endeavor. More than 20,000 fraud and cybercrimes are perpetrated every day, the f irst official estimates of the scale of the offences in the UK suggest. Research found there we re 5.1 million incidents of fraud in England and Wales in the last year, with 3.8 million victi ms. It indicates the category is the now most common form of crime.

In addition, there were an estimated 2.5 million incidents which fall under the Comput er Misuse Act, such as hacking attacks. There were an estimated 2.5 million incidents which fall under the Computer Misuse Act, such as hacking attacks. There were an estimated 2.5 m illion incidents which fall under the Computer Misuse Act, such as hacking attacks. The data also suggest that on average one in 12 adults have experienced fraud and one in 22 is a victi m of cyber fraud.

The disclosures prompted claims that the overall crime count is substantially higher th an previously thought, while police said they showed how the internet is "changing the nat ure of crime". Statisticians stressed that the figures for the categories are preliminary but th e number of fraud incidents is nearly a third higher than theft offences - the highest categor y in the established Crime Survey for England and Wales (CSEW) at 3.9 million. Around 1.4 million people suffered computer virus attacks, with almost 650,000 people reporting that t heir email or social media profile had been hacked.

Youth involvement is a recurring concern in both countries. In India, crime statistics released by the National Crime Records Bureau and discussed by Mahajan (2013) showed that, of 43,506 crimes attributed to juveniles and registered under the Indian Penal Code (IPC) and Special and Local Laws (SLL), 28,830 (about two-thirds) involved offenders aged 16–18 years. In Nigeria, internet fraud is frequently associated with young people, a pattern that studies link to socioeconomic pressures such as unemployment, poverty, urbanisation and peer influence Aborisade, (2023); Soares & Lazarus, (2024)and that is aggravated by persistently high youth unemployment (Olubusoye et al., 2023). Because young people are central to nation building

(Adeniyi, 1999), their involvement in cybercrime carries long-term economic and social costs.

The study is also urgent. Both countries are pursuing digital-economy strategies that depend on public trust in online transactions, and every additional fraud incident erodes that trust and raises the cost of doing business (Lonkar et al., 2025; Sule et al., 2023). The rapid growth of cybercrime, evident in India’s official statistics and in Nigeria’s recurrent legislative interventions, suggests that existing measures have not kept pace with offenders. Moreover, because a large share of offenders are young people, any delay in addressing the problem risks diverting a significant part of both countries’ human capital into criminal activity.

Despite this literature, three gaps remain. First, most studies analyse India or Nigeria in isolation (Saluja, 2024; Soares & Lazarus, 2024), and systematic comparisons of the two countries both large, youthful and rapidly digitising economies with distinct cybercrime profilesare scarce. Second, much of the existing work emphasises criminological or technical aspects (Loggen et al., 2024), whereas the economic consequences of cybercrime are usually mentioned only in passing, even though measuring these costs is recognised as methodologically challenging (Anderson et al., 2013).

Third, recent legal and institutional reforms, such as Nigeria's Cybercrimes (Prohibitio n, Prevention, etc.) (Amendment) Act, 2024 and India's Digital Personal Data Protection Ac t, 2023, have not yet been examined together from a comparative economic perspective. Th e novelty of this study therefore lies in a structured India–Nigeria comparison across comm on dimensions the scale and forms of cybercrime, economic losses, legal frameworks and e nforcement capacity that links the causes of youth involvement in cybercrime to its econom ic effects and to policy responses.

Accordingly, the objectives of this study are to examine the causes of cybercrime amon g young adults in India and Nigeria; to identify the effects of cybercrime on the economies o f India and Nigeria; and to propose appropriate solutions to the menace of cybercrime in th e study countries. In line with these objectives, the overall purpose of the study is to establi sh the effects of cybercrime on various stakeholders, namely individuals, companies, gover nment departments and business owners, in the countries under study.

Theoretically, the study contributes to the literature on the economics of cybercrime in developing countries by offering a comparative framework that can be applied to other em erging economies. Practically, its findings are expected to benefit policymakers, law-enforc ement agencies, financial institutions and businesses in India and Nigeria by identifying sha red vulnerabilities and transferable practices. The study also has implications for cybercrim e legislation, investigative capacity building, public awareness campaigns and youth emplo yment policy.

RESEARCH METHOD

This study uses a descriptive comparative desk-review design based on secondary data. The units of comparison are India and Nigeria, and the analysis is limited to documentary material already assembled in the manuscript concerning cybercrime, its economic consequences, and institutional responses in the two countries. The sources consist of documented scholarly written materials, legislation and other publications cited in the article. Because the original source set does not report a systematic search period, database strategy, or formal inclusion and exclusion criteria, these elements are not reconstructed or invented in this revision.

The analysis was conducted by organizing the available secondary evidence into common themes that permit comparison between India and Nigeria. The principal analytical dimensions are: the conditions associated with the escalation of cybercrime; forms of fraud and cyber offences; economic consequences for individuals, businesses, and public institutions; legal and evidentiary challenges; enforcement and investigative capacity; cyber-security and forensic skills; and proposed preventive or institutional responses.

Evidence concerning global losses is used as contextual material, while country-specific material is compared to identify similarities and differences relevant to the study objectives. The study does not generate primary survey, interview, experimental, or administrative data. Accordingly, the findings are interpreted as a synthesis of the secondary evidence available in the manuscript rather than as estimates of national prevalence or causal effects.

RESULT AND DISCUSSION

Cyber- crime is a crime perpetrated through electronic communication networ, particularly the internet. This menace is very rampant in youths within the age of fourteen to twenty-one and it had done incalculable damages to the image of our Nation. Cyber- crime

could be perpetrated through internet calls, sending of scam emails containing "get rich quick" proposals to entice unsuspecting victims. In the case of email, sometimes it comes in form of marriage proposal, unclaimed fund, donatio, lottery, help, bonanza, bank transaction notification / credit alert, etc. (Abubakari, 2024). Some of the youths send as many as 10,000 of such scam emails everyday while others send more to increase their chances of getting victims that will fall to their prey. Youths are proverbially referred to as leaders of tomorrow but how can they be true leaders if they engage in cyber- crime at their early age (Lazarus, Olaigbe, et al., 2023).

State Of Cyber Crime In India

Recent reports indicate that India is one of the top ten countries in the world for the incidence of cybercrime (Bruce et al., 2024). Yet other reports also indicate that spend on cyber and network security by Indian businesses is one of the lowest in the world. The debate is on-going in technology circles where the threats and risks are well understood. While conducting this research, a cyber -thriller, I met several people engaged in different aspects of cyber safety. Their stories corroborated the above mentioned reports. Online consumer fraud is increasing. Companies and governments are also facing threats, several leading to material losses, and a growing tribe of cyber forensics professionals in different cities are tracking down the shadowy culprits.

Yet the stories on cyber- crime that dominate Indian news are about Sony and Target hacks that happened in other countries and affected other people. True, there have been some local stories of cyber stalking, bullying and faked photo scandals affecting our youth and celebrities, and stories around morphed videos leading to riots and scandals. There is growing effort to create cyber safety awareness for consumers. But what about news of larger scale crime that affects both consumers and firms? The challenge, perhaps, lies in the awareness and acknowledgement of this in the broader network of stakeholders. Here could be some reasons why.

Latency And Lifecycle Of Ideas

Ideas, like products or companies, go through a lifecycle – latent at first, till they become obvious to someone. They are championed by the early adopters at first, till they become widespread. By the time a notion is accepted as a general principle, it perhaps loses some of its significance. Our Internet usage has been growing at a rapid pace over the past few years. But tens of millions of new internet users start every year, many of them over their mobile phone. Their first brush with the excitement of being online is beginning. Hence cyber- crime and awareness of the risks of the digital world are still seeping into our psyche.

Decision Making For Technology

Does it only seem like short while back that our companies and government were debating the usage of technology? Our IT industry grew through massive technology transformation projects for global clients. But domestic clients followed several years later. The last decade saw the debates around whether the operations, human resources, customer management and other functions needed to be technology enabled or not.

While the technology leaders were convinced that business efficiency would increase given technology usage, it took a long while for CEOs, CFOs, and the Board to be convinced. Today no one questions the need for technology. The need for security is already being spoken about in the digital forums led by technology leaders and vendors. The question is whether business decision makers are listening and understanding the issue yet.

Voids In A New Area Of Business

Cyber security is a new area, and like all new domains it faces gaps- not just in understanding and awareness of it, but also in the key enablers.

Legal And Penal Framework

The IT Laws under the Indian Penal Code were amended in 2008 to include hacking, data theft, identify theft, email spoofing and spreading of viruses or worms as punishable and bail-able offences. Cyber- crime cells have been established. Law firms are keenly trying to educate both the police and the judiciary on the technical intricacies and prevalence of cyber- crime. This is a new area for the governing and judicial bodies, without many precedents and will take some time before cyber- crime gets fully understood.

Burden Of Proof

While cyber- crime is a culpable offence, the challenge lies in the ability of an individual or an organisation to prove that a wrongdoing is taking place. An individual or consumer who has been conned may find it hard to prove that a crime has been committed. Even if it is a systemic crime where multiple card users of a particular bank have been scammed, the bank may not be willing to declare that its data and systems have been breached. The law does not mandate it. In cases of major data theft or hacking, companies or governments may not file an FIR because it may affect credibility or market economics. Without an FIR, neither the police nor the justice system can operate.

Tracking The Hacker

Cyber forensics is a growing field in India and several private companies have come up, leveraging the services of ethical hacker. If the malicious hacker is sophisticated and uses anonymous underground networks such as Tor, it becomes harder to trace the origin of an attack. It took all the might of the US government and its various monitoring agencies to track the trail to North Korea in the case of the recent hacking incident at Sony. Most organizations and governments might not have the required resources.

In the case where an individual or organization is identified as the culprit, the person could be residing in some other country, outside the jurisdiction of local authorities (Button et al., 2025). For example, the hacker could be located in Pakistan, buying malware tools from the US, spoofing server addresses of China and causing mayhem in India. It becomes impossible to react to civilian cases that affect individuals or businesses.

Lack Of Talent

India graduates a large number of people in engineering and computer science every year. But very few people are trained in cyber security and forensics. There are many candidates available for coding and testing type jobs. But cyber security requires advanced skills in testing and tracing, as well as a keen, independent analytical mind to piece together the puzzle. What's needed is a modern era Sherlock Holmes, indeed. Experts and businesses agree that there is a severe shortage of talent in the area (Furnell, 2021).

Manning The Internet Perimeters

Many large businesses today have multi-layered security environments, and not every hacker is sophisticated and technically advanced. Globally as well as in India, majority of breaches happen due to internal hackers (tech savvy employee turned hacker) or driven by internal staff, whether indirectly (through social engineering, to get access to passwords) or directly (through collusion with an employee, who allows access through the legal firewalls). A lot of financial and data theft happens this way (Lazarus et al., 2025). The average time it takes a firm to catch an internal hacker is several weeks. Sometimes it is a junior systems admin or tech help person. Sometimes it is a savvy executive.

It appears legitimate business transactions or siphoning off money, making it harder to catch. These stories never make it to the public domain. While Breach is fiction, it has been informed by stories of cyber- crime within India. Given the paucity of local case studies to spread awareness on cyber safety in India, perhaps narrative storytelling could be an easy way to let consumers and executives get a feel for the perils of our interconnected,

networked existence.

State Of Cyber Crime In Nigeria

Cyber- crime is an emerging trend that is rapidly growing in scope and frequently. The revolution in information and communication technology ICT had greatly promoted the scope and trend in cyber -crime in Nigeria. The world being a global village, Nigeria could not have been in isolation in embracing the usage of social media and internet's which are greater promoter of cybercrime to put it succinctly, cybercrime is a product of wrong usage or abuse of ICT or internet service.

Why The Escalation In Nigeria:

No doubt the menace of cybercrime in Nigeria has been on the increase due to some crucial factors, mostly bothering on lack of specific laws designed to address the problem. Most law enforcement agencies including the police are not prepared to deal with online crime due to the complex and intricate nature of the investigation couple with the rapid advancement of new technology. Our society continue to get more involved in the crime, while the public expects our law enforcement agencies to keep pace with modern technology as it affects the investigation and prosecution process, and by extension tackling crime in general. Cybercrime still remain a major cause of concern in Nigeria for many government security departments, and combating cyber threats are becoming harder to content with due to the sophisticated and complex manners in which cyber criminals are operating, and the poor investigative approaches by law enforcement agencies.

Economic Menace Of Cyber Crime:

While the escalation of cyber -crime could not be curtailed adequately by crime prevention agencies, the effects continue to bite hard on our economy, both locally and internationally. Aside from the social menace it is creating in our entire systems to a large extent, cyber -crime has thrown up a large number of 419 perpetrators in our economic system. Very easily people are able to commit economic crime through the internet by duping one another of large sum of money locally and internationally. Corporate internet fraud has been on the increase as even unscrupulous banking officials are conniving with outsiders to steal depositor's funds.

Aside from local economic sabotage and fraud, a large number of Nigerians particularly the youths are also engaged in perpetrating internet fraud by duping individuals and corporate institutions abroad through spurious economic deals (Lusthaus et al., 2025). Fraudulent practices through cybercrime has thrown up emergency millionaires, even billionaires in our economic system which is injurious to our economic growth as most of such funds acquired, illegally are not been used productively to promote the economy. Such funds could not be easily traced by law enforcement agencies. In deed economic sabotage resulting from cyber- crime cannot be over-emphasized.

Social Menace Of Cybercrime:

Another serious aspect of cyber- crime or social media abuse is how dubious relationship are easily courted or established, which often lead to disastrous ends, particularly amongst our youths (Lazarus, Whittaker, et al., 2023). We have seen instances where such relationship established through internet process ended up in untimely deaths of innocent people (male & female). Lots of social media links for social engagement had ended in disasters often creating bottle necks for law enforcement agencies due to lapses or lack of concrete laws in place to address the situation.

Nigeria Image:

In all of these, Nigeria's image has continuously been the worse for it. It has been seriously battered internally and externally (Lazarus & Button, 2022). Though cybercrime

is a global phenomenon, individual countries suffers the effects differently depending on what laws each country has in place to address the situation, as well as how effective their law and crime prevention agencies are able to curtail the menace. This is why the proposed urgent need for the establishment of the Nigeria Police Internet Crime Complaint Centre (NPIC3) in Nigeria, which will be in affiliation with the internet crime complaint centre of the United States of America (IC3), is most welcomed.

Also, the urgent inclusion of online Forensics Graphognomy course into the curriculum of Nigeria Police Education Unit, which will strategically enhance the know-how of methodologies of online scamming technicalities being used by cyber criminals thereby making investigation of cybercrime intelligence information gathering reports easier for law enforcement agencies, as otherwise stated above. Certainly, the approval of this proposal will enable the Nigeria Police readdress the emerging facts that have shown Nigeria to be one of the leading cybercrime perpetrators in the world, as earlier acknowledged by the National Security Adviser (NSA) Col. Sambo Dasuki (Rtd) on Wednesday March 20th 2013, edition of Leadership Newspaper. Because of the foregoing, the danger attached to cybercrimes as reflects on the online image of our country, has made it more difficult for Nigeria to engage in online business and other cyber related activities.

CONCLUSION

Cybercrime is an emerging trend that is rapidly growing in scope and frequently, creating economic and social consequences in India and Nigeria. The effects continue to bite hard on the economy, both locally and internationally, affecting individuals, businesses, government departments and business owners. Youth involvement, internet fraud, data theft, hacking, identity theft and fraud remain serious challenges, while poor investigative approaches, limited cyber-security and forensic skills, and difficulties in tracking offenders constrain effective responses. Computer users are therefore urged to take precautions when liaising with other people online and engaging in financial transactions.

Serious action is needed to protect cyber space as a national security requirement. Increased training and knowledge for anti-fraud professionals, stronger investigative capacity, public awareness, and legal and institutional responses are necessary. Addressing these challenges can strengthen cyber safety, reduce economic losses, protect individuals and organisations, and support safer use of internet services in India and Nigeria.

FUNDING

The authors state that no financial support has been received for the implementation of this research and/or the publication of this article.

CONFLICT OF INTEREST

The authors declare that this research was conducted without any commercial or financial relationship that could be interpreted as a potential conflict of interest.

AUTHOR CONTRIBUTION

Idris Muhammed Ango conceptualized the study, designed the descriptive comparative desk-review, and prepared the original draft of the manuscript. Salihu Ahmed and Bala Aliyu collected and organized the secondary sources, including scholarly materials, legislation and other publications on cybercrime in India and Nigeria. Muhammad Sani Umar contributed to the thematic analysis and comparison of the evidence between the two countries. Maimuna Muhammad Harande contributed to the review and editing of the manuscript. All authors have read and approved the final version of the manuscript and are accountable for its content.

GENERATIVE ARTIFICIAL INTELLIGENCE USAGE STATEMENT

The authors state that generative artificial intelligence (AI) was used in the preparation of this manuscript. The authors acknowledge the use of generative AI to help improve language clarity and improve the grammatical structure of the manuscript. The use was carried out in compliance with applicable ethical guidelines regarding the use and disclosure of generative AI in scientific research. Each author has made substantial intellectual contributions to this work. No generative AI tool was used to generate data, analyses, findings or conclusions, nor was any such tool listed as an author. The entire content of the manuscript has been carefully reviewed by the authors to ensure its accuracy, and the authors are solely responsible for the integrity and final content of the manuscript.

REFERENCES

Aborisade, R. A. (2023). Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition Towards Children's Involvement in Cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Abubakari, Y. (2024). Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters. *Journal of Economic Criminology*, *6*, 100112. https://doi.org/10.1016/j.jeconc.2024.100112

Adeniyi, P. O. (1999). *Youth and Nation building: A continue challenge in Nigeria.*

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE*, *19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

Button, M., Hock, B., Suh, J. B., & Koh, C. S. (2025). Policing cross-border fraud 'Above and below the surface': mapping actions and developing a more effective global response. *Crime, Law and Social Change*, *83*(1), 5. https://doi.org/10.1007/s10611-024-10186-2

Cooper, A. (1997). The Internet and sexuality: Into the next millenium. *Taylor & FrancisA CooperJournal of Sex Education and Therapy, 1997•Taylor & Francis*, *22*(1), 5–6. https://doi.org/10.1080/01614576.1997.11074164

Elster, J. (1990). *Merton's functionalism and the unintended consequences of action.*

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Lazarus, S. (2025). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity. *Deviant Behavior*, *46*(4), 456–480. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., Button, M., Garba, K. H., Soares, A. B., & Hughes, M. (2025). Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. *Journal of Economic Criminology*, *7*, 100128. https://doi.org/10.1016/j.jeconc.2025.100128

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, *2*, 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, *52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2025). Tackling digital payment frauds: a study of consumer preparedness in India. *Journal of Financial Crime*, *32*(2), 257–278. https://doi.org/10.1108/JFC-01-2024-0029

Lusthaus, J., Holt, T. J., Levi, M., Kleemans, E., & Leukfeldt, E. R. (2025). The evolution of Nigerian cybercrime: Two case studies of UK-based offender networks. *European Journal of Criminology*, *22*(4), 557–577. https://doi.org/10.1177/14773708251329695

Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, *30*(6), 1653–1663. https://doi.org/10.1108/JFC-08-2022-0185

Olubusoye, O. E., Salisu, A. A., & Olofin, S. O. (2023). Youth unemployment in Nigeria: nature, causes and solutions. *Quality & Quantity*, *57*(2), 1125–1157. https://doi.org/10.1007/s11135-022-01388-8

Saluja, S. (2024). Identity theft fraud- major loophole for FinTech industry in India. *Journal of Financial Crime*, *31*(1), 146–157. https://doi.org/10.1108/JFC-08-2022-0211

Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies*, *37*(4), 328–351. https://doi.org/10.1080/1478601X.2024.2429088

Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, *30*(6), 1557–1574. https://doi.org/10.1108/JFC-07-2022-0157