

THE MENACE OF FRAUD-BASED CYBERCRIME AND NIGERIA'S GLOBAL CYBERSECURITY PROFILE

Daniel Uchechukwu Lawrence

Department of Political Science
Nnamdi Azikiwe University, Awka
dannyuche2014@gmail.com

ORCID: <https://orcid.org/0009-0005-8278-4455>

Okafor Uzodimma C. PhD

Department of Political Science
Nnamdi Azikiwe University, Awka
cu.okafor@unizik.edu.ng

ORCID: <https://orcid.org/0000-0003-2984-9318>

Ignatius Ifesinachi Ngini PhD

Department of Political Science
Nnamdi Azikiwe University, Awka
ig.ngini@unizik.edu.ng

ORCID: <https://orcid.org/0009-0007-9465-9795>

ABSTRACT

Amid escalating global concerns over cybercrime, Nigeria's digital space has emerged as both a site of innovation and a center of fraudulent practices associated with "Yahoo Boys," posing serious implications for its global reputation. This study investigates the relationship between cyberfraud and Nigeria's cybersecurity profile between 2015 and 2024, employing Kenneth Boulding's Image Theory of International Relations (1959) as a theoretical framework. Using an explanatory research design, it applies a mixed-methods approach, combining Key Informant Interviews (KII) with secondary data drawn from official reports, scholarly works, and media sources. Content analysis highlights thematic connections between Nigeria's cybersecurity performance and the persistence of cyber fraud. Findings reveal a paradox: Nigeria's Global Cybersecurity Index (GCI) improved significantly from 0.441 in 2015 to 84.76 in 2020, before experiencing a slight decline in 2024. Despite this progress, Nigeria's global image remains overshadowed by fraud-based cybercrime, as reflected in its recurring presence in the FBI's IC3 complaints and the 2024 World Cybercrime Index. The study recommends enhanced collaboration across government, private, and community actors for intelligence sharing, the integration of digital literacy and ethics in education, improved law enforcement capacity, and the modernization of cybercrime legislation to align with international frameworks.

INTRODUCTION

The twenty-first has seen a rapid technological advancement, with increasing dependence on information and communications technology (ICT) by individuals, organizations, and governments across the globe. In Nigeria, this digital transformation is particularly evident in the exponential growth of internet users, which rose from 141.9 million in 2021 to 163.8 million in 2023 (Sulaimon, 2024). Despite the evident advantages of digital expansion in enhancing connectivity and socio-economic productivity, it has also exposed Nigeria's cyberspace to growing cyber-related threats. As more Nigerians come online, the cyberspace has become increasingly weaponized by individuals exploiting technological tools for fraudulent purposes. This development threatens the integrity of Nigeria's cybersecurity framework and global image (Abdul-Rasheed et al., 2016; Jaiyeola, 2024). The growing incidence of internet fraud, commonly referred to as "Yahoo Yahoo" in Nigerian parlance, has emerged as a dominant form of cybercrime in the country (Ojedokun & Ilori, 2021). These fraudulent schemes, ranging from phishing and identity theft to romance and business email compromise scams, have not only wreaked havoc on victims globally but have also severely damaged Nigeria's international reputation (EFCC, 2023). High-profile cases, such as those involving Obinwanne Okeke and Ramon Abbas (popularly known as Hushpuppi), have attracted global attention and underscored the scale and sophistication of cybercrime operations linked to Nigeria (Ayub & Akor, 2022; US DOJ, 2022). The financial and reputational consequences of these criminal acts have made Nigeria a focal point in global cybersecurity discourse.

In 2023 alone, the FBI's Internet Crime Complaint Center (IC3) recorded 1,779 cyberfraud complaints linked to Nigeria, and the country was ranked 5th in the inaugural World Cybercrime Index, following global cybercrime hubs such as Russia and China (FBI, 2023; Bruce et al., 2024). These metrics not only illustrate the scale of Nigeria-linked cybercrime but also point to the urgent need for more robust cybersecurity governance, both nationally and in collaboration with international partners. Although various Nigerian administrations have

attempted to counter this reputational crisis through rebranding initiatives and cybersecurity legislation, most recently the 2024 Cybercrime Act, fraudulent activities of cybercriminals continue to flourish (Aliyu, 2021; Omogbolagun, 2023). The persistence of these crimes raises serious questions about the efficacy of current regulatory frameworks and enforcement mechanisms. It also exposes a critical gap between Nigeria's technological expansion and its preparedness to secure the digital space. Against this backdrop, this study seeks to critically examine the impact of cyberfraud on Nigeria's global cybersecurity profile from 2015 to 2024.

LITERATURE REVIEW

Cyberfraud, a critical subset of the broader phenomenon of cybercrime, has garnered increasing scholarly attention due to its rising prevalence and the significant socio-economic risks it poses. Conceptually, fraud according to Singleton and Singleton in Jegede (2014) and echoed by the Nigerian Financial Intelligence Unit (2023) involves the strategic use of deception, through surprise, trickery, or manipulation, to unjustly acquire financial or material advantage. In the digital space, this deceit known as cyberfraud, manifest where the internet and computer technologies are employed to defraud individuals or organizations, often resulting in substantial financial harm. Scholars such as Smyth and Carleton (2011) identify various manifestations of cyberfraud, including fraudulent online transactions, contractual breaches, and the theft of digitally transmitted funds. Dzumira (2014) established the link between the proliferation of electronic banking and the escalation of financially motivated cyber-attacks. Furthermore, Levi and Burrows in Ogunleye et al. (2019) offer a better understanding of victimhood in cyberfraud, distinguishing between direct (primary) and indirect (secondary) victims, thereby highlighting the layered impact of such crimes. Collectively, these scholarly perspectives frame cyberfraud not merely as a technical infraction but as a complex socio-technical threat embedded within broader digital vulnerabilities. Thus, cyberfraud can be defined as the deliberate use of digital or internet-enabled technologies to deceive individuals, organizations, or systems for the purpose of illicit financial or material gain, typically involving manipulative tactics such as misinformation, identity misrepresentation, or unauthorized access to digital assets. It encompasses a spectrum of activities, ranging from phishing and online contract breaches to fraudulent fund transfers, and often implicates both direct victims and secondary entities such as financial institutions. Central to cyberfraud is the strategic exploitation of trust and system vulnerabilities within cyberspace, making it a dynamic and evolving threat within the broader domain of cybercrime.

The increasing association of Nigeria with cybercrime, particularly in the context of financial fraud, has not only tarnished the country's global image but also exposed significant weaknesses in its cybersecurity infrastructure. Makeri (2017) notes that prior to the early 2000s, Nigeria was rarely linked to cyber-related offenses, but the advent of widespread internet access catalyzed a dramatic shift. Cybercriminals began to innovate techniques that outpaced the nation's limited cyber-policing capabilities. As highlighted by scholars such as Jegede (2014) and Ekolama et al. (2022), technological advancements in Nigeria have inadvertently empowered cybercriminals with tools for document falsification, data manipulation, and sophisticated intrusion techniques. The easy accessibility of software tools, personal computing devices, and public Wi-Fi services, particularly in unregulated environments such as cyber cafés, has enabled the rapid proliferation of fraudulent activities. Meanwhile, cybercrime-related losses continue to escalate, with Ekolama et al. (2022) estimating global losses exceeding \$400 billion, and projecting a potential \$6 trillion loss for Nigeria by 2030 if structural cybersecurity issues remain unaddressed. This development has placed Nigeria under increasing international scrutiny, framing its cybersecurity crisis as both a national threat and a global concern.

Nigeria's cybersecurity challenges are further accentuated by global indices and reports, which reveal structural vulnerabilities in both public and private digital infrastructures. The International Institute for Strategic Studies (2023) highlights systemic gaps in cybersecurity governance, noting Nigeria's fluctuating rankings on the Global Cybersecurity Index—57th in 2018 and 47th in 2020, despite persistent cyberattacks on critical national assets and cloud infrastructures. Moreover, a recent World Cybercrime Index places Nigeria as the fifth most significant source of cybercrime globally, behind only Russia, Ukraine, China, and the United States (Akintaro, 2024). This ranking is alarming, given that Nigeria lacks a comprehensive national cyber threat intelligence framework, and coordination between law enforcement and ICT regulators remains fragmented. The cybersecurity vacuum has created fertile ground for cybercriminals, who leverage weak digital identity verification systems, outdated security protocols, and insufficient legislative implementation. This shows the urgency of institutionalizing secure digital identity systems and bolstering national cyber incident response capacities to protect Nigeria's digital economy.

THEORETICAL EXPOSITION

This study is anchored on the Kenneth Boulding's *Image Theory of International Relations* (1959). The theory posits that the conduct of states on the world stage is not necessarily grounded in objective reality, but rather shaped by the mental images or cognitive representations they hold of themselves and other actors. According to

Boulding, these images, which may include conceptions such as allies, enemies, or imperialists, are shaped by past experiences, cultural narratives, and ongoing interactions. The central tenet of the theory is that state behaviour is determined less by material conditions and more by the psychological impressions and symbolic meanings attributed to others in the system, which form cognitive schemas that guide foreign policy choices.

Boulding also makes a key distinction between *image* and *message*: the former refers to the internalized perception held by a state, while the latter encompasses the outward signals—diplomatic acts, leadership behaviour, media narratives, and even citizen interactions—that can shape or reshape such images. These messages play a crucial role in the dynamic process of image construction and revision in international relations. Boulding argues that states consciously engage in image-making to cultivate favourable international reputations, using tools like diplomacy and public relations, especially in today’s media-driven world. While the theory does not deeply account for the influence of domestic political ideologies or grassroots digital activism in shaping state images, it remains a foundational contribution to the understanding of how perceptions govern state behaviour and interactions in global affairs.

Applying the relevance of the theory to this study, Nigeria’s global image is not formed solely by objective security metrics but through the interpretive lens of other states and international bodies influenced by persistent reports of cybercrime originating from within its borders. These actions, constituting the message, emanating from state actors’ inaction, poor regulatory frameworks, and publicized cases of online fraud, contribute to a deteriorating image of Nigeria as a cyber-insecure state. This unfavourable image then influences Nigeria’s ranking in global cybersecurity indices, as it is perceived as lacking credibility, control, and capacity in cyberspace governance.

METHOD

This study employed an explanatory research design Utilizing a mixed-method approach, data were collected from both primary and secondary sources. The primary data came from Key Informant Interviews (KII), while secondary data were sourced from official reports, media coverage, and academic publications, offering contextual evidence to support interview findings. For analysis, the study adopted content analysis to examine patterns and themes in fraud-related cybercrime discourse and its correlation with Nigeria’s cybersecurity ranking.

ANALYSIS OF FINDINGS

Between 2015 and 2023, the FBI’s IC3 documented millions of cybercrime complaints worldwide, identifying global hotspots based on complainants’ geographic locations (Federal Bureau of Investigation, 2015). Across these years, the IC3 reports consistently revealed that most reported internet crimes were fraud-related, encompassing offenses such as identity theft, phishing, credit card fraud, business email compromise (BEC), romance scams, charity scams, and other variants of financial deception (Federal Bureau of Investigation, 2015–2023). Among the notable trends identified in these reports is Nigeria’s evolving role in global cybercrime. In 2015, the FBI ranked Nigeria as the third most reported source of cybercrime complaints globally, accounting for 2.2% of complaints and financial losses of approximately \$275 million from over 8,000 cases (Federal Bureau of Investigation, 2015). The group widely known as “Yahoo Boys” was cited for its high-level involvement in internet fraud, earning Nigeria the label of the third most dangerous cybercrime group globally (Suleman, 2023).

However, by 2016, while complaints had surged to nearly 299,000 globally with losses exceeding \$1.3 billion, Nigeria’s position dropped to 19th with only 188 complaints (Federal Bureau of Investigation, 2016). Between 2017 and 2019, Nigeria was absent from the top 20 countries in IC3 rankings, with South Africa emerging as the only African nation consistently ranked 13th (Federal Bureau of Investigation, 2017–2019). In 2020, as global complaints rose to 791,790 and losses reached \$4.2 billion, Nigeria reappeared in the 16th position with 443 complaints (Federal Bureau of Investigation, 2020). The following two years, 2021 and 2022, saw Nigeria once again fall off the top 20 list, leaving South Africa as the sole African country represented (Federal Bureau of Investigation, 2021, 2022). However, in 2023, Nigeria re-entered the list at 17th place with 1,779 complaints, coinciding with a record 880,418 global complaints and an unprecedented \$12.5 billion in financial losses (Federal Bureau of Investigation, 2023).

Table 1: Federal Bureau of Investigation Internet Crime Report (2015-2023)

Year	Total Annual Complaints Received by FBI’s IC3	Economic Loss	Nigeria’s Ranking on Global Cybercrime Complaints Location	Total Complaints from Nigeria
2015	Over 8,000	Nearly \$275 million	3rd out of 5 top countries	Not specified
2016	298,728	Over \$1.3 billion	19 th out of 20 top countries excluding the United States	188

2017	301,580	\$1.4 billion	Nigeria is not ranked in the top 20 countries	Not specified
2018	351,937	Over \$2.7 billion	Nigeria is not ranked in the top 20 countries	Not specified
2019	467,361	Over \$3.5 billion	Nigeria is not ranked in the top 20 countries	Not specified
2020	791,790	\$4.2 billion	16 th out of 20 top countries excluding the United States	443
2021	847,376	\$6.9 billion	Nigeria is not ranked in the top 20 countries	Not specified
2022	800,944	\$10.3 billion	Nigeria is not ranked in the top 20 countries	Not specified
2023	880,418	\$12.5 billion	17 th out of 20 top countries excluding the United States	1,779

Source: Federal Bureau of Investigation (2015-2023)

In 2024, the inaugural *World Cybercrime Index* was released, providing the first comprehensive global ranking of countries based on their level of cybercrime threat. This index was the outcome of a rigorous three-year survey led by an international research team composed of 92 leading cybercrime experts from across the globe, all actively engaged in cybercrime intelligence and investigative work (University of Oxford, 2024). The *World Cybercrime Index* aims to identify key global hotspots of cybercrime by assessing and ranking the most prominent national sources of cybercriminal activity. According to the findings, Nigeria was ranked fifth among the world's primary sources of cybercrime, receiving a World Cybercrime Index Score of 21.28. It followed Russia, which topped the list, as well as Ukraine, China, and the United States, which ranked second, third, and fourth respectively (Bruce et al., 2024; University of Oxford, 2024). The remaining countries that completed the top ten global cybercrime hotspots were Romania, North Korea, the United Kingdom, Brazil, and India.

Fig. 1: World Cybercrime Index



Source: University of Oxford (2024)

A high prevalence of cybercrime within a country often indicates weaknesses in its digital infrastructure and reflects the perceived level of governmental commitment to implementing effective cybersecurity measures. Between 2015 and 2024, data from the FBI's Internet Crime Complaint Centre (IC3) and the World Cybercrime Index consistently positioned Nigeria as a leading actor in fraud-related cybercrimes, both within Africa and on the global stage. This persistent ranking has negatively influenced international perceptions of Nigeria's efforts to secure its digital ecosystem, highlighting deficiencies when measured against key global cybersecurity indicators and benchmarks.

Since 2015, the International Telecommunication Union (ITU), a specialized agency of the United Nations for information and communication technologies, has assessed national commitments to cybersecurity through its Global Cybersecurity Index (GCI). The ITU evaluates countries across five critical pillars: (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation (International Telecommunication Union, 2015). Nigeria's cybersecurity performance has varied significantly over the years. In the 2015 GCI report (based on 2014 data), Nigeria scored 0.441, ranking 14th globally out of 226 countries and 4th in Africa (ITU, 2015). Although the 2017 index (based on 2016 data) recorded an improved score of 0.569, Nigeria fell to 46th globally while maintaining its 4th place in Africa (ITU, 2017). The 2018 index

(based on 2017 data) showed further improvement in score to 0.650, but a drop in global rank to 57th and 5th place in Africa (ITU, 2018). A notable recovery was recorded in the 2020 index (based on data from 2018–2019), with Nigeria scoring 84.76 on a revised scale, placing it 47th globally and 4th in Africa (ITU, 2020). The 2024 GCI report (Fifth Edition), based on data from 2023–2024, introduced a tier-based ranking system. Nigeria was classified as a Tier-3 country, scoring highest in legal measures with 19.52 out of 20 points (Ibeh, 2024; ITU, 2024). According to the ITU, countries in Tier-3 typically score between 55 and 85, reflecting progress in digital service expansion and internet access, but with remaining gaps in integrating cybersecurity into broader digital inclusion goals (Ibeh, 2024; ITU, 2024).

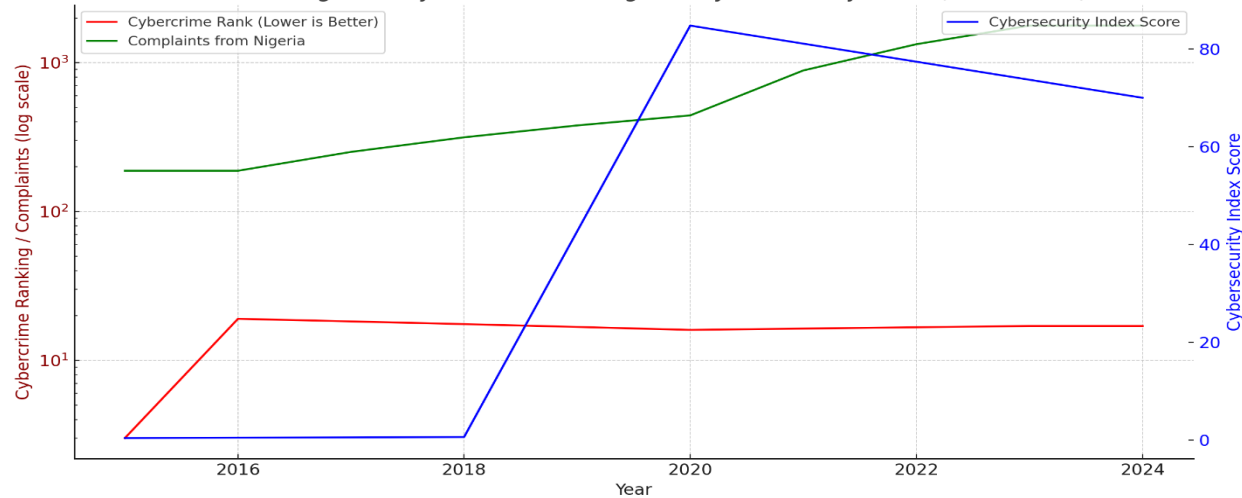
Table 2: International Telecommunication Union Cybersecurity Index Reports

Year of Report	Edition	Data Collection Period	Index Score	Global Ranking (Out of Total Countries)	African Region Ranking	Notable Details
2015	First Edition	2014	0.441	14 out of 226	4	-
2017	Second Edition	2016	0.569	46 out of 193	4	-
2018	Third Edition	2017	0.650	57 out of 193	5	-
2020	Fourth Edition	2018–2019	84.76	47 out of 194	4	-
2024	Fifth Edition	2023–2024	55–85	Tier-3	Not applicable	Adopted tier ranking system; Nigeria scored 19.52/20 in legal measures and was categorized as Tier-3 (score: 55–85).

Source: International Telecommunication Union (2015-2024)

The evolving relationship between Nigeria’s annual cybercrime complaint figures, its global cybercrime ranking, and its cybersecurity index from 2015 to 2024 reflects both growing concerns and emerging prospects. Nigeria’s position among the world’s leading sources of cybercrime has fluctuated notably during this period, beginning as the 3rd most implicated country in 2015, then improving to 19th in 2016, and largely maintaining a lower international profile in the years that followed, apart from 2020 and 2023, when it ranked 16th and 17th respectively. Although Nigeria was absent from the top 20 cybercrime source countries from 2017 to 2019, as well as in 2021 and 2022, it continues to be regarded as a significant actor in global cybercrime. This persistent relevance is underscored by its ranking as the 5th most prominent country on the World Cybercrime Index in 2024.

Chart 1: Trends in Nigeria’s Cybercrime Ranking and Cybersecurity Index (2015-2024)
Trends in Nigeria's Cybercrime Ranking and Cybersecurity Index (2015-2024)



Source: International Telecommunication Union (2015-2024)

Empirical data indicates that Nigeria’s cybersecurity index experienced substantial improvement between 2015, when it recorded a score of 0.441, and 2020, with a markedly higher score of 84.76. However, a slight decline was noted in the 2024 estimate. This progression suggests a growing commitment to cybersecurity initiatives over time, particularly following the enactment of the Cybercrime (Prohibition, Prevention, etc.) Act in 2015. Despite

these advances, Nigeria continues to rank prominently as a significant source of cybercrime both within Africa and on the global stage. This persistent trend highlights enduring structural and institutional vulnerabilities which, if left unaddressed by the government and relevant stakeholders, may continue to perpetuate negative global perceptions of the country

The comments of some interview respondents lend credence to the findings of this study. According to Chukwuebuka C. Ume-Ezeoke:

An increasing number of Nigerians involved in cybercrime and being victims of cybercrime have negatively impacted the country's ranking on international cybercrime perception indexes, often placing the country in an unfavourable light (*Cybersecurity expert at CED Technologies, London, United Kingdom, LinkedIn communication, July 17, 2024*).

In the same vein, *Respondent A*, a law enforcement officer offered a similar opinion:

Unfortunately, the illegal activities of a few individuals within Nigeria's cyberspace have cast a damaging shadow over the country's reputation. The activities of cybercriminals in Nigeria, particularly those in different forms of internet fraud have placed Nigeria as a country among the major sources of cybercrime in Africa and the world. This continues to make efforts being made by the government in Nigeria to make our cyberspace safe for all look insignificant (*Economic and Financial Crimes Commission (EFCC) officer, Abuja, e-mail communication, April 21, 2024*).

These perspectives underscore the detrimental effects of cybercrime, especially fraud-related offences, on Nigeria's international reputation, as both the participation of Nigerians in such criminal activities and their experiences as victims contribute significantly to shaping a negative global perception of the country.

CONCLUSION AND RECOMMENDATIONS

Nigeria's trajectory in global cybercrime rankings, beginning as the third-highest source of FBI IC3 complaints in 2015 and ultimately ranking fifth in the inaugural World Cybercrime Index, reflects both the country's significant role in fraud-related online offenses and the uneven progress of its cybersecurity infrastructure. Improvements in Nigeria's Global Cybersecurity Index scores, rising from 0.441 in 2015 to 84.76 in 2020 before a slight decline in 2024, demonstrate growing legal and organizational commitments, yet persistent gaps remain in technical measures and public-private cooperation. These empirical trends, corroborated by expert observations that ongoing cybercriminal activities, most notably by groups like the "Yahoo Boys", continue to undermine international confidence in Nigeria's digital governance. This reveals the urgent need for comprehensive, multi-stakeholder strategies to bolster cyber resilience and rehabilitate the nation's global reputation. Based on the findings, it is recommended that:

- i. The Nigerian government should establish robust, institutionalised partnerships between public agencies, private sector actors (especially in tech and finance), academia, and civil society to enhance proactive cyber threat detection and mitigation. This collaboration should focus on intelligence sharing, coordinated response mechanisms, and the development of indigenous cybersecurity solutions.
- ii. Also, given the prominence of youth involvement in cyber fraud, the government must invest in nationwide digital literacy campaigns and job-oriented ICT training programmes. Embedding cybersecurity ethics in school curricula and launching targeted mentorship or tech incubation programmes can redirect tech-savvy youths from cybercrime to innovation-driven entrepreneurship.
- iii. Lastly, law enforcement agencies like the EFCC and the cybercrime unit of the Nigerian Police Force, should be equipped with advanced digital forensic tools and continuous training to keep pace with evolving cybercrime tactics. Moreover, Nigeria must deepen international cooperation by aligning its cybercrime laws and enforcement practices with global standards (e.g., the Budapest Convention), facilitating joint investigations and extradition of transnational cybercriminals.

REFERENCES

- Abdul-Rasheed, S. L., Lateef, I., Yinusa, M. A., & Abdullateef, R. (2016). Cybercrime and Nigeria's external image: A critical assessment. *Africology: The Journal of Pan African Studies*, 9(6), 119–132.
- Akintaro, S. (2024, April 12). Nigeria ranks 5th in global cybercrime index. *Nairametrics*. <https://nairametrics.com/2024/04/12/nigeria-ranks-5th-in-global-cybercrime-index/>
- Aliyu, S. A. (2021, September 2). Change begins with me, more than a political slogan. *Tribune Online*. https://tribuneonlineng.com/change-begins-with-me-more-than-a-political-slogan/#google_vignette
- Ayub, A. O., & Akor, L. (2022). Trends, patterns and consequences of cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences*, 5(1), 241–262.
- Boulding, K. E. (1959). National images and international systems. *Journal of Conflict Resolution*, 3(2), 120–131. <https://doi.org/10.1177/002200275900300204>

- 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>
- 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>
- Dzomira, S. (2014). Electronic payments' awareness and adoption in Nigeria. *International Journal of Business and Economic Development*, 2(1), 75–90.
- EFCC. (2023). EFCC decries non-release of budgetary allocation, demands adequate funding. *Arise News*. <https://www.arise.tv/efcc-decries-non-release-of-budgetary-allocation-demands-adequate-funding/>
- Ekolama, N. A., Adebayo, A., & Ayibakuro, I. (2022). Impact of cybercrime on Nigeria's economic growth and security. *Journal of Social and Development Studies*, 15(3), 45–61.
- Federal Bureau of Investigation (2015). 2015 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2015_IC3Report.pdf
- Federal Bureau of Investigation (2016). 2016 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2016_IC3Report.pdf
- Federal Bureau of Investigation (2017). 2017 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf
- Federal Bureau of Investigation (2018). 2018 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf
- Federal Bureau of Investigation (2019). 2019 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf
- Federal Bureau of Investigation (2020). 2020 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf
- Federal Bureau of Investigation (2020). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Federal Bureau of Investigation (2021). 2021 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf
- Federal Bureau of Investigation (2022). 2022 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf
- Federal Bureau of Investigation (2023). 2023 internet crime report. *Internet Crime Complaint Centre (IC3)*. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
- Ibeh, R. (2024). Cybersecurity Index: Nigeria Among Tier-3 Countries – ITU. *Leadership Newspaper*. <https://leadership.ng/cybersecurity-index-nigeria-among-tier-3-countries-itu/>
- International Telecommunication Union (2015). Global Cybersecurity Index & Cyberwellness Profiles April 2015. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
- International Telecommunication Union (2017). Global Cybersecurity Index (GCI) 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
- International Telecommunication Union (2018). Global Cybersecurity Index (GCI) 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- International Telecommunication Union (2020). Global Cybersecurity Index 2020. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>
- International Telecommunication Union (2024). Global Cybersecurity Index 2024. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>
- Jaiyeola, T. (2024, March 19). Nigeria's internet usage up 38% on smartphone uptake. *Business Day*. <https://businessday.ng/technology/article/nigerias-internet-usage-up-38-on-smartphone-uptake/>
- Jegade, E. A. (2014). Cyber fraud, global trade, and youth crime burden: Nigerian experience. *Afro Asian Journal of Social Sciences*, 5(4), 1-21.
- Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology*, 48, 293-318.
- Makeri, Y. A. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), 315-321.
- Nigerian Financial Intelligence Unit (NFIU) (2023). Money laundering typologies through fraud in Nigeria. https://www.nfiu.gov.ng/home/downloadfile?filepath=c%3a%5cnfiu%5cwwwroot%5cdocuments%5ctml%5cmltfin_l0ajr2
- Ojedokun, U. A., & Ilori, A. A. (2021). Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria. *International Journal of Criminal Justice*, 3, 1–24.
- Omogbolagun, T. (2023, November 22). Senate laments Nigeria's loss of \$500m annually to cybercrime. *Punch*. <https://punchng.com/senate-laments-nigerias-loss-of-500m-annually-to-cybercrime/>

- Smyth, S. M., & Carleton, R. (2011). *Measuring the extent of cyber fraud: A discussion paper on potential methods and data sources*. Public Safety Canada.
- Sulaimon, A. (2024, February 24). FULL LIST: Lagos, Kaduna, others top Nigeria's internet users. <https://punchng.com/full-list-lagos-kaduna-others-top-nigerias-internet-users/>
- Suleman, L. (2023, February 2). Social media users compare internet fraudsters to Nigerian politicians. *London School of Economics and Political Science*. <https://blogs.lse.ac.uk/africaatlse/2023/02/02/social-media-users-compare-internet-fraudsters-to-nigerian-politicians/>
- University of Oxford (2024, April 10). World-first "Cybercrime Index" ranks countries by cybercrime threat level. <https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level>
- US Department of Justice (2022, November 7). Nigerian man sentenced to over 11 years in federal prison for conspiring to launder tens of millions of dollars from online scams. *U.S. Attorney's Office, Central District of California*. <https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions>