The Overview of Cybercrime and Cyber Security in Nigeria and Its Future Trends

Aminu Muhammad Auwal (i.elameenu@gmail.com)
University of Jos

Research Article

Keywords: Cybercrime, Cyber security, Nigeria, Computer Network

Posted Date: September 20th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3307532/v2

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract

The prevalence of cybercrimes in Nigeria has exhibited a consistent upward trajectory in recent years. This paper aims to offer a comprehensive assessment of the rate of cybercrime and cybersecurity incidents in Nigeria over a specified period.

The study utilizes data sourced from the Economic and Financial Crime Commission (EFCC) as well as a distributed survey administered to a diverse cohort of students, staff, and workers, employing basic statistical analysis and nearest neighbour analysis.

The study's findings reveal a significant surge in cybercrime rates in recent times, particularly within sectors encompassing social, financial, and educational domains, among others. The findings also underscore the persistent increase of cybercrime over time, which is largely attributed to inadequate action from government bodies, stakeholders, and regulatory agencies.

Consequently, it is recommended that law enforcement agencies and regulatory entities intensify their efforts to monitor and address these criminal activities. Ultimately, proactive initiatives should be directed towards safeguarding the most vulnerable demographic groups against cybercrime victimization.

Introduction

Cybercrimes have emerged as prevalent social issues within Nigeria, encompassing a range of illicit activities conducted using computers or networks. The term "cybercrime" encapsulates a spectrum of unlawful actions, employing computer technology as a tool, target, or platform for their execution (Moulton, 2010). Nzekor (n.d.) further defines the term to encompass an amalgamation of criminal activities tied to computers or networks, including e-fraud, e-pedophilia, and e-sexual grooming. The multifaceted nature of cybercrime has sparked diverse discussions, often approached from varied angles, each revealing distinct perspectives. Notably, since the late 1900s, studies such as those by Laura (1995) have illuminated the transformation of cybercrimes from conventional offenses to threats that impinge on the national security of nations, including technologically advanced ones such as the United States.

Past researchers have diligently scrutinized cybercrime, yielding valuable insights. For instance, Erin et al. (2020) highlighted that recent high-profile cyber-attacks on financial institutions have triggered global discussions among board executives, regulators, risk professionals, and scholars. Additionally, researchers have examined cybercrime not only within Nigeria but also across the broader African landscape. Despite escalating concerns about cybercrime, Africa as a continent has been relatively sluggish in its response to the escalating challenges in the cyberspace. While some nations have yet to enact comprehensive cybercrime legislation, only a limited few have ratified the African Union Convention on Cyber Security and Personal Data Protection (Ndubueze, 2020).

In the Nigerian context, several studies underscore the escalating cybercrime scenario. Statistical analysis from around 2013 positions Nigeria as the 43rd among EMEA nations and third among global leaders in cybercrime (Frank, 2013). A report by the IC3 under the Federal Bureau of Investigation (FBI) in 2020 ranked Nigeria as the 16th among countries grappling with significant cybercrime issues. Furthermore, Queen's report (2022) highlights the exponential rise in cybercrime incidents, with over 2000 and about 3000 convictions recorded in 2021 and 2022, respectively. Despite these insights into cybercrime offenders, a significant gap remains - the victim's perspective, a comprehensive overview, and the current incidence rate in Nigeria remain unexplored.

The present paper endeavors to delve into the realm of Cybercrime and Cybersecurity, elucidating their concepts while proposing effective strategies to mitigate associated challenges. By providing an overarching view of cybercrime and delineating its frequency within Nigeria, this study addresses significant gaps within the existing literature. Notably, prior research often focuses on foreign contexts, leaving Nigerian cybercrime studies sparse and inconclusive. Consequently, this paper embarks on a holistic exploration, beginning with a literature review encompassing theory and previous research on cybercrime. Subsequently, the study expounds on the employed methodologies, followed by the presentation of results, discussions, and conclusions.

Literature Review

2.1 Cybercrime

The term "cybercrime" was coined by Peter Cassidy, Secretary General of the Anti-Phishing Working Group, to distinguish computer programs specifically designed to orchestrate financial crimes from other malicious software (Shehu, 2014). Cybercrime encompasses a range of activities that exploit computers and the internet for fraudulent purposes. These activities span from identity theft to money laundering, targeting victims via diverse strategies (Halder & Jaishankar, 2011). This definition, however, limits cybercrime to internet-aided offenses directed at individuals and groups (Jack & Ene, 2016).

A more comprehensive perspective classifies cybercrime as crimes committed on the internet or through computers, involving either the use of the computer as a tool or the computer's owner as a target (Kamini, 2011). This classification encapsulates a wide array of offenses, including fraud, forgery, identity theft, phishing, spam, and more, thereby highlighting the intertwining of technology and victims in all cybercrimes (Kamini, 2011).

2.2 Cybercrime in Nigeria

In Nigeria, cybercrime refers to criminal activities conducted using computers, the internet, and digital devices, either by attacking computer systems or utilizing them as tools (Jack & Ene, 2016). The country faces a multitude of cybercrime challenges, including computer-related and internet fraud, hacking, identity theft, phishing, child sexual exploitation, malware attacks, and more (Cybercrime Act, 2015).

Nigeria's policy response to cybersecurity and cybercrime includes the Cybercrime Act of 2015, which outlines offenses punishable by law, ranging from unauthorized access to computer systems to cyber terrorism (Cybercrime Act, 2015). Studies underline the severity of cybercrime incidents in Nigeria. Reports from the Internet Crime Complaint Centre revealed Nigeria ranking third among sources of global cybercrime, trailing only the United States and the UK (Jack &
Ene, 2016; Daily Trust report, 2010 cited in Maitanmi et al., 2013; Folashade & Abimbola, 2013). Additionally, Nigeria is identified as a hub for malicious cyber activities in the African region (Ribadu, 2007), indicating its potential for negative impact not only within the country but across West Africa as well.

2.3 Types of Cybercrime in Nigeria

Various forms of cybercrime are prevalent in Nigeria, including hacking, credit card fraud, identity theft, ransomware, DDoS attacks, spam, and more (Bowker, 2012; Denning, 1999; Choo, 2007; Barford & Yegneswaran, 2007; Yar, 2005). These offenses exploit technology to compromise victims' personal and financial information, disrupt services, and spread malware. Despite the prevalence of cybercrime in Nigeria, few studies have explored victimization frequencies and experiences (Sule et al., 2021; Ajiji, 2017; Omodunbi et al., 2016; Akpan, 2019; Maitanmi et al., 2013; Medium.com, 2020). The paucity of victim-focused research underscores a significant gap in understanding the human dimension of cybercrime in the Nigerian context.

2.4 Cybersecurity

Cybersecurity encompasses measures and practices aimed at safeguarding computer systems, networks, and data from unauthorized access, disruption, and destruction (Whitman & Mattord, 2018). It ensures confidentiality, integrity, and availability of digital information. Continuous vigilance and adaptation to evolving threats are crucial in maintaining effective cybersecurity (Moreta et al., 2023). Recognizing the shift towards e-governance and its security implications, policies on cybersecurity are essential for protecting sensitive information, maintaining privacy, and upholding critical services (Sule et al., 2021).

Methods

3.1 Study Area

The study is centered in the Federal Republic of Nigeria, a West African country with a population exceeding 230 million, making it both Africa's most populous nation and the sixth-most populous country globally. Renowned for having the largest economy in Africa, Nigeria ranks 31st by nominal GDP and 30th by PPP-adjusted GDP. As of 2022, its GDP (PPP) per capita stands at US$9,148. This places it ahead of Ghana and Ivory Coast, while slightly trailing South Africa, Egypt, and Morocco. Nigeria is a prominent force in various sectors, including energy, finance, pharmaceuticals, and entertainment. Besides petroleum, remittances from Nigerians abroad are a significant source of foreign exchange. The country boasts a well-developed financial services sector that encompasses local and international banks, asset management firms, insurance companies, and investment banks.

3.2 Data Source

Data for this study was primarily obtained from two sources:

1. Economic and Financial Crime Commission (EFCC): We accessed cybercrime and cybersecurity incident reports filed with the EFCC over the specified period. These reports provided detailed information on the types of cybercrimes, their frequency, and the sectors affected. The dataset includes incident-level information related to cybercrimes spanning from 2022 and preceding years. A summary of cybercrime incidents, presented in Table 1, offers insights into their prevalence within the country. Notably, the recorded incidents surged from 40 in 2020 to 60 in 2021, and subsequently reached 100 in 2022.

2. Distributed Survey: To complement the official data, an extensive distributed survey was conducted among a diverse cohort of participants in Nigeria. This cohort included students, staff, and workers from various sectors, ensuring a wide-ranging perspective. The survey collected information on individuals' experiences with cybercrime, their awareness of cybersecurity measures, and their perception of the cybercrime landscape. Table 2, offers insights into their prevalence within the country.

3.3 Data Collection:

EFCC Data: We obtained permission to access EFCC records, ensuring compliance with ethical and legal considerations. The EFCC provided anonymized data that excluded any personally identifiable information.

Distributed Survey: The survey was designed and distributed using established survey platforms. Participants voluntarily participated, and their responses were anonymized and kept confidential.

Ethical guidelines are strictly followed, including informed consent, anonymity, and confidentiality. Participant rights are prioritized based on academic and research standards.

3.5 Data Analysis:

Statistical Analysis: We employed basic statistical analysis to examine trends and patterns in cybercrime occurrence rates over the specified period. Descriptive statistics, including means, and medians were calculated as well as Excel spreadsheets that facilitated the calculation of relevant counts, percentages, and the creation of graphical representations to identify significant surge of cybercrime incidents.

Nearest Neighbour Analysis: To identify areas or sectors most affected by cybercrimes, we conducted nearest neighbour analysis, pinpointing clusters of incidents and their characteristics.

To analyze the data, a combination of simple statistical methods and advanced spatial statistics was employed.
Limitation Regarding the Data

Data Collection Bias: The study relies on data from the Economic and Financial Crime Commission (EFCC) and a survey. There may be inherent biases in the data collected by the EFCC, which could influence the accuracy of the cybercrime rates. Additionally, the survey responses are subject to self-reporting bias, as participants may underreport or overreport their experiences with cybercrimes.

Results

This section unveils the outcomes of the comprehensive analysis undertaken, shedding light on the pervasive nature of cybercrime and its escalating frequency in Nigeria. Prior to delving into the visual representation of the substantial rise in cybercrimes, it is imperative to present the extensive dataset collected from the Economic and Financial Crime Commission (EFCC) and through a rigorous questionnaire respectively which is displayed in Table 1 and Table 2 below.

Table 1. Summary of the number of convicted cybercrime incidents in Nigeria from the EFCC, 2019-2022.

<table>
<thead>
<tr>
<th>Year</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>877</td>
<td>30%</td>
</tr>
<tr>
<td>2020</td>
<td>1890</td>
<td>65%</td>
</tr>
<tr>
<td>2021</td>
<td>2400</td>
<td>83%</td>
</tr>
<tr>
<td>2022</td>
<td>2900</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 2. The Summary of Findings on Extensive Survey on Cybercrime Incidents in Nigeria

<table>
<thead>
<tr>
<th>ITEM</th>
<th>TYPE</th>
<th>FREQUENCY</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed consent response</td>
<td>Yes</td>
<td>896</td>
<td>99.24%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>7</td>
<td>0.76%</td>
</tr>
<tr>
<td>Total No. of respondents</td>
<td></td>
<td>889</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>584</td>
<td>65.69%</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>312</td>
<td>35.10%</td>
</tr>
<tr>
<td>Educational Level</td>
<td>Undergraduates</td>
<td>341</td>
<td>38.36%</td>
</tr>
<tr>
<td></td>
<td>Masters' Students</td>
<td>522</td>
<td>58.72%</td>
</tr>
<tr>
<td></td>
<td>Doctoral Candidates</td>
<td>21</td>
<td>2.36%</td>
</tr>
<tr>
<td></td>
<td>Teachers and Workers</td>
<td>12</td>
<td>1.35%</td>
</tr>
<tr>
<td>Confirmed negative experience on cybercrime</td>
<td>Yes</td>
<td>588</td>
<td>66.14%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>301</td>
<td>33.86%</td>
</tr>
<tr>
<td>Type of Cybercrime</td>
<td>E-Banking/Payment-Card Fraud</td>
<td>554</td>
<td>62.32%</td>
</tr>
<tr>
<td></td>
<td>Identity Theft</td>
<td>67</td>
<td>7.54%</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>295</td>
<td>33.18%</td>
</tr>
<tr>
<td>Reported?</td>
<td>Yes</td>
<td>322</td>
<td>36.22%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>577</td>
<td>64.90%</td>
</tr>
<tr>
<td>Stolen Money reversed/Suitable Action Taken?</td>
<td>Yes</td>
<td>54</td>
<td>6.07%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>835</td>
<td>93.93%</td>
</tr>
</tbody>
</table>

4.1 Overview of Cybercrime Occurrence

Offering an overarching perspective on cybercrime, this study examines its prevalence and the corresponding rate of incidents in Nigeria. Before delving into the pronounced escalation of cybercrimes, it is essential to showcase the robust dataset amassed through meticulous data collection. Moreover, this analysis incorporates a comprehensive view of cybercrime incidents, examining their occurrence across diverse spatial locations.

4.2 Unveiling Cybercrime Patterns in Nigeria: The Case of Jos City

Table 2 presents a succinct summary of the findings pertaining to cybercrime in Jos City, Nigeria. The table's insights underscore a compelling narrative. Notably, out of a total of 889 respondents, a significant 66% (588 individuals) confirmed encountering negative experiences with cybercrime. This statistic vividly highlights the escalating trajectory of cyber misconduct, demanding immediate attention.

The dataset, however, unveils a striking facet – approximately 64% (577 out of 899) of these cybercrimes go unreported. This alarming revelation underscores the gravity of the situation, emphasizing the urgent need for vigilant countermeasures. This aligns with the observations of Medium.com (2020), which
emphasizes Nigeria's inclination towards underreporting cyber security incidents, thus hindering meaningful cross-country comparisons. This phenomenon mirrors South Africa's scenario, where the prevalence of cyber misconduct similarly prevails.

### 4.3 Impact on Sectors and the Financial Landscape

Importantly, the data indicates that while cybercrimes permeate various sectors, the financial domain, particularly E-Banking/Payment-Card fraud, bears a significant brunt of these criminal activities. Furthermore, the data indicates a critical aspect - the post-misconduct redressal mechanisms, encompassing actions such as recovering stolen funds, providing compensation, or delivering prompt solutions, are realized at an average rate of only 93% (835 out of 889 respondents). This calls for more robust strategies in addressing the aftermath of cybercrime incidents.

### 4.4 Temporal Evolution of Cybercrime Incidents

The analysis, enriched by the comprehensive questionnaire, is further supplemented by Figure 1. This visual representation graphically traces the escalating trajectory of cybercrime incidents spanning the years 2019 to 2022. The graph starkly illustrates the substantial surge in cyber misconduct incidents over this period, underlining the gravity of the issue.

Following the comprehensive study of cybercrime incidents through an extensive questionnaire, Figure 1 visually represents the temporal trajectory of this phenomenon. The graph depicted in Figure 1 illustrates the progression of cybercrime incidents from the years 2019 to 2022, shedding light on the evolving landscape of cyber misconduct.

### Discussion

This paper endeavors to explore the realms of Cybercrime and Cybersecurity by establishing clear definitions and proposing potential solutions to the issues at hand. It particularly aims to provide an overarching view of cybercrime while delving into the determination of its prevalence in Nigeria. The ensuing discussion serves as the response to the inquiries posed in the initial purpose statement. This study is of paramount significance in bridging substantial gaps prevalent in the existing literature. The dearth of comprehensive studies in Nigeria, especially concerning the rate and magnitude of cybercrimes, accentuates the necessity for this research. Furthermore, the requirement for up-to-date data to gauge the pace of cybercrime propagation is undeniable.

The study’s outcomes vividly portray the escalating rate of cybercrime in Nigeria. Specifically, it illuminates the rapidity with which cybercrime has infiltrated Nigerian society and its neighboring regions in recent years. These findings substantiate the observations made by Bello and Temitayo (2017) in their study, "The Legal Chronicle of Cybercrime," wherein they highlighted the profound damages inflicted by cybercrimes in Nigeria. Consequently, their recommendation for a holistic approach to safeguarding the world, particularly developing nations like Nigeria, from the perils of cybercrime is apt. Thus, the findings affirm the worrisome increase in cybercrime over recent years, a trend that exhibits no signs of abating.

The practical implications of the study's findings are equally significant. The insights gleaned from this research hold profound relevance for governments at all levels, elucidating the socio-economic repercussions of cybercrime in Nigeria. Such insights can facilitate the judicious allocation of limited resources to counter these threats. Additionally, the study extends its utility to students, researchers, and scholars interested in further delving into the subject matter.

Household heads, too, bear the responsibility of vigilant oversight when family members exhibit excessive attachment to computers and the internet or display suspicious behavior. To mitigate victimization, individuals should exercise heightened vigilance when navigating the intricacies of the internet and public computer systems.

However, the study is not without its limitations, which necessitate consideration in future research endeavors. Primarily, this study primarily focuses on providing an overview of cybercrime and cybersecurity rates. Therefore, the findings primarily serve to illuminate and raise awareness among the general public, governmental bodies, and security agencies, empowering them to develop appropriate solutions. Furthermore, the scope of available data is constrained by redundancy, and police data often conceal the true extent of cybercrime due to underreporting. Many victims might refrain from reporting incidents due to a lack of technical proficiency. Subsequent research could rectify these limitations by exploring the government's role in combating cybercrime in Nigeria, outlining strategies to enhance this battle, and potentially employing alternative survey methodologies to address the issue of underreporting.

### Conclusion

In conclusion, this research paper strives to delve into the realms of cybercrime and cybersecurity, offering clear definitions and suggesting potential solutions to the challenges posed. The study’s primary aim is to provide an overarching view of cybercrime while examining its frequency within Nigeria. The Discussion section provides insight into the implications of the study's findings, highlighting the urgent need to address the escalating rate of cybercrime. This research bridges crucial gaps in the existing literature and underscores the necessity for comprehensive efforts to combat cybercrime in Nigeria. Moving forward, it is imperative for stakeholders, government bodies, and regulatory agencies to collaborate on proactive initiatives aimed at safeguarding vulnerable demographic groups against cybercrime victimization.

### References


Denning, S M. (1999). "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). Center for Strategic Leadership. Archived from the original (PDF)

Economic and Financial Crime Commission (EFCC),


**Declarations**

**Ethics approval and consent to participate**

- Not Applicable

**Consent for publication**

- Not Applicable

**Statement Regarding Research Involving Human Participants and/or Animals**

- Not Applicable

**Availability of data and material**

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to their containing information that could compromise the privacy of research researchers and or, participants.

**Competing interests**

The authors declare that they have no competing interests.

**Funding**

There is/are no funding available for this research from any institution.

**Authors’ contributions**

Aminu, M.A. contributed by writing the literature review, interpreted the data set for this study of this paper, also worked on the methodology section and writing the introductory section of the paper and performed general editing of the manuscript.

**Acknowledgements**

Not applicable.

**Authors’ information (optional)**

- Not Applicable

**Figures**
Figure 1

Cybercrime incidents from 2019-2022