Peer-reviewed academic journal

Innovative Issues and Approaches in Social Sciences

IIASS VOLUME 19 (2026)

Innovative Issues and Approaches in Social Sciences

IIASS is a double blind peer review academic journal published 3 times yearly (January, May, September) covering different social sciences: political science, sociology, economy, public administration, law, management, communication science, psychology and education.

IIASS has started as a SIdip – Slovenian Association for Innovative Political Science journal and is being published by ERUDIO Center for Higher Education.

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; the headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International, DOAJ, Google scholar.

Publication Data:
ERUDIO Education Center

Innovative issues and approaches in social sciences, 2026, vol. 19

ISSN 1855-0541

Additional information: www.iiass.com

STRATEGIES FOR COMBATING CYBERCRIME AS AN EFFECTIVE TOOL FOR ENHANCING E-GOVERNANCE IN NIGERIA

Yusuf Nabil[1], Abdullahi Nuhu Shawai[2]

ABSTRACT
Cybercrime continue to threaten the shift to digital governance in Nigeria. Major risks like hacking, data breaches, and identity theft weaken public confidence in e-governance and slow down sustainable development. The purpose of this study was to examine the strategies for combating cybercrime as an effective tool for enhancing e-governance in Nigeria. Structured interviews were developed to source the data from the concerned agencies, ministries and private sectors. The findings reveal that Nigeria's current cyber security efforts fall short, calling for a multi-layered strategy with stronger laws, better cyber security infrastructure, and public education. The study found that Nigeria's success in e-governance relies on strong security and public trust, suggesting that collaboration between government, private sector, and international partners is essential to tackling cyber threats and achieving a secure digital future.
Keywords: Cybercrime, Cyber Security, E-governance, Cyber Space, Nigeria

BACKROUND TO THE STUDY

The advent of information and communication technology opened a new opportunities in the areas of communication, industrial sciences, education, and government. More and more, development strategies are based on the need for developing countries to embrace information technology both as a way to avoid further economic and social marginalization as well as to offer opportunities for both growth and diversification of their economies (Abubakar, 2017).), It is indisputable that the internet revolution and digital explosion provide

[1] Department of Political Science, Federal University of Kashere, Gombe State, Mobile; 09032238810, nabilyusuf8810@gmail.com
[2] Department of Political Science, Federal University of Kashere, Gombe State Mobile; 08038398164, abdullahinuhushawai55@gmail.com

immense benefit to mankind including ecommerce, digital marketing, e-governance, social interconnectivity and ease of living for the globe (Sule et'al, 2022). This contribution of internet to the development of mankind has been marred by cybercrime.

However, the conscious evolution of new waves of crime has hampered the ICT contribution in the political landscape. Additionally, the most effective and secure criminal activity thrives in the internet (Ezekiel et'al, 2021. Cybercrime has become a major security concern globally, as it is threatening global stability in terms of the security of critical national infrastructure, the safety of cyberspace and digital economic development as well as protection of personal private data and confidentiality (Koops, 2016).

Cybercrime is perceived as any computer-related crime: any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network (Maitanmiet'al 2013).

Cybercrimes pose a significant threat to society everywhere. Due to its transnational nature, the fight against cybercrime necessitates an international effort that is well-coordinated. Due to the fact that a cyberattack can destroy a nation without requiring personnel to travel to the targeted nation, cybercrime has emerged as a new permanent threat (Nuredini, 2019). The effects of cybercrime are biting hard on nations' economy, locally and internationally.

Therefore, the misfortune assessment because of cybercrimes is incredibly high. According to Morgan (2020), cybercrime-related financial losses are anticipated to rise globally by 15% annually for the next five years. Going on like this, it will hit a yearly misfortune pace of $10.5 trillion by 2025, which will be an increment from $3 trillion, in 2015. Ransom ware increased by 40% and malicious Internet infiltration by more than 600% since 2019. The Federal Bureau of Investigation (FBI, 2009) estimated that cybercrimes cost the United States of America (USA) more than 10 billion dollars annually. Africa experiences hundreds of millions of cyberattacks annually (Kshetri, 2019).Even more concerning is the fact that cybercriminals are focusing their efforts on emerging economies because these economies are convenient targets that they consider to be "low-hanging fruit" (Kshetri, 2019). In addition, the growing vulnerability of the African economy to cybercrime is cause for concern due to the continent's developing nations' increasing reliance on networked computer systems (Peter, 2017).

More so, cybercrime in 2017 cost African economies USA $3.5 billion (Kshetri, 2019). As per Serianu (in Kshetri, 2019), who works for a Kenya-based IT and business warning firm, cybercrimes cost African economies $3.5 billion in 2017. In that year, annual losses to cybercrimes were estimated for Nigeria at $649 million, and Kenya at $210 million. Likewise, according to the South African Banking Risk Information Centre (SABRIC), South Africa loses $157 million annually to cyber attacks (Kshetri, 2019).

According to Fassassi & Akoussan (2016), Nigeria's economy is estimated to be losing $500 million annually, due to the scourge of cybercrime. Nigeria is now ranked third among the top ten sources of cybercrime in the world (FBI). Sending spam emails, stealing personal information, breaking into someone's computer to view or alter data (hacking) and tricking someone into revealing their personal information (phishing), making Internet services unavailable to users, advanced fee fraud 419 (also known as Yahoo-yahoo), credit card fraud, plagiarism and software piracy, porn such countless wrongdoings are perpetrated consistently in the Nigerian internet (Maitanmiet'al 2013).

The danger attached to cybercrimes as reflects on the country's image, has made it more difficult for Nigeria to engage in online business and other cyber related activities. This shows an important threshold for the study of cybercrime in Nigeria. Given this alarming shooting up of cybercrime victimization among individual and groups, it's vital to examined how this threatens the Nigeria's quest for E governance.

1.1 Statement of the Problem

Therefore, the cases of cybercrimes are becoming increasingly alarming with each passing day. The face of E governance and national development has experienced numerous setbacks as a result of this trend.

Nevertheless, researches by Sule et'al, (2021), Abubakar I,(2010), Udelue and Bentina, (2019), Ezekiel et'al,(2021), Sekav, (2016), Kshetri,(2019), on cyber security revealed that, despite the efforts made by the Nigerian government to combat cybercrime, it continues to flourish due to week cyber security capabilities, lack of trained cyber security personnels. The absence of adequate legislation to combat cybercrime, inadequate funding for cybersecurity programs, and the absence of adequate cybersecurity infrastructure and the lack of political will on the part of the government to combat the prevalence of cybercrime are additional obstacles. The study present

different approach from the previous works in the field, as many scholars have not been given adequate attention on the provision of social security and providing practical policy postulations in the combat against cybercrime in Nigeria. It is against this backdrop the study is aimed at investigating the strategies for combating cybercrime as an effective tool for enhanced e-governance in Nigeria.

1.2 AIM AND OBJECTIVES

The general objective of the Study is to investigate the strategies for combating cybercrime as an effective tool for enhancing E-Governance in Nigeria. While the specific objectives are;

To examine the reasons for the prevalence of cybercrime in Nigeria

To investigate the threats posed by cybercrime towards Nigerian quest for achieving E-GOVERNANCE

To examine the Nigerian policy respond to the spread of cybercrime

To proffer solutions to the problems of cybercrime to enhance E-governance in Nigeria

LITERATURE REVIEW

2.1 Cyber Security

Cyber Security is very crucial area in today's digital world, for the development of a nation, it focused on safeguarding computer systems, networks, and data from threats and vulnerabilities. Cyber security embraces both the protection of cyber space and also the pursuit of wider security policy through exploitation of the many opportunities that cyber space offers (Cyber Crime Strategy, 2010). Cyber security is a comprehensive set of practices, technologies, and processes designed to protect digital systems, networks, devices, and data from unauthorized access, breaches, damage, or theft, while ensuring their availability, integrity, and confidentiality (Disterer et al., 2016). It covers set of strategies and measures aimed at mitigating cyber threats and vulnerabilities to maintain the security and resilience of the digital ecosystem. In the view of Anderson, (2015) cyber security refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, cyber attacks, and data breaches while ensuring the confidentiality, integrity, and availability of digital assets.

According Kanellis et al., (2019) expand that cyber security extends beyond technological aspects to include policies, user education, incident response, and legal frameworks, all working together to

create a resilient defense against evolving cyber threats. Disterer et al., (2016) opined that cyber security aims to develop innovative solutions, methodologies, and best practices to mitigate cyber risks and enhance the security and resilience of the digital ecosystem. Cyber security measures protect government systems and citizen data from cyber threats (Kshetri, 2013). The increasing sophistication of cyber threats requires continuous efforts to bolster cyber security measures (West, 2018). The surge in crypto-related crimes has also highlighted the urgent need for stricter regulations and better security measures in the digital financial space (Chainalysis, 2022).

2.2 Cybercrime

Computers, the internet and electronic communications play an ever-increasing part in all our lives, with the use of the internet in the home, at work or in educational establishments now standard and continuing to grow, (Cyber Crime Strategy, 2010). The impact increases as new, and often unpredicted, applications of technologies are quickly adopted by significant proportions of the population, (CCS, 2010). Mobile internet devices, such as smart phones, are now common, and a growing number of services, such as location based services, are being created to work with them (CCS, 2010).

Cybercrime has become a major security concern globally, as it is threatening global stability in terms of the security of critical national infrastructure, the safety of cyberspace and digital economic development as well as protection of personal private data and confidentiality (Koops, 2016, cited in Sule et'al, 2022). The effects of cybercrime are biting hard on nations' economy, locally and internationally

The interconnected nature of the internet means that cybercrime transcends borders, making it a global concern (Holt, 2016). Nuredini, (2019) also justified that cyberattack can destroy a nation without requiring personnel to travel to the targeted nation, cybercrime has emerged as a new permanent threat. Additionally, Ezekiel et'al, (2021), opined that the most effective and secure criminal activity thrives in the internet. It is indisputable that the internet revolution and digital explosion provide immense benefit to mankind including ecommerce, digital marketing, e-governance, social interconnectivity and ease of living for the globe (Sule et'al, 2022).

Therefore, cybercrime is a wide range of offences that can be committed through communication technology. Cybercrimes are

commonly considered as falling into one of two categories: new offences committed using new technologies, such as offences against computer systems and data, dealt with in the Computer Misuse Act 1990; and old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence. In the former are crimes such as hacking or breaking into computer systems to steal or alter data; in the latter, crimes such as the transfer of illegal images or fraud. The former are often a precursor to the latter, based on motives of financial gain. (Cyber Crime Strategy, 2010). According to the United Nations cited in Ali, (2022), Cybercrime covers any illegal behavior directed by means of electronic operations that targets the security of computer system, and the data processed by them. According to Nuredini, (2019), Cybercrimes are means of unauthorized interception of computer systems and computer data through computers with intent to intercept the network and computer systems, in order to obtain personal data or manipulate with these data, use of computer resources for terrorism, intercept and obtain data from computer systems for financial, political and blackmailing purposes, unlawful hindrance of computer systems, acts against confidentiality, integrity and availability of the computer system data etc. There are a vast number of actions that are connected with cybercrimes in social aspect such as copyright issues on distribution of protected material such as scientific publications, musical projects, audio, video and other business and academic activities Nuredini, (2019). Cybercrime has far reaching consequences, including financial losses, reputational damage, and breaches of privacy (Anderson and Moore, 2020). It can also undermine national security, disrupt critical infrastructure, and erode public trust in digital technologies (Bocij and McFarlane, 2020).

In more recent years, Nigeria has faced a growing wave of cybercrime that mirrors global trends, but with its own unique challenges. Ransomware attacks have become more common, hitting key sectors like finance and healthcare. In 2020, a report on Nigeria's Cybercrime Act showed a spike in these attacks, causing major service disruptions and financial losses. These incidents have exposed weaknesses in Nigeria’s digital defenses, especially as more businesses move their operations online (NITDA, 2020).

The country's financial institutions have been a major target for cybercriminals. In 2020, the Central Bank of Nigeria (CBN) noted a massive 534% increase in fraud cases, mostly involving phishing, malware, and social engineering. The surge in online banking during

the pandemic made the sector more vulnerable, highlighting the urgent need for better cybersecurity to protect customer data and financial transactions (CBN, 2020).

Online fraud has also shooted, with scammers using social media and e-commerce platforms to trick people. A 2021 report by the Nigeria Internet Registration Association (NiRA) showed a 43% rise in domain names linked to fraudulent activities. These scams often target individuals with phishing emails, fake investments, and identity theft, challenging Nigeria's push to create a safe digital economy (NiRA, 2021).

Data breaches are another growing concern, affecting both government and private entities. In 2021, Nigeria's National Information Technology Development Agency (NITDA) reported unauthorized access to government databases, exposing sensitive information of citizens. This incident raised questions about the effectiveness of Nigeria's data protection policies and highlighted the gaps in its privacy laws (NITDA, 2021).

As Nigeria's use of crypto currency expands, so does the risk of cybercrime. In 2021, Nigeria had the highest rate of crypto currency adoption in Africa, but this also led to a surge in crypto-related scams. The Economic and Financial Crimes Commission (EFCC) reported a rise in fraudulent schemes, including fake exchanges, Ponzi schemes, and false investment opportunities, leading to significant losses for many Nigerians. This shows the urgent need for clearer regulations and better security in Nigeria's digital finance sector (EFCC, 2021).

These examples illustrate Nigeria's evolving cyber security challenges as the country undergoes digital transformation. With more people accessing the internet and using digital financial services, there's a clear need for stronger cyber security policies and infrastructure to protect individuals and the economy as a whole.

E-Governance

Advancement in information and communication technology is the foundation for the quest of e-governance. This includes hardware, software, networks, and data centers that support digital services and information management (West, 2018). E-governance, or electronic governance, is the use of information and communication technologies (ICT) to enhance the efficiency, transparency, and effectiveness of government operations, public services, and citizen engagement (Heeks, 2006).

According to United Nations (2006), e government is the development of internet and world wide web for the delivery of

government information, and services to the citizens. In another vein the World Bank defines e government as the use of information and communication technologies by government to enhanced the range and qualities information and services provided by citizens, business, civil society organizations, and other government agencies in an efficient, cost-effective and convenient manner, making government processing more transparent and accountable and strengthening democracy. Information and communication technology facilitate and improve the government effective and efficient service delivery to the citizens.

More to that government provide a range of digital services to citizens and businesses, including online forms, e-payment gateways, and information portals, accessible through various channels (UN, 2021). Effective data collection, storage, and analysis are essential for evidence-based decision-making and service delivery (Bannister & Connolly, 2011).

Therefore, the system promotes transparency promotes transparency by providing access to government information, policies, and decision-making processes (UN, 2018), as well as accountability government agencies are accountable for their actions and decisions in the digital realm, with mechanisms for citizens to seek redress (West, 2018). It also encourages citizen participation in policy formulation, service design, and feedback mechanisms (UN, 2018). It ensure that the marginalized and vulnerable populations have access to e-governance services is essential to promote inclusivity (UN, 2021). It also brings government closer to the people, as citizen demand, yearnings and aspirations can easily be heard through the use of media.

Cybercrime in Nigeria

Cybercrime in Nigeria has been a growing concern due to the increasing use of digital technology and the internet the most prevalence are cybercrime activities, including phishing, ransom ware attacks, and identity theft. These trends underscore the need for cyber security measures to protect government systems and citizen data.

Nigeria is infamous for advance-fee fraud or "419 scams," where fraudsters lure victims into paying an upfront fee in exchange for a promised financial windfall. These scams have evolved over time to encompass various forms of online fraud (Ogun, 2017). Phishing and Identity Theft: Cybercriminals use phishing emails and fake websites

to steal personal and financial information from unsuspecting victims, both within Nigeria and abroad (Oludele and Salawu, 2016).
Therefore, there have been cases of online banking fraud, where cybercriminals gain unauthorized access to individuals' bank accounts and conduct fraudulent transactions (Adegbite et al., 2016). Similarly, the use of malicious software, including ransom ware, to compromise computer systems and extort money from victims has become a prevalent cyber threat in Nigeria (Ogungbemi et al., 2019). Cyber bullying and harassment through social media platforms have also been reported, impacting the safety and well-being of individuals (Adewale et al., 2016).

Causes of cybercrimes in Nigeria

Several factors contribute to the rise of cybercrime in Nigeria, with socio-economic challenges, inadequate cybersecurity awareness, and regulatory gaps playing significant roles. One of the primary drivers is the high unemployment rate, particularly among the youth. According to the National Bureau of Statistics (NBS), the unemployment rate in Nigeria reached 33.3% in 2022, with many young people struggling to find stable jobs. This economic hardship often pushes individuals toward cybercrime, such as internet fraud, commonly known as "Yahoo Yahoo," as a way to make quick money. The allure of financial gain can be compelling in an environment where traditional job opportunities are scarce.
Another contributing factor is the rapid increase in internet penetration in Nigeria, which has not been matched by a corresponding rise in cyber security awareness. The Nigeria Internet Registration Association (NiRA) reported in 2021 that while internet usage was on the rise, many Nigerians remained unaware of basic online security practices. This lack of understanding leaves individuals vulnerable to various cyber threats, including phishing, fraud, and identity theft, ultimately creating a conducive environment for cybercriminals to operate.
The weak cyber security infrastructure in Nigeria further exacerbates the issue. A report by the National Information Technology Development Agency (NITDA) in 2021 highlighted that many Nigerian businesses, especially small and medium-sized enterprises, lack robust cyber security measures. This vulnerability is appealing to cybercriminals, as organizations with inadequate defenses are more susceptible to attacks like ransom ware and data breaches. The absence of strong cyber security practices makes it easier for

criminals to exploit systems and gain unauthorized access to sensitive information.

Moreover, there is a lack of strong cybercrime laws and enforcement in Nigeria. Although the Nigerian Cybercrime Act of 2015 established legal frameworks to combat cybercrime, enforcement remains a significant challenge. A review by the Cyber Security Experts Association of Nigeria (CSEAN) in 2022 pointed out that while the laws exist, coordination among enforcement agencies is often lacking, which hampers effective prosecution. This weak enforcement landscape emboldens cybercriminals, who perceive a low risk of facing legal consequences for their actions.

In another parlance rise of crypto currency and unregulated digital finance has added another layer to the cybercrime issue in Nigeria. The increasing popularity of crypto currencies has made them attractive to cybercriminals, who exploit their anonymity for illegal activities such as money laundering and fraud. A report by Chainalysis in 2021 indicated that Nigeria was a hotspot for crypto-related scams, with a noticeable uptick in fraudulent schemes involving digital currencies. The lack of clear regulations surrounding digital finance further compounds the problem, as cybercriminals can exploit these regulatory gaps to execute their illicit activities.

Cybercrime and E Governance

In an era dominated by digital transformation, the coexistence of cybercrime and e-governance has created a complex interrelationship that has far-reaching implications for societies globally. E-Governance platforms can be vulnerable to various cyber threats, such as data breaches and system manipulation. Identifying and addressing these vulnerabilities are critical to maintaining the integrity and security of government digital systems. Moreover, e-governance, characterized by the use of digital platforms to facilitate government functions, services, and interactions with citizens, offers numerous benefits in terms of efficiency, transparency, and accessibility. However, the rise of cybercrime poses a significant threat to these systems. Cybercriminals exploit vulnerabilities in e-governance platforms to perpetrate a wide range of illicit activities, including unauthorized data access, identity theft, financial fraud, and service disruption (Serrao and Harrison, 2018).

Simultaneously, the growth of e-governance contributes to the evolution of cybercrime. As governments digitize their services, they amass vast repositories of sensitive citizen data, presenting an attractive target for cybercriminals. The interconnectedness of e-

governance systems also provides cybercriminals with potential points of entry for attacks (Kshetri, 2017).

The rapid shift to remote work during the COVID-19 pandemic led to an increased reliance on digital communication tools. This created new avenues for cybercriminals to exploit vulnerabilities in both government and corporate systems, resulting in a surge of phishing and malware attacks (Interpol, 2020).

Strategies for Combating Cybercrime

Governments worldwide are responding to the problem posed by cybercrime towards achieving e-governance with diverse strategies. These strategies encompass legislative reforms, capacity building, international cooperation, and public-private partnerships (Matusiak, 2021).

Governments, law enforcement agencies, and the private sector have implemented various strategies to combat cybercrime (Brenner, 2019). These include, Legislation, Enacting and enforcing cybercrime laws to deter criminals and prosecute offenders (Balkin, 2017). Employing cyber security measures, such as firewalls, antivirus software, and encryption, to protect against cyber attacks (Schneier, 2015). Facilitating cooperation between nations to address transnational cyber threats (Nye, 2019). Educating individuals and organizations about cyber threats and best practices for online safety (Cavelty and Suter, 2018). Developing incident response plans to mitigate the impact of cyberattacks when they occur (Whitman & Mattord, 2019). Nigeria collaborates with international organizations like interpol and regional partners to combat cybercrime. Such collaborations are vital given the global nature of cyber threats (Ezenyilimba & Nnamdi, 2019).

A comprehensive approach to combating cybercrime involves the implementation of effective strategies. These strategies encompass a National Cybersecurity Policy, the development of cybersecurity infrastructure, and collaboration with international partners to share threat intelligence and best practices. A well-defined National Cybersecurity Policy provides a roadmap for securing digital systems and responding to cyber threats. Such a policy framework establishes guidelines for government agencies and private sectors to follow.

3. METHODOLOGY

3.1 RESEARCH DESIGN

The study makes use of Phenomenological qualitative research as a design of inquiry coming from philosophy and psychology in which the researcher describes the lived experiences of individuals about a phenomenon as described by participants. This description culminates in the essence of the experiences for several individuals who have all experienced the phenomenon (Creswell, 2014). The qualitative method, allow for compiling data from both primary and secondary sources to make qualitative analysis. The study's affordability, feasibility, and reliability, are the reasons this research design is chosen. Using questionnaires and sampling as part of a survey to gather data is impractical from a financial standpoint.

However, a qualitative research design is utilized and chosen due to the importance of the subject matter, and through the use of subject matter experts more firsthand information can be obtained to fill the research gap for social responsibility than the sampling method, and the presence of alternative data collection strategies are the reasons why this design would be adopted.

3.2 SOURCES OF DATA

The sources of data collection are both primary and secondary. For primary in-depth interview with relevant agencies concern with the subject matter. This is in view of their skill to the topic of study. These technocrats are therefore, chosen from agencies concern with countering the menace of cybercrime. In this regard, two cyber security academic experts in Nigerian universities base on closeness of the researcher are interviewed, one Police security officer from the department of cybercrime, a team leader (CCS), from economic and financial crime commission (EFCC), Educational Institutions (a system analyst was interviewed from Gombe State University), Private Sector were also interviewed a focal person from Amsal Digital Solutions was interviewed, Lead analyst was interviewed from Murshid Enterprise, system analyst was interviewed from Fointatech Intelligent Solutions, and three youths who are acquinted with computer and ICT driven business were also interviewed. Documented materials like books, journal articles, magazines, and the Google search were consulted and all make up the secondary sources.

3.3 INSTRUMENT OF DATA COLLECTION

The instruments used for the sources of data for this study are both primary and secondary, for the use of primary an indepth interview were designed to source the data from Law Enforcement one Inspector from Nigerian Police Force was interviewed, a team leader (CCS), from economic and financial crime commission (EFCC), Educational Institutions (a system analyst was interviewed from Gombe State University), Private Sector were also interviewed a focal person from Amsal Digital Solutions was interviewed, Lead analyst was interviewed from Murshid Enterprise, system analyst was interviewed from Fointatech Intelligent Solutions), whereas the secondary data covers both the published and text books, journals, articles, research gate, google scholar are all used to cover the secondary source.

3.4 DATA ANALYSIS

The data obtain from this study would be analyze in qualitative method of data analysis. The data obtain from interview were be collated, and analyze qualitatively using content analysis.

Analysis of findings

The findings of this research are located in the response of the above interviewees who were granted on the 20th January, 2024.

What do you think are the reasons for the prevalence of cybercrime in Nigeria?

The most prevalence cybercrime in Nigeria during the conduct of this research with top identified reasons are: Technological Advancement: 1 respondent; the rapid adoption and advancement of technology in Nigeria have created both opportunities and vulnerabilities. While digital platforms and innovations can lead to greater efficiency and access to services, they also expose gaps in security. Infrastructural and System Decay: 2 respondents, Economic and Societal Challenges (poverty, unemployment, restiveness): 3 respondents; Unemployment, poverty, and economic hardship in Nigeria have contributed significantly to the rise of cybercrime. The widespread availability of technical skills, particularly among Nigeria's youth, combined with a lack of viable job opportunities, has made cybercrime an attractive alternative. Corruption and Lack of Cyber Laws: 3 respondents, Lack of Cyber security Awareness/Skilled Professionals: 2 respondents; The legislative and judicial systems in Nigeria have struggled to keep up with the dynamic and rapidly evolving nature of cybercrime. While laws such as the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 provide a legal basis for

prosecuting cybercriminals, enforcement remains weak. Many cybercrime cases are either not pursued or inadequately addressed due to a lack of technical expertise, bureaucratic inefficiency, and resource constraints within law enforcement agencies.

In what ways does cybercrime pose challenge to the Nigeria's quest for E governance?

Cybercrimes pose a great threat to Nigeria's efforts to implement effective e-governance systems. The following are key areas where respondents emphasize on how cybercrimes undermine e-governance:

Cyberattacks targeting government databases can result in unauthorized access to sensitive information. This compromises not only the privacy of individuals but also the integrity of government services. Hacking and data breaches can lead to the disruption of public services, resulting in financial losses, compromised projects, and weakened public confidence in e-governance systems.

When citizens lose faith in the government's ability to secure personal and sensitive data, they become reluctant to engage with e-governance platforms. Data breaches, identity theft, and online fraud erode trust in government services, which is essential for the success of e-governance initiatives. Public apprehension about the safety of digital platforms can delay or reduce the adoption of e-governance services.

Cybercriminals exploit weaknesses in government infrastructure, potentially accessing confidential data or disrupting essential services such as healthcare, education, or public transportation. A compromised government system can lead to delays in service delivery and jeopardize national security, thus undermining the effectiveness of e-governance efforts.

Cybercrime has direct economic consequences for the government, including financial losses from fraud, theft, or ransom payments. Additionally, the cost of defending against cyber threats diverts resources that could be used for development projects or essential public services. The high costs of cybercrime prevention strain government budgets, hindering the progress of e-governance initiatives.

Cybercriminals targeting critical infrastructure, such as power grids, communication networks, or financial institutions, can severely disrupt national development. Such attacks can cripple government operations and slow down the country's progress toward digital governance. The threat of widespread infrastructure disruption

represents a significant risk to both governance and sustainable development.

The overarching goal of e-governance is to improve transparency, accountability, and sustainable development. However, cybercrime impedes this goal by introducing risks that prevent the full realization of e-governance benefits. With ongoing cyber threats, the potential of digital governance to drive sustainable economic and social development is compromised.

How effective are the current cyber security of Nigeria?

The effectiveness of Cybersecurity Measures in Nigeria are presented by the view of the respondents as; Fairly Effective: 4 respondents, Not Effective: 4 respondents, Satisfactory but with weaknesses: 2 respondents, Global Cybercrime Breach Ranking (Nigeria's position): 32nd most breached country in Q1 2023 (as reported by 1 respondent). Current cyber security measures are deemed insufficient by the majority of respondents, with four respondents noting the inadequacy of existing measures in effectively combating cybercrime

How does the e governance become a source of sustainable development?

The interviewees' respondents by given the Key contributions to sustainability; Improved, Public Service Delivery and Access to Information: 3 respondents, Security and Monitoring of Policies: 2 respondents, Enabling Free and Fair Elections: 1 respondent, Enhanced Local Access to Governance: 1 respondent. E-governance can enhance sustainable development, particularly by improving access to government services, enhancing security, and supporting the implementation of policies.

what measure does you suggest to curb the prevalence of cybercrime towards the realization of e governance

The suggested measures to combat the prevalence of cybercrime as given by the respondents are: Strengthening Legal Frameworks and Laws: 3 respondents, Investing in Modern Cyber security Infrastructure and Tools: 3 respondents, Public Awareness and Cyber security Education: 2 respondents, Creating Specialized Cybercrime Courts: 1 respondent, Training Law Enforcement and Cyber security Professionals: 2 respondents.

Nigeria must update and enforce its cybercrime laws to stay aligned with the latest global standards. The Cybercrime Act of 2015 needs continuous revision to address emerging threats such as crypto

currency fraud and deep fake technology. In addition, law enforcement agencies must receive adequate resources, training, and technical support to enforce these laws effectively.

A significant step in mitigating cybercrime involves upgrading Nigeria's cybersecurity infrastructure. Government systems should be equipped with advanced encryption, firewalls, real-time monitoring, and threat detection systems. Investing in cybersecurity training for personnel across sectors is essential for building resilience against cyber threats.

Training law enforcement officers, including establishing specialized cybercrime units, is critical for effective investigation and prosecution. Agencies must be equipped with the tools and knowledge to combat sophisticated cybercrime techniques. Additionally, cross-sector collaboration between law enforcement, intelligence agencies, and technology companies can facilitate information sharing and improve the collective fight against cybercrime.

Comprehensive cybersecurity education campaigns are needed to teach citizens and businesses about safe online behavior. The government should launch programs promoting cyber hygiene, including best practices for password management, phishing prevention, and data protection.

Addressing unemployment and socioeconomic inequality is vital for reducing the lure of cybercrime. Youth empowerment programs, particularly those focused on technology, can provide alternatives to cybercrime by offering employment opportunities in sectors such as IT, cybersecurity, and software development. Government initiatives to promote digital entrepreneurship and vocational training can also help alleviate economic pressures that lead to cybercrime. Therefore the respondent also affirmed that building trust in e-governance platforms requires a commitment to transparency, accountability, and effective communication. Governments should prioritize secure systems that protect users' data while ensuring seamless access to digital public services. By fostering trust, the government can increase the adoption of e-governance services, reducing the opportunities for cybercrime to disrupt national development.

Summary of Findings

The study shows that cybercrime in Nigeria is mainly fueled by socioeconomic issues like poverty and high unemployment, along with outdated infrastructure and rapidly growing technology. Many young people struggling to find work see cybercrime as a way to make a living. Additionally, because there aren't enough cyber

security experts and the systems protecting organizations are often weak, it's easy for criminals to take advantage of the gaps in digital security.

E-governance in Nigeria, which aims to provide government services online, is facing major challenges from cybercrime. Key threats like hacking, identity theft, phishing scams, and data breaches put government data and citizens' information at risk, which makes people hesitant to use digital services. When citizens don't feel safe using these platforms, it delays the country's progress toward an effective digital government system.

Most people agree that Nigeria's current cyber security efforts are not enough. Though the government has made progress in setting up cyber security policies, these haven't kept up with how fast cyber threats are changing. Without ongoing investment and upgrades, Nigeria's security measures are still too weak to prevent attacks, leaving both public and private sector systems vulnerable.

E-governance could play a major role in Nigeria's development by improving public service delivery, policy monitoring, and information access. With strong security measures in place, e-governance could increase transparency and accountability, which would greatly benefit Nigeria's growth. However, these benefits will only be realized if a secure digital environment is established.

To reduce cybercrime, the study recommends that Nigeria adopts a comprehensive approach. This should include stronger laws, better cyber security infrastructure, specialized training for cybersecurity and law enforcement professionals, and public awareness programs on online safety. By reinforcing laws, investing in advanced security tools, and educating the public, Nigeria can build a more secure digital space, paving the way for successful e-governance and sustainable development.

Conclusion and Recommendations

Cybercrime poses a major challenge to Nigeria's efforts in building a digital government. Economic struggles, lack of job opportunities, and weak cyber security systems allow cybercrime to flourish, eroding data security and public trust. While digital governance has great potential to improve services and transparency, its success depends on Nigeria's ability to create strong and secure cyber security systems. For this to happen, a collaborative effort between the government and private sector is crucial to address the causes of cybercrime, strengthen cyber security measures, and raise public

awareness. Without this united approach, achieving a secure and lasting digital government in Nigeria will remain difficult.

To tackle cybercrime and advance e-governance, this study suggests the following steps:

Updating Legal Frameworks and Strengthening Enforcement: Nigeria should regularly revise its cybercrime laws to address new threats, such as crypto currency scams and deep fake technology. Increased funding and specialized training for law enforcement are essential to effectively implement these laws. Enhancing Cyber security Infrastructure: Strengthening cyber security infrastructure is crucial for protecting both government and private sector systems. This includes adding advanced encryption, threat detection tools, and real-time monitoring capabilities.

Building Capacity in Law Enforcement: Creating specialized units equipped to handle cyber threats, along with partnerships with tech companies and intelligence agencies, will improve skills and facilitate information sharing for effective enforcement.

Raising Public Awareness and Promoting Cyber security Education: Educating the public on safe online practices through widespread campaigns can help individuals and businesses protect themselves, reducing their vulnerability to cyber-attacks.

Promoting International Collaboration: Given that cybercrime often spans borders, Nigeria should work closely with international cyber security organizations like INTERPOL to share information and collaborate on responses to global threats.

Supporting Economic Development Initiatives: Programs to increase youth employment and skills in technology and cyber security can provide alternatives to cybercrime. Government initiatives that promote digital entrepreneurship and vocational training will help reduce economic pressures that drive cybercrime.

Building Public Trust in E-governance: Secure, transparent, and accountable digital systems are key to gaining public trust in e-governance. Prioritizing data protection and engaging citizens will encourage the use of digital services and support Nigeria’s digital transformation.

References

Adebayo, O. S., Afolayan, J. O., & Abubakar, N. M. (2018). Social engineering attacks: Issues and challenges in Nigeria. International Journal of Advanced Computer Science and Applications.

Adebayo, O. S., Ojugo, A. A., & Ogundile, O. O. (2019). Business email compromise (BEC) and its trends in Nigeria. In Proceedings of the International Conference on Information Resources Management.

Adebowale, A. A., & Babalola, R. S. (2020). Assessment of data breaches and the implication for data privacy in Nigeria. In Proceedings of the International Conference on Computational Science and Its Applications.

Adebowale, A. A., Oluwaseun, I. A., & Rasaq, A. A. (2017). Towards effective cybercrime legislation in Nigeria: A critical appraisal of the Cybercrime Act 2015. Journal of Information Security.

Afolabi, A., Oyedele, A. O., & Emezue, C. A. (2020). Ransomware attacks in Nigeria: Implications for critical infrastructure. International Journal of Computer Applications.

Adeloye, O. A., Afolabi, O. A., & Adeloye, D. (2019). Business email compromise: A threat to Nigerian organizations. International Journal of Computer Applications.

Adekola, O. M., & Ajayi, G. K. (2019). Cybercrime and its implication for national security in Nigeria. International Journal of Research and Innovation in Social Science.

Adegbite, S. A., Ogun, F., & Ogundipe, O. A. (2016). Assessment of online banking fraud and the challenges of combating the menace. International Journal of Economics, Commerce and Management.

Adewale, A. S., Sulaimon, T. A., & Odunayo, S. A. (2016). Cyber bullying: A conceptual overview. International Journal of Psychology and Behavioral Sciences.

Anderson, R., & Moore, T. (2020). The Economics of Cybercrime. Journal of Economic Perspectives.

Awofeso, A., Osofisan, A., & Adeola, O. (2016). Developing cybersecurity awareness in Nigeria. International Journal of Computer Applications.

Babatunde, B. O., & Babatunde, A. B. (2020). Capacity building for cybercrime investigation in Nigeria: A critical appraisal. Journal of the Institute of Justice and International Studies.

Balkin, J. M. (2017). The three laws of robotics in the age of big data. Texas Law Review.

BBC News. (2021). Facebook data on 530 million users found on the web.
Bocij, P., & McFarlane, L. (2020). Cybercrime: A review of the evidence. Deviant Behavior.
Brenner, S. W. (2019). Cybercrime metrics. In The Oxford Handbook of Cyber Security. Oxford University Press.
Broadhurst, R., & Chon, S. (2015). Cybercrime and society. SAGE Publications.
Cavelty, M., & Suter, M. (2018). The role of public–private partnerships in cybersecurity. Journal of Cyber Security.
Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.
Chainalysis. (2022). The 2022 Crypto Crime Report.
Chainalysis. (2021). Crypto crime report: Trends in cybercrime and cryptocurrency.
Cheng, L. (2018). SingHealth data breach: How it happened. The Straits Times.
Choo, K. K. R. (2011). Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences. Australian & New Zealand Journal of Criminology.
Cisco. (2021). Cybersecurity threat trends: Phishing, crypto top the list.
Cybersecurity Ventures. (2021). 2021 Ransomware Damage Report.
Cyber Security Experts Association of Nigeria (CSEAN). (2022). Assessment of cybercrime law enforcement in Nigeria.
Cybersecurity & Infrastructure Security Agency (CISA). (2021). Alert AA21-008A: Detecting post-compromise activity in Microsoft cloud environments.
Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
Ezenyilimba, E., & Nnamdi, N. (2019). Transnational cyber crime and Nigeria's security architecture: Issues, trends, and responses. International Journal of Cyber Criminology.
Finklea, K. M. (2020). Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws. Congressional Research Service.
Higgins, G. E., Wolfe, S. E., & Ricketts, M. L. (2020). Identity theft: A research review and framework for study. Deviant Behavior.
Holt, T. J. (2016). Digital crime and digital terrorism. Routledge.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Heeks, R. (2006). Implementing and managing eGovernment: An international text. Sage Publications.

Interpol. (2020). Cybercrime threat landscape.

Kshetri, N. (2013). Cybersecurity and cybercrime: Issues and solutions in the digital age. Springer.

Kshetri, N. (2017). The global cybercrime industry: Economic, institutional and strategic perspectives. Journal of International Management.

McGuire, M., & Clayton, R. (2017). The economics of ransomware: A case study of the Locky malware. Journal of Cybersecurity.

Matusiak, K. (2021). Cybercrime countermeasures: Responses to the changing nature of cyber threats. The British Journal of Criminology.

National Bureau of Statistics (NBS). (2022). Labour force statistics.

National Information Technology Development Agency (NITDA). (2021). Cybersecurity infrastructure report.

Nigeria Internet Registration Association (NiRA). (2021). Annual report on internet usage and cybersecurity awareness.

Nye, J. S. (2019). Deterrence and dissuasion in cyberspace. International Security.

Ogungbemi, A., Ikuesan, R., & Ajiboye, J. (2019). Mitigating ransomware attacks: A study of ransomware threats in Nigeria. International Journal of Advanced Computer Science and Applications.

Oludele, M. R., & Salawu, M. B. (2016). Phishing attacks and cybercrime in Nigeria: A conceptual analysis. International Journal of Computer Applications.

Onuoha, F. (2017). Regulating cybercrime in Nigeria: An overview of the Cybercrimes Act 2015. African Security Review.

Ogun, S. A. (2021). Cryptocurrency-related crimes in Nigeria: A review of trends and challenges. In Proceedings of the International Conference on Information Resources Management.

Patchin, J. W., & Hinduja, S. (2018). Cyber bullying among adolescents: A brief overview and prevention measures. International Journal of Adolescent Medicine and Health.

Serrao, A., & Harrison, T. M. (2018). Exploring the link between cybercrime and e-governance. Government Information Quarterly.

UN. (2018). United Nations E-Government Survey 2018: Gearing E-Government to support transformation towards sustainable and resilient societies.

UN. (2021). World Public Sector Report 2021: Building an integrated approach to the pursuit of sustainable development goals.
UNDESA. (2018). UN E-Government Survey 2018: Gearing E-Government to support transformation towards sustainable and resilient societies.
United Nations. (2019). The impact of rapid technological change on sustainable development.
West, D. M. (2018). Digital government: Technology and public sector performance. Princeton University Press.