Management Analytics and Social Insights

www.masi.reapress.com

Manag. Anal. Soc. Insights.Vol. 2, No. 3 (2025) 230–244.

Paper Type: Original Article

Cybercrime and Cyber-Security in Nigeria

Olanrewaju Joseph Ilugbami[1,*], Olanrewaju Tolu Omigbodun[2], Ernest Edim[3], Ayobami Abdulmateen Gbadegesin[2], Yetunde Victoria Odeyinka[4]

[1] Rufus Giwa Polytecnic, Owo, Ondo State, Nigeria; ilugbamijosepg@gmail.com.
[2] Department of Transport Planning and Logistics, University of Ilesa, Ilesa, Nigeria; olanrewaju_omigbodun@unilesa.edu.ng; ayobami_gbadegesin@unilesa.edu.ng.
[3] School of Science, Engineering and Environment, University of Salford, United Kingdom; e.edim@edu.salford.ac.uk.
[4] Department of Agricultural and Resource Economics, Federal University of Technology, Akure, Nigeria; victoriaodeyinka@gmail.com.

Citation:

Received: 21 September 2024 *Revised: 17 November 2024* *Accepted: 23 January 2025*	Ilugbami, O. J., Omigbodun, O. T., Edim, E., Gbadegesin, A. A., & Odeyinka, V. V. (2025). Cybercrime and cyber-security in Nigeria. *Management analytics and social insights*, 2(3), 230-244.

Abstract

Different activities, such as commercial, social, and human, among others, are afforded limitless options via the Global Information Infrastructure(GII). However, hackers are increasingly attacking the GII, and the frequency of these attacks raises concerns regarding their quantity, cost, and complexity. In order to explain the pertinent conditions and risks of cybercrime in Nigeria, this study aims to investigate the social and technological aspects of cybersecurity and cybercrime. The research used a theoretical and investigative approach to the problem of cybercrime. Structured interviews were targeted at law enforcement agents organizational organizations on cybersecurity. To comprehend the objectives and tactics of Nigerian cybercriminals and to explain their actions in light of current theories of crime, data collected through these study instruments were submitted to descriptive analysis and frequency counts. Four theories of crime were found to be influenced by Nigerian cybercrime: the technology enabled crime theory, the routine activity theory, the Marxian Theory, and the Structural Functionalism Theory. The examination of current legislation revealed that there are presently no provisions in Nigerian statutes that particularly address cybercrime.

Keywords: Cybercrime, Cyber-security, Information, Nigeria.

1 | Introduction

Civilization and information technology is growing side-by-side the second is driving the first. Internet especially is an aspect of information technology that enables us to communicate with one another globally irrespective of the country and the continent within a twinkle of an eye. Both individuals who participate in illicit activities and those who work and conduct business have benefited from the expansion of the Internet

Corresponding Author: ilugbamijosepg@gmail.com

https://doi.org/10.22105/masi.v2i3.77

and the increased accessibility of computer technology. In addition to causing a sharp rise in the frequency of criminal activity, the development of technology and online communication has also given rise to what seems to be a new range of criminal activity[1]. Legal systems and law enforcement have difficulties due to the rise in criminal activity and the potential for new types of criminal behavior to arise [2].

The ability to reproduce, distribute, control, and publish information has undergone radical changes due to technological advancements; however, the Internet in particular has significantly changed the economics and ease of reproduction [3], and computer networks have significantly changed the economics of distribution [4]. With transmission speeds approaching a billion characters per second, networks allow the sending of information products worldwide, cheaply, and almost instantly. Nigeria, a country currently trying to protect its reputation from cybercrimes, is now focusing on the conduits and sources of cybercrimes.

Re-dignifying honest people and de-stigmatizing cybercrime are more difficult tasks than instituting deterrent mechanisms like the Economic and Financial Crime Commission (EFCC), the Independent Corrupt Practice Commission (ICPC), and the code of conduct Bureau. This comes after years of being at the bottom of the global list of corrupt countries, according to an index created by the anti-corruption advocacy group Transparency International (TI) [5].

There are countless prospects for social, business, and other human endeavors thanks to the Internet. However, the Internet poses unique threats due to cybercrime. What risks to Nigeria can cybercrime and cybersecurity pose? According to Adeniran and Obembe[6], the terrible degree of corruption poses a threat to Vision 20:2020. Cybercrime is a barrier that might prevent the country from making development. Aluko [7] provided seventeen (17) strategies to prevent financial corruption in Nigeria because of this. According to him, cybercrimes are one of these crimes. There is now a rise in criminal activity in the global community.

It is pathetic to note that some individuals in Nigeria have embraced cyber-crime as a way of life. Many have become rich while some others have been caught by the law [35]. This new crime is denting and drilling holes in the economy of the nation. For example, in a recent report by the Internet Crime Complaint Center which is a partnership between the FBI and America's National White Collar Crime Center, revealed that Nigeria now ranked third among the list of top ten sources of cybercrime in the world [36]. Also the Central Bank of Nigeria (CBN) in its banking sector supervision report revealed that the Nigeria banking sector lost 7.2 billion naira to internet fraud [36].

The newspaper's pages are always replete with stories about cybercrime, which is a major global issue by now. Criminal cases are almost often documented in locations with computers and Internet access. The advent of surfing via the Global System for Mobile-telecommunication (GSM) has led to the development of new modes of operation. These criminals frequently include a large number of young individuals. They browse for hours and even remain up all night to continue their evil deeds. Most of the individuals participating are between the ages of fifteen and thirty.

Cybercrimes are one of the criminal activities with the greatest rate of growth in the world, according to Erhabor[8]. It encompasses a wide variety of illicit activities, he reiterated, including financial schemes, computer hacking, obtaining pornographic photos from the Internet, virus attacks, stalking, and the creation of hateful websites. Young students in higher education have been involved in several forms of forgery in recent years, including falsified entrance documents, receipts for school tuition, certificate racketeering, and examination malpractice, which is the practice of using a phone or other electronic device to get important information during an exam.

According to[9], South Africa, Ghana, and Nigeria have the highest rates of cybercrime in Africa. Nigeria is not exempt from the suffering brought on by cybercrimes. The study aims to examine the social and technological variables impacting cybercrime and cyber security in Nigeria in order to curtail and provide solutions for the concerning results mentioned.

The purpose of this study is to offer data and analysis that Nigerian legislators, policymakers, and law enforcement organizations may utilize to develop legislative definitions of cybercrime and cybersecurity that are relevant from a sociological and technological standpoint. Finding the informal, social, and technological causes of cybercrime and cybersecurity in Nigeria as well as analyzing the strategies used by Nigerian law enforcement and cyber-security players to prevent cybercrime and maintain cyber-security are the particular goals.

For sufficient insight and information to solve and accomplish the research challenge and objectives, a mixed research strategy is required. The research will take a theoretical and investigative approach to the problem of cybercrime. In-depth primary research, secondary sources from the Internet, and current literature reviews will all be used in this project. Governmental organizations involved in cyber-security and law enforcement comprise the study population.

2 | Literature Review

2.1 | Cybercrime

The absence of a uniform and legal definition for the types of acts that might be considered cybercrime is a major issue for the study of cybercrime [10]. Determining what constitutes cybercrime presents conceptual challenges [11]. Cybercrime is defined in a variety of ways. Apart from its challenging definition, it is also referred to by several different names, including Internet crime [12], virtual crime [13],[14]computer crime, computer-related crime, digital crime, information technology crime [15], e-crime, and net crime [16]. It seems sense that a broad range of criminal actions and activities might be considered cybercrime.

Cybercrime was separated into two categories and described as follows at a workshop at the tenth United Nations Congress on the prevention of crime and treatment of offenders that focused on crimes involving computer networks:

I. Cybercrime, in its strictest definition, is any unlawful activity that attacks the security of computer systems and the data they handle and is carried out using electronic methods.

II. In a broader sense, cybercrime refers to any unlawful activity carried out through or in connection with a computer system or network, including offenses like unlawful possession and the offering or dissemination of information via a computer system or network.

Cybercrime is used as a catch-all word in the council of Europe's 2001 convention on Cybercrime to describe a variety of illegal actions, including violations of computer data and systems, offenses pertaining to computers, violations of content, and violations of copyright.

The four primary categories of cybercrime covered by the treaty are:

I. Violations of the confidentiality, integrity, and availability of computer data and systems, including unlawful access, illegal interception, interference with data or systems, and illegal devices;

II. Violations of computer-related offenses, such as computer-related fraud and forgery;

III. Violations of content (Such as child pornography); and

IV. Violations of copyright and related rights.

Thomas and Loader [17] provide a workable definition of cybercrime in this vein, defining it as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks." Canadian law enforcement agencies are increasingly adopting the Canadian Police College's working definition of cybercrime, which is defined as a criminal offense in which a computer is either the goal of the crime or the instrument used to perpetrate a major component of the offense [18].

Cybercrime is defined as any illegal activity that targets a computer, computer systems, information network, or data, as well as known illegal activities or crimes that are actively carried out using or aided by a computer, computer systems, information network, or data. It is important to remember that cybercrime lacks a standardized and legal definition[19].

2.2 | Cybersecurity

Making cyberspace secure from dangers, namely cyberthreats, is the focus of cybersecurity. The term “cyber-threat” is a bit nebulous and refers to the malicious use of Information and Communication Technology (ICT) by a variety of bad actors, either as a tool or as a target. National security and cyber-security are frequently confused; however, according to NCWG coordinator Odumesi[20], national security may frequently be linked to certain cyber-security incidents. The phrase "cyber-security" solely describes the protection of networks and systems, including computers, electronics, and related equipment.

According to Odumesi[20], typical cyber-security concerns include information Confidentiality, System Integrity(CIS), and network survivability. Cybersecurity's main goals are to defend against external infiltration and to prevent unauthorized access and data tampering on networks and systems. Three things are often referred to by the phrase “cyber-security”:

I. A collection of technical and nontechnical actions and measures meant to defend computers, computer networks, associated hardware and software devices, and the data and software they contain and exchange, as well as other components of cyberspace, against all threats, including those to national security;

II. The level of protection brought about by the implementation of these actions and measures;

III. The related field of professional endeavor, including research and analysis, aimed at putting those actions into practice and enhancing their quality.

Since information security is at the core of the issue, cybersecurity is therefore more than just data security or information security, yet it is strongly tied to those two areas. Information security encompasses all facets of information protection. These factors are often divided into three groups: information availability, confidentiality, and integrity. While "integrity" relates to preventing unauthorized alterations to information, "confidentiality" refers to preventing information from being disclosed to unauthenticated persons.

“Availability” refers to the fact that authorized parties should be able to access the information upon request. Occasionally, the list is expanded to include "accountability," which is the requirement that an entity's activities be uniquely traceable to that entity.

Making sure that systems are consistently reliable in the face of many forms of malicious activity, especially denial-of-service assaults, has effectively become the primary objective of contemporary information security. Network topologies' dominance affects how protection policies are formulated and, in turn, how suitable protection initiatives, objectives, tactics, and tools for problem-solving are chosen.

I. Cybersecurity as an information technology issue: With a particular emphasis on internet security, cybersecurity can be viewed as an IT security or information assurance issue. Therefore, policies are designed to use technological tools like firewalls, antivirus software, or intrusion detection software to combat threats to the information infrastructure. The primary anticipated risks are cyber attacks, human error, system malfunctions, accidents, and poor programming.

II. Cybersecurity as an economic issue: Cybersecurity is important for business continuity, particularly for e-business, which, to guarantee optimal company performance, needs constant access to ICT infrastructures and business processes. Private sector representatives are the primary players. Viruses, worms, human error, hacker assaults of all kinds, and cybercrime are the biggest dangers.

III. Cybersecurity as a problem for law enforcement: Cybercrime is seen to be related to cybersecurity. The word "cybercrime" is fairly wide and can refer to anything from crimes against individual computers to crimes made possible by technology. Law enforcement officials are the primary actors. Cyberterrorism and computer crime are the two biggest concerns.

IV. Cybersecurity is a national security issue: Because they rely on ICT, society and its fundamental principles are in peril. The danger is being addressed on a number of levels, including the organizational, international, legislative, and technical levels. Security experts are the primary players. Terrorists pose the biggest threat, but other governments also pose a threat from information warfare.

3 | Theoretical Review

A study's theoretical framework, according to[21], is a structure that may hold or support a research work's theory. It lays forth the hypothesis that explains the existence of the issue being studied. Therefore, the theoretical framework is only a hypothesis that provides a foundation for study. Your study is guided by a theoretical framework that establishes the variables you will measure and the statistical associations you will seek. The following will be used by the researcher in this investigation: Theory of technology-enabled crime, routine activity theory, Marxian theory, and structural-functionalism theory.

3.1 | Structural Functionalism Theory

The structural-functional theory's central finding is that crime and deviance are essential components of social organization. According to this theory, society is an organism made up of several components that work together to contribute to its overall efficacy and efficiency. According to the consensus theory known as structural-functionalism, society is based on balance, order, and relationships between its many components in order to preserve the seamless operation of the whole.

According to the idea, social order is founded on unspoken agreements between groups and organizations, shared norms and values form the foundation of society, and social change happens gradually and in a planned manner. When Merton [22]wrote in the middle of the 1930s, he believed that crime and deviance were reactions to the failure to accomplish societal objectives. This theory of crime is known as the "anomie theory" because Merton [22]emphasizes a conflict or strain between:

I. A society's cultural objectives, and

II. The accepted or formalized methods by which these objectives are accomplished.

The idea is relevant to this study because it helps us realize that crime and deviance are not the result of a few "bad apples," but rather are an essential part of "good" social existence. As a result, Nigeria's government should pass legislation and establish institutional structures to uphold law and order and cybersecurity to reduce crime.

3.2 | Marxian Theory

The theory's central finding is that crime is a natural byproduct of capitalism and that society is always evolving in reaction to social conflict and inequality. The foundation of capitalism as an economic system is the private ownership of property, which promotes individual wealth rather than the welfare of the group. According to the thesis, capitalism both contributes to and is a crime in and of itself. Its foundation is the economic exploitation and oppression of the majority, which fosters a competitive environment that is conducive to corruption, violence, and greed.

According to Giddens [23], Bonger [24] offered a very early understanding of Marxian concepts related to crime and deviance. Bonger[24] believed that people are naturally altruistic and not competitive. According to Bonger[24], capitalism as an economic system breeds selfishness and greed in people. Following Bonger's[24], in Giddens[23], contends that the working class is oppressed by the law under capitalism. He contends that only until capitalism itself is eradicated will what we currently consider to be "criminal" cease to exist.

He argues that under socialism, there won't be any greed or profit-seeking, and the ruling class won't have the power to utilize the law as a tool to label working-class behaviors that they don't want to permit as criminal or deviant. The Marxian hypothesis is pertinent to this research since it offers a substantial explanation for why individuals commit crimes, particularly young people without jobs. It is hardly surprising that cybercrime is so common in Nigeria given the country's high levels of political, economic, and corruption instability.

A portion of the majority's disadvantaged members have turned to alternate methods of survival as a result of the majority's oppression, exploitation, and alienation for the elites' gain. These other methods include, among other things, armed robbery and prostitution. It is evident that some factors, including extreme poverty, relative social deprivation, widespread corruption, excessive materialism and greed, and others, have affected crime in Nigeria.

3.3 | Routine Activity Theory

Cohen and Felson [25] introduced the Routine Activity Theory in Miller [26]. They argued that three conditions had to be met for a crime to occur: a motivated criminal, a suitable target, and the lack of competent guardians. According to the notion, crime is common and contingent on the circumstances. Crime will occur if a target is not sufficiently protected and if the payoff is worthwhile. Hardened criminals, super predators, convicted felons, and evildoers are not necessary for crime. All crime requires is an opportunity. According to this, for a crime to be committed, three conditions must be met simultaneously and in the same location:

I. There is an appropriate target available.

II. The absence of an appropriate guardian to stop the crime from occurring

III. There is a motivated and probable criminal present.

The theory is pertinent to this research since it offers a substantial insight into the motivations for cybercrime. The efficacy of indirect guardianship is more closely related to cybercrime, which is why it occurs. Additionally, the Global Information Infrastructure (GII) is unrestricted and open, and the Internet's processes are made to move data, not to analyze it.

3.4 | The Theory of Technology-Enabled Crime

In order to help society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and challenging types of crime to prevent, investigate, and control, the theory integrates a number of criminological theories. This is its main insight. According to McQuade [27], it might be challenging to comprehend and sustain somewhat complicated crime at first, and law enforcement and criminals are always competing for technological advantages. To avoid, regulate, dissuade, and prevent new types of crime, law enforcement must keep up with the imaginative and novel ways that criminals are committing crimes. According to McQuade [28], the notion of technology-enabled crime includes:

I. Direct crimes against computers and computer systems,

II. High tech crime, computer crime, or cybercrime are terms frequently used to describe these types of activities.

III. The use of technology to commit or assist in the commission of traditional crimes, and

IV. The use of technology to enable crimes like fraud, scams, and harassment presents special difficulties for traditional crimes.

The theory offers a framework for comprehending all types of criminal activity, particularly those that are developing in tandem with advancements in computing and telecommunications technology. The idea is relevant to comprehending current dangers from transnational crime, cybercrime, and terrorist networks that challenge established criminal justice and security mechanisms for crime prevention and control. Because it gives us insight into the new tools and tactics used by cybercriminals that is, the transition from basic crimes performed with simple tools to complex crimes conducted with sophisticated tools the theory is pertinent to this study. It also aids in comprehending novel types of criminal activity, social abuse, and deviance that involve creative use of technology.

4 | Methods

The study used the survey research approach and is descriptive. The survey research approach was chosen due to its effectiveness in determining the circumstances that were in place at a particular moment in time[29]. If properly built, it provides accurate and trustworthy information. According to Aina (2002), research techniques and data-collecting instruments are the two fundamental processes that make up study design. Creswell and Creswell [29] asserts that a survey study design frequently concentrates on a population's characteristics. These are certain population-level phenomena of relevance. Its outcome is easily analyzed for prompt action or required intervention. Two law enforcement agencies and one government agency focused on cybersecurity comprise the study's population.

The sample used in this investigation was non-probability. Purposive sampling is a non-probabilistic sampling method that was applied in this investigation. Because the researcher is interested in a specific group of stakeholders in cyber operations who have a wealth of information, this approach was chosen. The following sample sizes were used for every research population type. Data was gathered from representatives of the following organizations: The National Information Technology Development Agency (NITDA), which represents the cyber-security agency; the Nigeria Police Force (NPF); and the EFCC, which represents law enforcement agencies.

To learn more about the strategies used by Nigerian law enforcement organizations and cyber-security stakeholders to prevent cybercrime and maintain cyber-security, the following questions were posed to the EFCC, NPF, and NITDA during the interview section:

I. How do law enforcement organizations in Nigeria spot cybercrime activity?

II. How do law enforcement organizations in Nigeria obtain evidence to support convictions?

III. What tools or provisions of the Nigerian Criminal Law are available to combat cybercrime?

IV. How is cyber-security maintained by your organization?

V. What obstacles has your company faced in the fight against cybercrime?

VI. Do you think the fight against cybercrime is going well?

VII. Are there any recent instances of cybercrime in Nigeria that highlight the significance of anti-crime legislation?

VIII. How well-informed do you think the Nigerian public is on cybercrime and cybersecurity?

5 | Results

5.1 | Information Obtained from Law Enforcement Agencies

According to the information gathered, the Nigerian Police Force (NPF) and the EFCClearn about cybercrime activity through periodic evaluations of cybercafés, Internet monitoring, and complaints and reports from victims. Typically, forensic investigation of the suspects' computer systems and other tools used to carry out the crime provides them with evidence to support a conviction. In addition to these methods, further evidence utilized to guarantee the conviction of individuals who may be guilty includes victim oral testimony, correspondence between the suspects and the victims, and Internet Protocol address data from Internet Service Providers (ISPs).

The only laws in Nigerian criminal law that may be used to prosecute cybercriminals are the Advance Fee Fraud Act of 2006, the Money Laundering Act of 2004, section 12(1)(c)–(d), the EFCC Act of 2005, and the Evidence Act of 1948. By registering all potential cybercafes and educating the public, these security organizations guarantee cybersecurity. Insufficient provisions for cybercrime in the criminal code, non-registration of SIM cards and Internet modems, non-cooperation from telecoms and ISPs, a shortage of trained personnel, and a lack of regular training opportunities are some of the difficulties they face while carrying out their responsibilities to ensure cyber-security.

Duplication of duties and responsibilities among law enforcement agencies regarding cybercrime activities and Nigerian judges' lack of understanding of cybercrime issues and technicalities are also pertinent. The Nigerian Police Force (NPF) did not report positive results, attributing this inefficiency to a lack of information technology skills, funding, and the necessary motivation to effectively engage cybercriminals. The EFCCreports positive results in the fight against cybercrime because of regular raids of public Internet cafes, arrests, and the prosecution of suspects.

The case of Akeem Adejumo v. National Aeronauticand space agency of the United States is the most recent cybercrime case that highlights the significance of having a cybercrime law. The low penetration of Internet access, widespread illiteracy, and the incapacity of Internet users to take preventative measures are the reasons given by law enforcement agencies for their perception of a low level of general awareness of cybercrime and cybersecurity among Nigerian Internet users.

5.2 | Information Obtained from a Governmental Agency

According to the NITDA, Section 14 of the Nigerian Constitution, which declares that "no person shall be punished for a crime unless such crime is prohibited by written law and specific penalties are provided for the violation," is the main obstacle to identifying cybercrime activities. Because no written legislation in Nigeria forbids any online activity, there is no such thing as cybercrime. Since there are no specific legal provisions or tools in the Nigerian Criminal Law that deal with cybercrime, the agency reports that law enforcement agencies obtain evidence to support convictions through methods other than electronic evidence.

Through interactive sessions with the Bankers' Committee and law enforcement agencies, public education programs, and capacity development seminars on cybercrime, the agency supports efforts towards cybersecurity. Additionally, they partnered with the private sector to establish network security regulations, sponsored the cybercrime bill, and collaborated with the Law Reform Commission to update the Evidence Act. The fact that they are not a law enforcement organization is one of the difficulties they have when performing their tasks.

They also face the difficulty of the general public, law enforcement, and policymakers having very little understanding of cybercrime [30]. For example, Nigerian banks refuse to share information on cyber-security threats they receive with the law enforcement. Additionally, organizations lack institutional memory since individuals who may have received cybercrime training are occasionally assigned to roles where their learned knowledge may not be beneficial to the organization.

Another issue is the lack of financing, which makes it hard for them to equip and educate staff and set up a forensic laboratory. Although the agency acknowledges the relative achievements of the different law enforcement organizations, it notes that the Nigerian government frequently responds to the current circumstances. For example, we established ICPC when corruption became a significant problem, NDLEA when hard drugs became a problem, NAFDAC when fake medications became a problem, and so on.

According to the agency, attempts to present electronic evidence in court have been unsuccessful in a number of cases. The well-known Femi Fani-Kayode case serves as a prime example, in which the court denied the printed statement of accounts due to the Evidence Act's requirement that you provide a ledger, which is now not used by any banks. Regarding the broad understanding of cybercrime and cyber-security in Nigeria, the agency believes that most people only associate them with “Yahoo Yahoo Boys,” although there are other equally important aspects of the issue.

6 | Discussion

6.1 | Strategies Used by Nigerian Law Enforcement to Combat Cybercrime

The advance fee fraud act of 2006, the money laundering act of 2004 section 12(1)(c)–(d), the efcc act of 2005, and the evidence act of 1948 are the available enabling criminal laws that law enforcement agencies use, but they are insufficient to directly address the threat of cybercrime. Therefore, in order to combat cybercrime and guarantee cybersecurity, a suitable cyberlaw is urgently needed.

In addition to laws, law enforcement agencies must be given sufficient funding so they may purchase the instruments, apparatus, and expertise required for effective network system security against cyberattacks. If law enforcement agencies lack the expertise and training required to even operate a computer, then laws designed to prevent cybercrimes are pointless. Judges also need to be well-trained.

6.2 | Strategies Used by Nigeria Government to Guarantee Cybersecurity

However, these are insufficient; proactive measures are needed to ensure cyber safety on the Internet. For example, the International Telecommunication Union (ITU) toolkit is used to ensure cybersecurity. The government cyber-security agency ensures cyber-security through capacity building, workshops on cybercrime, public enlightenment programs, interactive sessions with the Bankers' Committee and law enforcement agencies, sponsoring the cybercrime bill, working with the Law Reform Commission to update the Evidence Act, and partnering with the private sector to set network security regulations.

A useful tool for developing a cyber-security legal framework and associated legislation is the ITUtoolbox. Furthermore, governments and the private sector must communicate, coordinate, and work together in order to fully align the policies, practices, and processes that will be used to address this issue. To tackle the difficulties of global technology and its associated issues, legislation at the national, regional, and international levels must be harmonized. But when it comes to forensic labs, Nigerian law enforcement and cyber-security government organizations are different.

Through forensic examination of suspects' computer systems and other tools used to commit the crime, the Nigerian Police Force (NPF) and the EFCCassert that they can obtain evidence to support convictions. However, the NITDAconfirmed that, due to the lack of forensic laboratories, law enforcement authorities get evidence to support convictions using any method other than electronic evidence.

6.3 | Factors Militating Against Nigerian Law Enforcement Agencies and Government in Combating Cybercrime

Odumesi[20] noted the following issues impeding Nigerian law enforcement agencies to effectively tackle cybercrime:

I. There is currently no legislation that effectively addresses the issues posed by technology, such as online crime and security breaches. Therefore, it is impossible to punish perpetrators when there are no laws (Legislation) to handle Internet criminality.

II. It has been challenging to identify and separate the actual criminal behavior that could be attributed to Nigeria on the Internet due to the lack of a national Internet gateway.

III. Inadequate infrastructure and national framework for managing and preventing electronic payment fraud and other cybercrimes. Therefore, the cost of system infrastructure cannot be borne by any one Nigerian law enforcement agency.

IV. The amount and scope of cybercrime damages in the nation are not sufficiently documented.

V. The Nigerian police and other law enforcement organizations lack a computerized forensic laboratory to look into and analyze cybercrime-related issues, and the officers themselves lack computer literacy.

VI. There is no centralized government organization that compiles and disseminates statistics on cybercrime in Nigeria's law enforcement authorities.

6.4 | Theories of Crime about Nigerian Cybercrime

In order to comprehend cybercrime in Nigeria, the researcher employed four theories of crime. The results are as follows:

I. According to the structural-functionalism theory, the government should pass legislation and establish the institutional frameworks necessary to carry it out to reduce crime. Concerning Nigeria, the government requires the implementation of a cyberlaw to meet the dynamic nature of cybercrime and cybersecurity concerns.

II. Marxian theory adopts the stance that crimes are simply actions that go against the interests of the elite and that crime will end when capitalism does. Cybercrime is an attitude that many offenders adopt. They view it as a source of income in a challenging economic climate that mostly impacts foreigners. Based on the disposition of criminals, the theory still offers some insight into the causes of cybercrime and cybersecurity threats in Nigeria, despite the fact that the country is not a pure capitalist economy. The main reasons why criminals commit cybercrime are unemployment, deprivation, and the need to emulate the higher socioeconomic statuses of those they observe who do not have easily visible sources of income to support their wealth.

III. The routine activity idea states that crime will only be performed if a potential offender feels that a target is acceptable and a capable guardian is absent. It is their judgment of a scenario that decides whether a crime will take place. The hypothesis is pertinent to Nigeria as the inefficiency of indirect guardianship is a major factor in cybercrime activities, which in turn catalyzes such crimes. Additionally, the GIIis unrestricted and open, and the Internet's protocols are largely intended for data transport rather than data analysis. Therefore, Nigeria's glaring absence of cyberlaw and cyberpolicing would keep encouraging Nigerian cybercriminals' actions..

IV. A framework for comprehending all types of criminal activity, particularly those that are developing with the use of ICT, is provided by the theory of technology-enabled crime. With regard to Nigeria, the theory gives us a clear understanding of the new instruments and methods employed in cybercrime. Changes brought about by the globalization of business and the rise of new economies, advancements in information digitization, the pervasive use of broadband services, mobile devices, and wireless technology, the development of electronic payment systems, and modifications in how governments use technology to enable citizens to interact with government organizations. Along with advantages, these and other innovations also bring threats. Therefore, it should come as no surprise that Nigeria's GII presents chances for illicit activity such as online advance fee fraud, identity theft, financial/investment scams, phishing, job scams, and more.

7 | Conclusion

As the Internet came into widespread commercial use, the nature of computer crimes began to shift [37]. While in some crimes, one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as a whole is committed in the online or electronic environment. These crimes, known as cybercrimes, generally occur in the virtual community of the Internet or in cyberspace. As a result of this, all innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of information technologies.

Unquestionably, the government's policies of Internet penetration and telecom liberalization have resulted in an unparalleled expansion of ICT, increasing reliance on technology by Nigerians, businesses, and governments to provide both essential and basic services. Therefore, a cyber-security framework is required to support these significant government initiatives, safeguard and preserve the underlying ICT infrastructures, and increase public and consumer confidence. Since it will affect how we are perceived in this global village, cybersecurity is a reality that needs to be addressed immediately.

The modern world is undergoing a significant transition, and tangible transactions in every aspect of daily life, from banking to managing our hybrid power plants, will be completed online. Therefore, a cyber-activities legislation is required to protect Nigerians living in Nigeria as well as foreigners who wish to invest there. Because of its complexity, cybercrime has proven to be challenging to combat. One of the most important steps in establishing a trustworthy environment for individuals and businesses is extending the rule of law into cyberspace.

Since legislation to properly prevent cybercrime is still being developed, it is vital for people, organizations, and the government to come up with solutions to secure their data and networks. More resources should be allocated to educating and raising knowledge of security procedures to provide this self-protection. Individuals, companies, and the government should concentrate on putting cyber-security strategies into action that address people, process, and technology challenges.

As a result, no one solution can guarantee cybersecurity and eliminate the threat of cybercrime. However, the most effective and efficient way to decrease risks will be through the combination of measures, as well as the sincerity and rigor with which they are administered and performed. Additionally, all Nigerians must possess information technology intelligence in addition to an understanding of it to combat cybercrime and cybersecurity concerns.

8 | Recommendations

According to the study's conclusions, cybercrime poses a serious risk to a country's peace, security, and economy. To combat this crime and guarantee cyber-security in all its implications, a comprehensive strategy is thus required. To do this, the researcher recommends the following strategies to prevent cybercrime and guarantee cybersecurity in Nigeria:

I. To address the ever-changing nature of cyber security risks, the priority is to evaluate current criminal laws and implement Nigerian cyberlaw.

II. Every law enforcement agency's investigative section should have a forensic laboratory.

III. Make sure that law enforcement agencies have access to progressive capacity-building programs on cybercrime and cybersecurity.

IV. To improve legislative frameworks for cyber-security, there should be a mutually beneficial interaction between businesses (Particularly ISPs), the government, and civil society.

V. Create a national framework for cybersecurity technologies that outlines baselines and requirements for each network user.

VI. Create, promote, and uphold a national security culture by standardizing and coordinating cybersecurity awareness and education initiatives at the elementary, secondary, and university levels of education.

VII. Lastly, it is crucial to remember that pervasive corruption, a difficult economic environment, and extreme poverty are all intertwined with cybercrime.

The Nigerian government must fight crime by addressing the root causes, which in this case include good governance, open elections, and government accountability. These measures put food on the table, improve schools and jobs, create a more equitable investment environment, and eventually lessen our citizens' propensity to engage in cybercrime. Along with the researcher's suggestions, Ehimen and Bola [31] made the following suggestions to combat cybercrime in Nigeria:

I. Cyber police should be established by the government and properly educated to deal with cybercrimes in Nigeria. To help the state and other law enforcement agencies guide and coordinate computer crime investigations, the police should establish a central computer crime response unit.

II. To provide guidelines, policies, and standards for network security protocols, the government should establish the national computer crime resource center, which should be made up of professionals and experts.

Given the inadequate nature of international legal protection against cybercrime, Ayofe and Oluwaseyifunmitan[32] proposed (In terms of security, education, and regulation) the following:

I. Make sure that all relevant local laws complement and are consistent with international laws, treaties, and conventions, including the Convention on Cybercrime of the Council of Europe.

II. Developing a framework for managing information security risks at all levels and establishing a framework for implementing information assurance in important economic sectors like public utilities, telecommunications, transportation, tourism, financial services, public sector, manufacturing, and agriculture.

III. Creation of an institutional framework in charge of information security situation monitoring, information security risk management, including reporting incidents and breaches, and the distribution of advisories on the most recent information security alerts.

IV. Businesses should protect their network data. Organizations can enforce property rights rules and penalize those who meddle with their property when they offer security for their networks [33].

V. Enhancing knowledge and proficiency in information security and exchanging best practices by fostering a cyber-security culture at all levels.

VI. Encourage safe online shopping and e-government services.

VII. Protecting people's right to privacy when utilizing technological communications.

Formalize the coordination and prioritization of cyber security research and development activities; disseminate vulnerability advisories and threat warnings promptly.

Implement an evaluation/certification programme for cyber security products and systems.

United Nations[34] outlined the following recommendations to be considered by countries in fighting cybercrime:

I. Cybercrime issues require a comprehensive, inclusive approach that goes beyond criminal legislation, penal processes, and law enforcement. Together with strategies to support and safeguard the innovation and wealth-creating potential and opportunities of information and computing technologies, such as early warning and response mechanisms in the event of cyberattacks, the focus should include requirements for the safe operation of a cyber-economy that maximizes business confidence and individual privacy. The bigger issue of fostering a worldwide culture of cyber-security and meeting the demands of all societies—including developing nations with their still-emerging and precarious information technology structures—lies behind the prevention and punishment of computer-related crimes.

II. There should be more development of international collaboration at all levels. Because of its universal nature, the United Nations system should play a leading role in intergovernmental efforts to guarantee the operation and protection of cyberspace so that criminals and terrorists cannot abuse or exploit it. This is especially true with the improved internal coordination mechanisms that the general assembly has called for. In order to prevent and lessen the detrimental effects of cybercrime on vital infrastructure, sustainable development, privacy protection, e-commerce, banking, and trade, the UN system should play a key role in promoting international strategies for fighting cybercrime and protocols for international cooperation.

III. To meet the unique characteristics of cybercrime, all states should be urged to amend their criminal laws as quickly as feasible. This updating may be accomplished by establishing new provisions for new crimes, such as unauthorized access to computers or computer networks, or by clarifying or eliminating outdated provisions that are no longer fully appropriate, such as statutes that cannot address the destruction or theft of intangibles. Procedural laws (For example, tracking communications) and agreements or arrangements on mutual legal assistance (For example, quick data preservation) should also be included in this updating. States should be urged to draw inspiration from the provisions of the Council of Europe Convention on Cybercrime when assessing the robustness of new legislation.

IV. To close the digital divide, increase public awareness of the dangers of cybercrime and implement suitable preventative measures, and strengthen the capabilities of criminal justice professionals, including law enforcement officers, prosecutors, and judges. Governments, the private sector, and non-governmental organizations should collaborate. For this reason, a thorough curriculum on computer-related crime should be a part of the teaching schedules of national judicial administrations and legal education institutions.

V. To guarantee efficacy and efficiency, cybercrime policies should be supported by evidence and rigorously reviewed. The establishment of financing mechanisms to support applied research and prevent numerous forms of newly developing cybercrime should thus be the focus of coordinated and concentrated international efforts. Nonetheless, it is equally crucial to make sure that research is coordinated globally and that the findings are publicly accessible.

Further studies

Due to the severity of their cybercrime offenses, which totaled one million naira (₦1,000,000), the arrested cybercriminals in the Advance Fee Fraud Unit of the Economic and Financial Crimes Commission (EFCC) and the Special Fraud Unit of the NPFcould not be assessed. Therefore, further research will be necessary to understand the sociological and demographic characteristics of cybercriminals. Finally, it was suggested that more research be done on the social and demographic traits of Nigerian cybercriminals to determine the elements that contribute to their continued involvement in cybercrime.

Author Contributions

OJI: Conceptualization, Writing - original draft, Introduction, Method, Editing. OTO: Conceptualization, Proofreading, Editing. EE: Conceptualization, Proofreading, Editing, Visualization. AAG: Conceptualization, Proofreading, Editing. YVO: Editing. The authors read and approved the final manuscript.

Institutional Review Board Statement

Not applicable.

Data Availability

Data is provided within the manuscript.

Funding

This research received no external funding.

Acknowledgement

The authors appreciate the editor and reviewers for adding valuable input to the manuscript.

Ethics Approval and Consent to Participate

Not applicable

Clinical Trial Number

Not applicable.

Informed Consent Statement

Not applicable

Consent to Publish

Not applicable

Conflicts of Interest

The author declares that there is no competing interest.

References

[1] Adeniran, A. O., Jadah, H. M., & Mohammed, N. H. (2020). Impact of information technology on strategic management in the banking sector of Iraq. *Insights into regional development*, *2*(2), 592–601. https://dx.doi.org/10.9770/IRD.2020.2.2(7)

[2] Brenner, S. (2007). *Law in an era of smart technology*. Oxford University Press.https://doi.org/10.1093/acprof:oso/9780195333480.001.0001

[3] Longe, O. B., Chiemeke, S. C.(2008). Cyber crime and criminality in Nigeria: What roles are internet access points in playing? *Journal of information technology impact*, *9*(3), 155–172. https://www.researchgate.net/deref/https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F228876250_Criminal_Uses_of_Information_Communication_Technologies_in_Sub-Saharan_Africa_Trends_Concerns_and_Perspectives%3FenrichId%3Drgreq-1e01304b72b5b1f9a0cc601d6b3e6315-XXX%26enrichSource%3DY292ZXJQYWdlOzIyODg3NjI1MDtBUzoxMDIyOTg2OTI4ODI0MzZAMTQwMTQwMTMxNzQ1Mw%253D%253D%26el%3D1_x_2%26_esc%3DpublicationCoverPdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

[4] Adeniran, A. O., Onuajah, S. I., Adeniran, A. A., & Ogunmola, M. A. (2024). Implementing cloud-centric IoT transformations: Merits and demerits. *Systemic analytics*, *2*(2), 174–187. https://doi.org/10.31181/sa22202422

[5] Adeniran, A. O. (2018). Assessment of federal governments' effort on looted assets recovery in nigeria as a means of fighting corruption and terrorism. *Discovery*, *54*(276), 453–462. https://www.researchgate.net/publication/329453250_Assessment_of_federal_governments'_effort_on_looted_assets_recovery_in_Nigeria_as_a_mea

[6] Adeniran, A. O., & Obembe, O. E. (2020). The significance of strategic management accounting on the performance of transport businesses in Nigeria. *Insights into regional development*, *2*(3), 677–688. https://dx.doi.org/10.9770/ird.2020.2.3(5)

[7] Aluko, M. (2004). *17 ways of stopping financial corruption in Nigeria*. https://dawodu.com/aluko103.htm

[8] Ullah, F., Ali, A., & Umar, Z. (2021). Understanding cybercrime and youth: A perception based approach. *Pakistan journal of social research*, *3*(3), 130–136. https://pdfs.semanticscholar.org/529a/dc0cadf9741234f5a89c5dde7713c2368a86.pdf

[9] Matthew, O. F. (2016). Sociological and technological factors that enhance cybercrime and cyber security in Nigeria. *International journal of law and legal studies*, *4*(5), 207–216. https://www.internationalscholarsjournals.com/articles/sociological-and-technological-factors-that-enhance-cybercrime-and-cyber-security-in-nigeria.pdf

[10] Yar, M. (2005). The Novelty of 'cybercrime' an assessment in light of routine activity theory. *European journal of criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

[11] Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal justice matters*, *58*(1), 22–23. https://doi.org/10.1080/09627250408553240

[12] Wall, D. (2003). Maintaining order and law on the internet David Wall. In *Crime and the internet* (p. 167). Routledge.https://doi.org/10.4324/9780203299180-14

[13] Lastowka, F. G., & Hunter, D. (2004). Virtual crimes. *New york law school law review*, *49*(1), 306–310. https://doi.org/10.18574/nyu/9780814739075.003.0009

[14] Grabosky, P. N. (2017). Virtual criminality: Old wine in new bottles? In *Cyberspace crime* (pp. 75–81). Routledge. https://doi.org/10.1177/a017405

[15] Cernomoreţ, S., & Nastas, A. (2023). *Comparative analysis of cybercrime in the criminal law system*. Adjuris-International Academic

Publishers.https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf

[16] Mann, D., & Sutton, M. (1998). Netcrime: More change in the organisation of thieving. *British journal of criminology*, *38*(2), 201–229. https://irep.ntu.ac.uk/id/eprint/25206

[17] Loader, B. D., & Thomas, D. (2013). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.https://doi.org/10.4324/9780203354643

[18] Canada, S. (2002). *Canadian community health survey cycle 1.2: Mental health and well-being*. https://www150.statcan.gc.ca/n1/en/catalogue/82C0026

[19] ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International cybersecurity law review*, *4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

[20] Odumesi, J. O. (2014). Combating the menace of cybercrime. *International journal of computer science and mobile computing*, *3*(6), 980–991. https://www.researchgate.net/profile/John-Odumesi/publication/263967391_Combating_the_Menace_of_Cybercrime/links/00b4953c7613e08fbd000000/Combating-the-Menace-of-Cybercrime.pdf

[21] Khan, E. R. (1999). *Developing the theoretical and conceptual framework*.http:// journclasses.pbworks.com/f/theoretical+framewor.ppt

[22] Merton, R. K. (1938). Social structure and anomie. *American sociological review*, *3*(5), 672–682. https://doi.org/10.2307/2084686

[23] Giddens, A. (2001). *The scope of sociology*. Politics & Social Sciences.https://www.amazon.com/Sociology-Anthony-Giddens/dp/0745623115

[24] Bonger, W. A. (1916). *Criminality and economic conditions*. Boston: Little, Brown.https://books.google.com/books?hl=en&lr=lang_en&id=CMAtAAAAIAAJ&oi=fnd&pg=PR11&dq=Bonger,+W.+A.+(1916).+Criminality+and+economic+conditions&ots=ycwC3z1W-O&sig=iEbzGhhBX5gaqyLWzLDElqJPAR0

[25] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

[26] Miller, J. (2013). Individual offending, routine activities, and activity settings: Revisiting the routine activity theory of general deviance. *Journal of research in crime and delinquency*, *50*(3), 390–416. https://doi.org/10.1177/0022427811432641

[27] McQuade, S. (2001). *Technology-enabled crime, policing and security*. Abingdon: Routledge.https://doi.org/10.21061/jots.v32i1.a.5

[28] McQuade, S. C., & Wellford, C. F. (2006). *Understanding and managing cybercrime*. Pearson/Allyn and Bacon Boston.https://www.ojp.gov/ncjrs/virtual-library/abstracts/understanding-and-managing-cybercrime

[29] Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf

[30] Adeniran, A. O., Muraina, J. M., Ilugbami, J. O., & Adeniran, A. A. (2023). Government policy: Meaning, types, manifestations, theories, and policy cycles. *Insights into regional development*, *5*(2), 83–99. http://doi.org/10.9770/IRD.2023.5.2(6)

[31] Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business intelligence journal*, *3*(1), 93–98.https://www.academia.edu/download/31076494/BIJ-Vol3No1.pdf#page=95

[32] Ayofe, A. N., & Oluwaseyifunmitan, O. (2009). Approach to solving cybercrime and cybersecurity. *(IJCSIS) International journal of computer science and information security*, *3*(1), 1–11. https://doi.org/10.48550/arXiv.0908.0099

[33] Adeniran, A. O., & Olorunfemi, S. O. (2020). The essence of knowledge management in the air transportation sector. *International journal of human capital in urban management*, *5*(2), 176–186. https://doi.org/10.22034/IJHCUM.2020.02.08

[34] UnitedNations. (2005). *UN recommendations on fighting cybercrime*. http://www.crime-research.org/news/13.05.2005/1225/ 25th

[35] Abdulhamid, S.M, Haruna, C., & Abubakar, A. (2011). Cybercrimes and the Nigeria academic institution networks. *The IUP Journal of Information Technology*, *VII*(1), 11.

[36] Ajewole, A. (2010). Curbing cybercrime in Nigeria. Fighting the masked enemy and promoting productive alternative for the youth. Available at: http/www.primopdf.com.

[37] Adeniran, A. O. (2016). Impacts of the Fourth Industrial Revolution on transportation in the developing nations. *International Educational Scientific Research Journal*, 2(11), 56-60.