ASSESSMENT OF CYBER CRIME REGULATIONS IN NIGERIA

BY

EMMANUEL Judith Omonese
LAW1805930

FACULTY OF LAW
UNIVERSITY OF BENIN
BENIN CITY

JUNE, 2024

CHAPTER ONE

1.1 Introduction

The ubiquity of digital technology and the integration of computing and communication devices have bridged geographical distances and facilitated global connectivity.it's amazing how we can now interact with people from different parts of the world with just a few clicks and taps. In less than 5 decades, the internet has expanded dramatically.transforming the way we communicate, acquire information and run businesses. it's really fascinating how the internet has evolved and become an integral part of our lives.it has transitioned from a novelty to a crucial component that we rely on daily. Data[1]estimates that the total number of internet users at the end of 2023 was around 5.3 billion, which amounted to 65.7 percent of the global population, of this total, 4.95 billion, or 61.4 percent of the world's population, were social media users [2]. While the technological advancement has brought myriads of advantages and improvements to various aspects of our lives.there's also a downside to these development: an unfortunate increase in criminal activities.As opportunities arise so does the potential for crime; almost every stride is accompanied by an opportunity for criminals to exploit.Starting from the emergence of viruses, worms, and other malicious software in the 1980s and 1990s, the 2000s witnessed a surge in identity theft, online scams, and financial fraud[3]. Subsequently, cybercrime continues to evolve, with new threats like ransomware and social engineering techniques.

Cybercrimes are simply offences carried out using computers or the internet. They encompass computer related forgery[4], identity theft[5], system interference[6], phishing[7], cyber

---

[1] Ani petrosyan, 'Global number of internet users 2005-2003' April 15,2024 .available at https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/#:~:text=As%20of%202023%2C%20the%20estimated,67%20percent%20of%20global%20population. > accessed 22 May 2024

[2] Internet User Statistics in 2024-(Global Demographics) https://www.demandsage.com/internet-user-statistics/ > accessed 23 of January 2024

[3] The history of cybercrime and why cybersecurity is so important today https://www.pc-docs.co.uk/the-history-of-cybercrime-and-why-cyber-security-is-so-important-today/ accessed 27 January 2024

[4] See section 13, of the Cybercrimes (Prohibition, Prevention etc.)(amendment)Act, 2024.

terrorism[8].cyber squatting[9] child pornography[10] etc.

Essentially, any crime committed using a computer as a tool is generally considered a cybercrime. Section 258 of the Evidence Act, 2011 (Nigeria) defines "computer" as any device for storing and processing information. Also, section 58 of the Cybercrimes Act defines "computer" as: an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols.

Currently, the global community has recognized the need for cybercrime laws. These laws are being developed to address the specific challenges and offenses that occur in cyberspace. Implementing these regulations is essential to protect individuals and organizations from the increasing threats in the digital world.

1.2 Background of the Study

This study examines the burgeoning menace of cybercrime and the regulations that have been put in place to safeguard individuals and organisations from its escalating threat.

Nigeria, just like other numerous nations has acknowledged the need to tackle cybercrimes.The government has implemented various laws and regulations to combat cybercrimes. Enacting laws on advance fee fraud was one of the Nigerian Government's earliest intervention in addressing cyber crimes ,but the law is inadequate to address the complexities of technological advancement.The latest legal provisions concerning cybercrimes in Nigeria is the Cybercrimes (Prohibition and Prevention etc) Act, 2015 and its recent amendments in 2024.The acclaimed targets of this act include the establishment of a

[5] Ibid section 22
[6] Ibid section 8
[7] Ibid section 32
[8] Ibid section 18
[9] Ibid section 25
[10] Ibid section 23

robust and integrated legal, regulatory, and institutional structure for combating cybercrimes in Nigeria. In addition to this Act, complementary regulations like the National Information Technology Development Agency (NITDA) Guidelines on Data Protection and the Central Bank of Nigeria (CBN) Guidelines on Electronic Banking contribute to the overall framework for addressing cyber threats.

Data estimates that the total number of internet users at the end of 2023 is around 5.3 billion, which amounted to 65.7 percent of the global population.[11]

While in Nigeria,As of 2022, the estimated number of internet users in the country was more than 108 million[12] in January 2023 there were 122.5 million internet users in Nigeria when Nigeria's internet penetration rate stood at 55.4 percent of the total population at the start of 2023[13]

The rapid advancement and widespread use of information and communication technologies (ICTs)have unfortunately provided criminals with a powerful tool to carry out various types of cyber crime.In the early 2000s,Nigeria wasn't widely associated with internet criminal fraud on a global level, since then, Nigeria has gained quite a reputation for criminal activities worldwide.

In 2020,in its internet crime report, the US Federal Bureau of Investigation (FBI) ranked Nigeria 16th among the countries most affected by internet crime in the world.[14]

---

[11] Internet User Statistics in 2024-(Global Demographics) https://www.demandsage.com/internet-user-statistics/ > accessed 23 January 2024

[12]Doris Sasu,'internet user penetration in Nigeria from 2018 to 2027' Available at , https://www.statista.com/statistics/484918/internet-use Accessed > 25 January 2024

[13] internet users statistics in 2023 available at https://datareportal.com/reports/digital-2023-nigeria Accessed > 25 January 2024

[14] Nigeria ranked 16th in FBI Global cyber crime report', https://www.thecable.ng/nigeria-ranked-16th-in-fbi-global-cybercrime-victims-report/#:~:text=Nigeria%20has%20been%20ranked%2016th,to%20internet%20crime%20last%20year.> accessed 25 January 2024

According to Sophos- a cyber security firm, 71% of Nigerian firms were hit with ransomware in 2021.They also reported that Nigerian businesses paid as much as $706,452 as ransom to cyber-criminals in 2021.[15]

The frequently encountered cyber crime associated with Nigeria is the advance free Fraud also known as "419" or "yahoo yahoo ".They use the cloak of the anonymity provided by the internet and mobile phones to commit heinous acts, which has given Nigeria a reputation as a hotspot for cybercrime. Subsequently it has come to light that the categories of people who practice these nefarious act mostly fell among the youths, and thousands of them are unemployed but highly knowledgeable and skillful in the use of computers.

Poverty, joblessness rate, social influences, greed, desire for a lavish lifestyle are some of the reasons why they engage in cybercrime .

In its report, the Nigerian Communications Commission had claimed that Nigeria "is losing $500 million annually to all forms of cybercrime including hacking, identity theft, cyber terrorism, harassment and Internet fraud."[16] This clearly demonstrates the significant repercussions of cybercrime on Nigeria's economy.

As a result, the Senate decided to reassess and modify the Cybercrime (Prohibition and Prevention) Act, 2015,leading to the 2024 amendments aimed at curbing the misuse of Nigeria's digital realm by cybercriminals and individuals with misguided motives.[17]

1.3 Statement of Problem

Cybercrime remains one of the fastest-growing areas of criminal activity, leveraging the speed, convenience, and anonymity provided by modern technologies. Historically,

---

[15]Ibid

[16] statistics on cybercrime 2021 https://nairametrics.com/2023/07/12/smes-in-nigeria-w accessed > 25 January 2024

[17] Senate begins Cybercrime Act 2015 Amendment process http://brtnews.ng/senate-begins-cybercrime-act-2015-amendment-process/ accessed >25 January 2024

cybercrimes were perpetrated by individuals or small groups. However, there is a emerging trend of traditional organized crime syndicates and criminally minded technology professionals collaborating, pooling resources and expertise to circumvent existing cybercrime regulations.

Despite various regulatory efforts, including the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 and other relevant regulations aimed at curbing cybercrimes in Nigeria, the effectiveness of these laws has been questioned. The Senate has acknowledged the limitations of these regulations, highlighting their inability to adequately address the evolving nature of cyber threats. In response, the Cybercrime (Prohibition, Prevention, etc.) Amendment Act of 2024 was enacted to address these gaps, introducing stringent measures and enhancing cybersecurity infrastructure.

Nevertheless, the continued rise in sophisticated cybercrimes indicates that even with the updated 2024 amendments, there are still challenges in the regulatory framework. It is imperative that Nigeria's regulatory framework evolves continuously to align with international best practices, particularly those of the UK and US, to effectively combat cybercrime. This project recommends further updates and improvements to Nigeria's cybersecurity laws to ensure they remain robust and effective against emerging cyber threats.

1.4 Aims and objectives of study

The primary objective is to explore cyber offenses in Nigeria and evaluate the effectiveness of the existing and newly amended regulations.

The specific objectives of this study are to:

1. Examine the legal framework in Nigeria, including the recent amendments in the Cybercrime (Prohibition, Prevention, etc.) Act of 2024.

2. Comparatively analyze the United States and United Kingdom’s legal frameworks and that of Nigeria to identify strengths and areas for improvement.

3.Evaluate the impact of the 2024 amendments on combating cybercrime and suggest further revisions to enhance Nigeria's cybersecurity laws.

1.5 The Scope of the study

The scope of the study is to examine the legal frameworks of cybercrime in Nigeria, exploring the effectiveness and enforcement mechanisms of cybercrime regulations, specifically the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 and its amendments in 2024. It will explore the types and prevalence of cybercrimes in Nigeria through statistical analysis and case studies, providing insights into the most common threats and their impact on individuals and businesses.

Challenges to effective regulation will be critically assessed, including technological, legal, and operational barriers that hinder law enforcement efforts. The study will also investigate the socio-economic impacts of cybercrime on Nigerian society and its economy, emphasizing the urgent need for robust regulatory measures.

The study also involves conducting a comparative analysis of different jurisdictions to understand how Nigeria's cybercrime regulations measure up against international standards. This analysis will identify areas for improvement and ensure that the country's legal framework is in line with global best practices.

Overall, the study will propose a set of recommendations to enhance Nigeria's cybercrime regulatory framework, including policy reforms, technological advancements, and capacity-building initiatives. These recommendations will aim to equip Nigeria with the tools and strategies necessary to effectively combat the evolving threat of cybercrime and protect its digital landscape.

1.6 Significance of study

The study is significant because it contributes to the debate on the necessity to review and update the regulatory frameworks on cybercrime in Nigeria. Despite the implementation of laws such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, and the recent amendments in 2024, cybercrimes remain prevalent in Nigeria. This persistence indicates that current regulations, even with updates, may not adequately address the complexities of modern cyber threats. By pointing out specific deficiencies and weaknesses in these laws, including those in the recent amendments, the study provides a clear understanding of why existing measures are insufficient. This understanding is the first step toward creating more effective regulations.

Guiding policy reforms is another significant aspect of the study. Policymakers and legislators can utilize the insights gained from this assessment to draft and implement further revisions and updates to the legal framework. The study's recommendations, especially those advocating alignment with the legal systems of the UK and US, suggest that Nigeria can benefit from adopting international best practices. This alignment not only strengthens domestic laws but also enhances Nigeria's capacity to engage in global efforts against cybercrime.

Promoting international standards is another vital contribution of the study. Cybercrime is a global issue, and no country can combat it effectively in isolation. By recommending that Nigeria's cybercrime laws align with those of the UK and US, the study emphasizes the importance of international cooperation. Such alignment facilitates cross-border collaboration and information sharing, making it harder for cybercriminals to exploit regulatory inconsistencies between countries.

Finally, the study contributes to academic discourse on cybercrime and regulation. It provides a foundation for further research and development in this field, encouraging scholars to explore new solutions and strategies. This academic contribution is crucial for the ongoing

evolution of cybercrime regulations, ensuring that they remain relevant and effective in the face of ever-changing cyber threats.

1.7 Research methodology

The doctrinal research method is largely used in the collection of data needed for the research of this work. The research will combine both primary and secondary sources of materials. The relevant statutes and case laws will be consulted to assist in this research work.

The nature of the work also demands that much reliance will be placed on internet materials, textbooks, journals and articles written in the area will also be used.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter provides an in-depth exploration of key concepts related to cybercrime, beginning with a clarification of terms to establish a solid foundation for understanding the subsequent discussions. It delves into historical examples of cybercrime on a global scale, highlighting significant incidents that have shaped the evolution of cyber threats and criminal activities in the digital realm. the chapter examines the landscape of cybercrime in Nigeria, offering insights into prevalent forms of cyber offenses and their implications for individuals, businesses, and the nation as a whole. By analyzing the reasons behind the proliferation of cybercrime in Nigeria, the chapter aims to uncover underlying factors driving this phenomenon.

Additionally, it investigates the multifaceted impact of cybercrime in Nigeria, elucidating its consequences across various sectors and aspects of society. From financial losses and reputational damage to threats to national security and erosion of public trust. This exploration informs and prepares readers to tackle the cyber threats prevalent in our interconnected world.

2.2 What is cybercrime?

To understand cybercrime, it's important to know what a crime is. A crime is an act that the law considers punishable.[18] This means that if someone commits an act that goes against the law, they can face consequences or punishment determined by the legal system. Sir Carleton Allen explains that a crime is labeled as such because it involves wrongdoing that poses a serious threat to society's security and well-being.[19] In order to prove someone guilty of a

[18] Black's Law Dictionary, 9th Edition, page 427
[19] CK Allen. the Nature of a Crime in leaal Duties (Oxford: Clarendon. 1931)

crime, the state must show that an injury happened and the defendant caused it. The prosecution needs to prove both the prohibited conduct (actus reus) and the guilty intention (mens rea).[20] Cybercrime is a dynamic and expansive concept that defies a singular, definitive definition. Ajetunmobi observes that the rapid progress of technology complicates the task of precisely defining cybercrimes. However, he emphasizes the necessity for any definition to encompass the understanding or utilization of computer-related offenses.[21] Sean Hoar[22] defines cybercrime as a criminal activity committed on a computer network, particularly the internet. Loader[23] similarly suggests that cybercrimes encompass computer-mediated activities deemed illegal or illicit by certain entities, often conducted via global electronic networks. However, this definition overlooks the fact that not all cybercrimes occur exclusively through global electronic networks. For instance, activities like hacking can be carried out without reliance on such networks. Cyber-crime, a compound term composed of 'cyber' and 'crime,' refers to criminal activities perpetrated using computers and communication devices within the cyberspace and Internet. As Sackson[24]explains, cyber-crime encompasses a spectrum of illicit actions involving computers and networks.[25] According to the Nigerian Communication Commission, cybercrime is typically seen as a criminal offense that either focuses on using a computer for illegal activities like hacking, phishing, and spamming, or uses a computer as a tool to facilitate crimes such as child pornography, hate crimes, and computer fraud.[26]

---

[20] Hyam V DPP (1955) AC 55

[21] R.L. Ajetunmobi, "Cybercrimes (Prohibition, Prevention, etc.) Act 2015: A Review" (2014-2015) NIALS Journal of Intellectual Property, 17, page 171.

[22] Hoar, s., 'Trends in Cybercrime: The Dark Side off the Internet' (2005) Criminal Justice. Vol20(3) pp1-10 at pp 1

[23] Loader, B., Douglas T., 'Cybercrime: Security and Surveillance in the Information Age' (2000 Bertledge)

[24] M.Sackson,'Computer Ethics:Are Students Concerned First Annual Ethics Conference (1996) http://www.maths.luc.edu/ethics96/papers/sackson.doc> accessed 12 may 2024

[25] O. Oke, 'An Appraisal of The Nigerian Cybercrime (Prohibition, Prevention etc) Act 2015' http://ssrn.com/abstract=2655593> accessed 12 May 2024

[26] Nigerian Communication Commission, 'Final Report on: Eflects of Cybercrime on Foreign Direct Investment and National Development,' 15 https://www.nec.gov.ng/documents/735-nmis-effectseybercrime-foreign-direct-investment/file >accessed 12 May 2024

Legal scholars have also argued that cybercrimes essentially involve traditional crimes executed through computers. In other words, while these offenses are already defined by law, they are now facilitated and perpetrated using digital technology, serving as a substitute tool in their commission. In the past, there was deliberation over how to classify cybercrimes, whether in a narrow or broad scope. At the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two distinct definitions were presented. Narrowly defined, cybercrime entails any illicit activity conducted via electronic means with the intent of compromising the security of computer systems and the data they handle. Conversely, in a broader sense, cybercrime (also known as computer-related crimes) encompasses any unlawful behavior carried out through or in relation to a computer system or network, including activities such as unauthorized possession, and the distribution or offering of information using computer systems or networks

Some other scholars[27] defined cybercrimes as " Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". While this definition provided captures some aspects of cybercrimes, it's not comprehensive. Cybercrimes encompass a broader range of offenses beyond just harming reputation or causing physical or mental harm. There's also financial motives, which are often a key driver behind many cybercrimes.

Ehiman & Bola[28] think of cybercrime as illegal activities that impact our communication technologies. These acts include unauthorized access, illegal interception of private computer data, and data interference, which can mean unauthorized tampering like damaging, deleting, changing, or suppressing computer data.

---

[27] D. Halder, and K. Jaishanka, Cyber crime and the victimization of women: laws, rights and regulations, (Information Science Reference 2011)

[28] Ehimen, O.R. & Bola, A.Cybercrime in Nigeria. Business Intelligence Journal,(2010)3(1).

The Department of Justice in the USA, according to its Criminal Justice Resource Manual, defines computer-related crime as any illegal activity that requires knowledge of computer technology for successful prosecution.[29]

In the view of this writer, cybercrime encompasses the illicit utilization of computers and networks, encompassing unauthorized system access, interception or alteration of data, and device exploitation. This broad category encompasses various nefarious activities such as intellectual property theft, system sabotage, espionage, illegal downloads, banking fraud, dissemination of viruses, online identity theft or fraud, exploitation of children, money laundering, counterfeiting, denial-of-service attacks, and beyond. Additionally, it includes the propagation of viruses, malware, phishing, cyberbullying, hacking, online scams, and credit card fraud.

2.2.1 Cyberspace: Cybercrime takes place in an intangible digital landscape known as "cyberspace", where electronics and electromagnetic waves are used to store, manage, and communicate information across interconnected networks and their physical infrastructures. Cyberspace, also known as the "cyber-domain," refers to all aspects associated with computer networks, information technology, and the internet. This encompasses the internet itself, the multitude of interconnected computers, the institutions facilitating its operation, and the wide array of experiences it facilitates.[30]

Richard Clarke provided a clear explanation when he stated:

> Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you

[29] National Criminal Justice Information and Statistics Service (now Bureau of Justice Statistics). U.S. Department of Justice. Computer crime: Criminal Justice Resource Manual 1979.

[30] K. Okafor, "Legal Perspectives to Cyber Security in Nigeria: Bold Perspectives" in Adedeji Adekunle (ed.), Combatting Cybercrimes in Nigeria: Trends and Issues (Nigerian Advanced Institute of Legal Studies: Lagos, 2017), page 249.

> should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet, but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like send data about money flows, stock market trades, and credit card transactions. Some networks are control systems that just allow machines to speak to other machines, like control panels talking to pumps, elevators, and generators.[31]

Scholars[32] have classified cybercrimes into various types such as cyber terrorism, cyber fraud, malware, cyberstalking, spam, wiretapping, logic bombs, and password sniffing. Wada and Odulaja [33]expanded this list to include phishing and counterfeit websites. These categories are outlined below.

2.2.2 Cyber Terrorism:

Lewis[34] defines cyber-terrorism as the malicious act of using computer network to disrupt the normal processes of critical national infrastructures (such as energy, transportation, government operations), including the coercion or intimidation of public and private citizens. Cyber-terrorism differs from traditional terrorism as it operates solely within the digital realm, requiring no physical presence at the targeted site. professor Dorothy Denning describes cyber terrorism as: the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death

[31] R.A. Clarke & Robert K. Knake, "Cyber War Excerpt" page 5, available at https://richardaclarke.net/wp-content/uploads/2019/05/Cyber-War-Excerpt.pdf accessed >13 May 2024

[32] A.B. Hassan, et.al, Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Technology Science and Technology,(2012) 2(7) 626-631

[33] Wada F. and Odulaia G.O.Assessing Cyber Crime and its Impact on E-banking in Nigeria Using Social Theories. African Journal of Computing & ICTs. (2012) 5(1)69-82

[34] Lewis A.J. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.Center for Strategic and International Studies(2002)

or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[35]

One potential issue with Professor Dorothy Denning's definition is that it sets a high threshold for an incident to be classified as cyberterrorism, requiring it to result in violence or significant harm. This narrow definition may exclude acts that cause widespread fear or disruption but fall short of causing physical harm or property damage. Additionally, the requirement for attacks to be politically or socially motivated could overlook instances of cybercrime or cyberwarfare that do not have explicit ideological objectives.

Cyberterrorism presents a compelling alternative for contemporary terrorists due to its cost-effectiveness compared to conventional tactics, its ability to offer greater anonymity, the vast array of potential targets, the convenience of remote execution, the potential to impact a wider audience, and the dissemination of malicious software like viruses, Trojan horses, worms, and logic bombs. Under Nigeria's Cybercrime Act, the clause addressing cyber-terrorism is Section 18, stating that life imprisonment awaits anyone who, with terroristic intent, accesses or facilitates access to any computer system or network.[36]

2.2.3 Cyber Fraud:

Simply put, fraud is deception. When a person misleads you or lets you think something untrue to gain an advantage, they're being deceitful and engaging in fraud.

Often, fraud involves tricking someone into willingly handing over money or assets to a party who has made false representations about themselves or their offerings. "Internet fraud" encompasses any fraudulent activity that leverages online platforms, like chat rooms, emails. message boards, or websites, to lure potential victims, execute dishonest transactions, or

---

[35] G. Weimann, "Cyberterrorism: How Real Is The Threat" United States Institute of Peace,Special Report 110 (2004)10, available at https://www.usip.org/sites/default/files/sr119.pdf accessed> 13 May 2024

[36] Section 18 of Cybercrimes probibition,provesationetc)act,2015

move ill-gotten gains.[37]This term covers various schemes, including bogus investment opportunities.

Auction scams, undelivered goods, inferior product delivery, delayed or non-delivery of items, or not providing complete information about a product or the sale conditions.[38] A prevalent form of computer fraud involves the Nigerian or 419 scam,[39] named after the section of Nigerian law it contravenes. In this scheme, an unsolicited email is sent to a potential victim, claiming the sender needs assistance in transferring a significant sum of money out of Nigeria. Typically, there is an obstacle preventing the direct transfer of funds, prompting the sender to request the victim's bank account details or other personal information to facilitate the transfer. At times, the victim is asked to cover the fees for transferring the money to their account. In return, the sender pledges to share a portion of the funds. However, the perpetrator exploits the provided bank account information or other details to steal money from the victim.[40]

2.2.4 Malware: Malware, an abbreviation for "malicious software," is a broad term encompassing software programs that alter the functioning of a computer. Initially, many early instances of malware were created as experiments, aiming to be bothersome or humorous rather than inflicting significant damage to files or computer systems. However, contemporary malware programs are primarily designed for malicious intent, aiming to damage computers or generate profit for cybercriminals.[41] In legal contexts, malware may

[37] Lawanson .J & Afolabi.M. Chasing the Nigerian Dream: The Proliferation of Cyber Fraud among Nigerian Youths and its Effect on Nigeria's Global Image.International Journal of Intellectual Discourse(2020)3(2)<https:/www.researchgate.net/publication/349173609 >accessed 13 May 2024

[38] Ibid

[39] The term "419* is coined from Section 419 of the Nigerian criminal code (part of Chapter 38: obtaining property by false pretenses: cheating) dealing with fraud

[40] Joshua BH and Marion.NE. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. Bloomsbury Academic,(2016)p 81

[41] Ibid

also be termed as a "computer contaminant." The dissemination of malware typically occurs through email attachments.[42]

Upon opening the attachment, the malware infiltrates the victim's computer. Subsequently, it can initiate various actions. It may be programmed to harm the computer or erase files. Alternatively, it can engage in data theft by functioning as a "keylogger," capturing keystrokes such as passwords or account details, or by copying files. Another prevalent tactic involves hijacking the system, granting the attacker remote control over the victim's computer.[43]

A significant risk associated with malware is that recipients frequently remain unaware of its presence on their computers. Studies[44] suggest that, on average, 54 days elapse from the moment malware is introduced to a computer until its detection. Moreover, approximately 15 percent of malware remains undetected for a duration of 180 days.[45]

Malware commonly encompasses various types of malicious software, such as computer viruses, worms, adware, spyware, keyloggers, logic bombs, rootkits, and Trojan horse programs, all aimed at modifying the operations of computer programs and files. Often, attacks employing malware involve blended tactics, where multiple types of malware are deployed simultaneously.

2.2.5 Cyberstalking: This is the practice of using digital forms of communication to harass a person in an aggressive, often threatening manner[46]Stalking is acknowledged as a criminal offense in various jurisdictions, and its definitions can differ across different locations or countries. The anonymity provided by the internet allows perpetrators to fully conceal their

---

[42] Ibid

[43] S. Furnell, "Hackers, Viruses and Malicious Software," in Handbook of Internet Crime, ed. Yvonne Jewkes and Maid Yar (Cullompton, England: Willan, 2010), 173-193.

[44] Zahra Salehi, et al ,"Using Feature Generation from API Calls for Malware Detec-tion," Computer Fraud and Security(2014)9-18.

[45] ibid

[46] Lexico, “Cyberstalking”, available at https://www.lexico.com/en/definition/cyberstalking >accessed 13 May 2024

identities. Cyberstalking frequently leads to offline instances of violent crime, underscoring the gravity of online harassment. For example, American actress Eva LaRue endured several years of stalking, during which threatening messages, sent by an unknown sender who identified himself as "Freddie Krueger," vowed to rape and kill her and her young daughter.[47]

2.2.6 Spam: Spamming refers to the indiscriminate dissemination of unsolicited or irrelevant information across the internet, often targeting a large number of users. Its purposes include advertising, phishing, spreading malware, and more.[48]

2.2.7 Wiretapping:

Wiretapping entails covertly monitoring and intercepting electronic communications via phone, fax, or internet. This clandestine practice typically involves accessing phone lines and using monitoring equipment to eavesdrop on conversations. It can be accomplished by placing a listening device, commonly known as a bug, on the targeted wire, or by utilizing inherent features within different communication technologies.[49]

2.2.8 Logic Bombs: A logic bomb is a term used to describe an unauthorized program that is introduced into a computer system. When triggered, it disrupts the normal operation of the computer.[50]

2.2.9 Password Sniffing: A password sniffer is a software tool designed to monitor and capture passwords transmitted over a computer or network interface. It actively listens to both incoming and outgoing network traffic, logging any data packets containing passwords.[51]

---

[47] Casarez.J and Griggs B. 'DNA from fast-food straw led FBI to stalker who threatened 'CSI Miami actress for 12 years.CNNWire(2022)<ABC Chicagoabc7chicago.comEva LaRue stalker: James David Rogers sentenced after threatening to rape, kill ...>accessed 13 May 2024

[48] Lexico, "Spam", available at https://www.lexico.com/en/definition/spam >accessed 13 May 2024

[49] Paul Kirvan, 'Wiretapping' What is Wiretapping? | Definition from TechTarget>accessed 13 May 2024

[50] Lexicon, 'Logic bomb' available at https://www.dictionary.com/browse/lexicon >accessed 13 May 2024

[51] Techopedia, 'password sniffer' available at https://www.techopedia.com/definition/8798/password-sniffer >Accessed 13 May 2024

2.2.10. Phishing: Phishing is characterized as a type of social engineering where a perpetrator, often referred to as a 'phisher,' tries to deceitfully obtain confidential or sensitive credentials from legitimate users by imitating electronic communications from a reputable or public organization using automated methods.[52]

It's described as a malicious attack in which cybercriminals craft counterfeit websites resembling popular online platforms such as social networks, online banking services, or gaming sites, employing diverse social engineering tactics to entice users to visit these sites.[53]

2.2.11 Counterfeit Websites: Counterfeit websites also known as Scam websites refer to unauthorized online platforms employed by malicious actors to trick users into fraudulent activities or malicious schemes[54]. Exploiting the anonymity afforded by the internet, scammers conceal their true identities and intentions through various disguises. These can manifest as false security alerts, fake giveaways, and other deceptive formats aimed at appearing legitimate. Such websites may exist independently, as pop-ups, or unauthorized overlays on genuine websites via clickjacking. Regardless of their form, these sites systematically aim to lure and deceive unsuspecting users.[55]

2.3. Historical Examples of Cybercrimes Globally

Determining the precise origin of cybercrime within cyberspace presents challenges; however, it is within our capacity to identify the initial significant attack on a computer network and discern its progression into contemporary forms of cybercrime.[56] The history of cybercrime

---

[52]Shi J., Saleem S., 'Phishing' Computer Security Research Reports, University of Arizona available at <http://www.cs.arizona.edu/collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5. final/report.pdf >accessed 13 May 2024

[53] David wong ' the evolution of phishing attacks (2023) <AT&T Cybersecurityhttps://cybersecurity.att.com › blogsThe evolution of phishing attacks> accessed 13 May 2024

[54] Kapersky 'scam websites ' available at Kasperskywww.kaspersky.comScam Websites: What They Are & How to Avoid Them > accessed 13 May 2024

[55] Ibid

[56] Le VPN, "Where Does Cybercrime Come From? The Origin & Evolution of Cybercrime", 18 October 2018, available at https://www.le-vpn.com/history-cyber-crime-origin-evolution/ >accessed 13 May 2024

traces back to the 1970s, characterized by criminal activities conducted through phone lines known as "phreaking," which involved the manipulation of specific tones to make free calls. John Draper, also known as Captain Crunch, a former United States Air Force engineer working in Silicon Valley in 1971, discovered that the whistle prizes found in "Cap'n Crunch Cereal" boxes emitted tones identical to those used by telephone-switching computers. He proceeded to disseminate instructions on utilizing these tones to place free long-distance calls, resulting in a surge in the number of phreakers. Draper inadvertently attracted attention to himself in a 1971 interview with Esquire magazine, leading to his arrest, conviction, and a five-year probationary sentence. Subsequently, he faced incarceration twice for phone fraud in 1976 and 1978.[57] The individuals involved in these activities were known as phreakers. During that era, phreakers primarily sought to showcase their expertise, earn admiration from fellow hackers, and challenge or provoke law enforcement. Their pursuit of recognition, exemplified by John Draper's subtle admission of his actions in a public interview, often contributed to their eventual apprehension.[58]Despite his illegal activities, Draper served as an inspiration and collaborator for the founders of Apple, Steve Jobs and Steve Wozniak.

In 1981, Ian Murphy, also known as Captain Zap, became the first individual to be prosecuted and convicted as a felon for cybercrime. He breached the AT&T mobile network, manipulating its internal clock to apply off-hours rates during peak hours, resulting in fraudulent charges to customers. Murphy received a sentence of 1,000 hours of community service and two and a half years of probation. His exploits served as inspiration for the 1992 film, "Sneakers." [59]

[57] D. O'Brien, "A Short History of Law Enforcement and Cyber Crime", 03 May 2018, available at https://medium.com/threat-intel/cyber-crime-takedowns-66915be7307 >accessed 13 may 2024
[58] Ibid
[59] Le VPN, as cited in note 30 Supra.

In 1982, a computer virus named "Elk Cloner," which targeted Apple II operating systems, was created as a prank by a 15-year-old. It stands as one of the earliest known viruses to spread extensively through floppy disks.

Shortly thereafter, the United States enacted the 1986 Computer Fraud and Abuse Act, criminalizing unauthorized access to computer systems. In 1988, Robert T. Morris Jr. unleashed a self-replicating worm known as the "Morris Worm" onto the United States Department of Defense's ARPANET, the precursor to the internet. This incident impacted over 6,000 networked computers. Morris was penalized with a $10,000 fine and three years of probation.[60] In 1989, the First National Bank of Chicago experienced a $70 million computer theft, causing worldwide alarm. In response, the United Kingdom implemented the Computer Misuse Act of 1990, which rendered unauthorized access to computer systems a criminal offense.[61]

The inaugural major ransomware incident was documented in 1989 under the name of the AIDS Trojan or PC Cyborg Ransomware. This malicious software was devised by a biologist named Joseph Popp, who distributed infected floppy disks to attendees of the World Health Organization's AIDS Conference under the guise of informational material about AIDS. To regain control of their computers, affected individuals were required to remit $189 to the PC Cyborg Corporation in Panama.[62]

The advent of the World Wide Web in 1994 revolutionized the landscape, providing black hat hackers with a fresh avenue to disseminate their illicit tools, transitioning from traditional bulletin boards to personalized websites. Illustrating the potential of this era, a UK student demonstrated the extent of access by breaching Korea's nuclear program and multiple

---

[60] Ibid

[61] Information Security Buzz, "The Secret History of Cyber Crime", 11 November 2015, available at https://www.informationsecuritybuzz.com/articles/the-secret-history-of-cyber-crime/ >accessed 13 May 2024

[62] KnowBe4, "AIDS Trojan or PC Cyborg Ransomware" available at https://www.knowbe4.com/aids-trojan >accessed 13 May 2024

intelligence agencies, utilizing only a Commodore Amiga computer and a "blue boxing program" sourced from the internet.[63]

The early 2000s saw cybercrime skyrocket with the advent of social media. As people eagerly filled their profiles with personal details, a deluge of sensitive information became available, spurring a rise in identity theft. Criminals exploited this data to drain bank accounts and commit various financial frauds.[64]

In 2000, a teen hacker known as "Mafiabex" unleashed DDoS attacks on major commercial websites like Amazon, Yahoo, CNN, and eBay, causing them to crash and resulting in massive financial losses.[65]

Observations indicate a significant shift in the breed of cybercriminals, transitioning from hackers motivated by defiance against authorities or the desire to impress peers, to those primarily driven by financial gain. Some individuals even engage as spies for foreign governments, selling data for profit. Unlike their predecessors, this new breed of cybercriminals is more cautious about publicizing their activities and maintains a low profile. This contemporary archetype characterizes the current landscape of cybercrime.

Furthermore, cybercrimes have undergone significant evolution over time, encompassing various forms such as denial of service attacks, malware outbreaks, unauthorized access and exploitation of computer systems, theft of intellectual property, cybersquatting, economic espionage, network infiltration, sabotage, and financial theft.[66]As technology advances, so do the opportunities for cybercriminals to exploit vulnerabilities and perpetrate crimes in the digital realm. Additionally, the proliferation of cryptocurrency has facilitated new forms of cybercrime, such as cryptojacking and ransomware payments, providing cybercriminals with

[63] Arctic Wolf ' A brief history of cybercrime', 19 April 2024 available at https://arcticwolf.com/resources/blog/decade-of-cybercrime/ > Accessed 13 May 2024

[64] Ibid

[65] Ibid

[66] Le VPN, "Where Does Cybercrime Come From? The Origin & Evolution of Cybercrime", 18 October 2018, available at https://www.le-vpn.com/history-cyber-crime-origin-evolution/ >accessed 13 May 2024

anonymous and decentralized means to launder illicit proceeds[67].These developments underscore the ever-evolving nature of cyber threats and the pressing need for robust cybersecurity measures to safeguard against them.[68]

2.4 Cybercrime In Nigeria

Cybercrime has emerged as a significant challenge in Nigeria, with the country grappling with various forms of digital malfeasance that pose threats to individuals, businesses, and the nation's cybersecurity infrastructure[69]. From sophisticated hacking attacks to financial scams and identity theft, cybercriminals in Nigeria exploit vulnerabilities in digital systems to perpetrate illicit activities with far-reaching consequences. “Yahoo Yahoo” is a term commonly used in Nigeria to describe various forms of online fraud, including advance fee fraud and phishing scams[70]. In 2023 the Nigerian anti-corruption agency,The Economic and financial Crime Commission disclosed that it had secured 1084 cyber crime convictions by the year 2023.[71] cybercriminals in Nigeria are known for enticing individuals worldwide through deceptive practices such as spam emails, money laundering schemes, and elaborate faux partnership offers.[72] Foreign individuals, especially women searching for online partners, frequently become victims of these schemes. Perpetrators pretend to be interested in forming enduring relationships, but ultimately exploit the trust of their victims. Some even coerce

---

[67] Julija Lapuh,‘cryptocurrency as facilitators of cybercrime’,2021.available at ResearchGatehttps://www.researchgate.net › 352...(PDF) Cryptocurrencies as facilitators of cybercrime>accessed 28 may 2024

[68] Ibid

[69] Babayo Sule et al,’cybersecurity and cybercrime in Nigeria:the implications on National security and digital Economy’,October 2021,Journal of intelligence and cybersecurity.4(1).available at https://www.academicapress.com/journal/V4-1/JICS_Vol4_Is1_Sule%20et%20al_final.pdf> accessed 28 may 2024

[70] Adesina, O. S. Cybercrime and Poverty in Nigeria. Canadian Social Science, (2017)13(4), 19-29. Available at http://dx.doi.org/10.3968/9394> accessed 13 may 2024

[71] Solomon Odeniyi ‘ FG decries rising cybercrimes, EFCC secures 1084 convictions’ 8 November 2023 available at Punch Newspapershttps://punchng.com › fg-decries-ris...FG decries rising cybercrimes, EFCC secures 1084 convictions > accessed 13 May

[72] Moga, Ezekiel,et al ‘A Historical Assessment of Cybercrime in Nigeria:Implication for Schools and National Development’.Journal of Research in Humanities and Social Science(2021)9(9)84-94.

victims into aiding with travel documents or residential permits, only to abruptly cease communication once their goals are fulfilled, before targeting their next victim.[73]

Another widespread cybercrime in Nigeria is phishing, a tactic where deceptive emails are sent to unsuspecting victims, often mimicking legitimate sources like banks. These emails prompt recipients to verify personal information by clicking on a link to a fraudulent webpage. Upon submission, the hacker gains access to the victim's financial information.[74]

In 2015, there was a notable increase in phishing emails originating from suspected cybercriminals in Nigeria, especially coinciding with the Central Bank of Nigeria (CBN) announcing the deadline for the Bank Verification Number (BVN).[75] Cybercriminals inundated unsuspecting bank customers with phishing emails, falsely warning them of imminent account blockages and subsequently stealing their credentials once they fell for the ruse and provided their details.

Cybercrime in Nigeria presents a multifaceted challenge, encompassing various illicit activities,despite efforts to combat these threats, the country continues to grapple with the pervasive impact of cybercriminal activities on individuals, businesses, and its cybersecurity infrastructure.

2.5 Reasons of Cybercrime in Nigeria

The rise of cybercrime in Nigeria is increasingly concerning, driven by a confluence of factors including high unemployment rates, ineffective enforcement mechanisms, and widespread poverty. As technology advances, so do the motives behind cybercriminal activities, often stemming from a pursuit of wealth amidst limited economic prospects.

---

[73] Ibid

[74] Adesina, O. S. Cybercrime and Poverty in Nigeria. Canadian Social Science, (2017)13(4), 19-29. Available at http://dx.doi.org/10.3968/9394> accessed 13 may 2024

[75] IDigest, 'Give force to cybercrime law' 22 Jan 2016 available at ittelecomdigest.comhttps://ittelecomdigest.com › give-...Give Force to Cybercrime Law - IT Telecom Digest > accessed 13 May 2024

Akanle et al[76]. underscore that factors such as unemployment, societal disintegration, and governance failures play pivotal roles in the escalation of cybercrime. The following are some of the reasons behind the surge of cybercrime in the country:

2.5.1 Unemployment; the connection to cybercrime is linked to the high unemployment rates, economic challenges, and educational deficiencies in Nigeria. The Nigerian National Bureau of Statistics reports nearly 20 million unemployed citizens, with approximately 2 million new individuals joining the ranks of the unemployed annually. This high level of unemployment among youth can lead to increased idle time, which may be channeled into cybercriminal activities[77].

2.5.2 Weak Enforcement: The enforcement of cybercrime laws is often weak and law enforcement agencies aren't always fully prepared to handle these crimes due to a lack of resources and training. The private sector also struggles to defend against tech-savvy criminals, including in Nigeria, where there's a shortage of advanced technology to effectively trace cybercriminals. Sometimes, even existing laws are outmaneuvered by these offenders. However, it's important to acknowledge that agencies like Nigeria's EFCC and ICPC have had some success in prosecuting cybercrime,[78]even though there's still plenty of room for improvement.

2.5.3 Poverty: is defined as the lack of sufficient resources to secure basic life necessities such as food, housing, clothing, and leisure activities. It's the state of being without the essentials needed for human well-being and comfort. This dire situation can sometimes drive

[76] Akanle O,et al 'Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria.African Journal of Science, Technology, Innovation and Development, 2016)8(2), 213-220.
[77] National bureau of statistics http://www.nigerianstat.gov.ng/ > accessed 13 May 2024
[78] EFCC reaffirms commitment to fight against cybercrimes 21 Jan 2021 available at Global Integrityhttps://ace.globalintegrity.org › ...PDFReassessing Anti-Corruption Law Enforcement in Nigeria - GI-ACE > accessed 13 May 2024

individuals to commit crimes as a means of survival. As of 2018, around half of the Nigerian population was living in severe poverty.[79]

2.5.4 Quest for Wealth: Another cause of cybercrime in Nigeria is quest for wealth, there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be substantial enough to justify the venture. This urgency for economic gains leads some into the realm of cybercrime as a shortcut to wealth.

2.6 Impacts of Cybercrime in Nigeria

The impact of cybercrime in Nigeria is staggering, with costs encompassing data destruction, lost productivity, theft of funds, intellectual property, and personal information, along with business disruptions, recovery and deletion costs for data and systems, reputational damage, and embezzlement. In Nigeria, these crimes tarnish the nation's global image significantly, Nigerians abroad often face discrimination and derogatory labels due to the actions of some Nigerian cybercriminals. This stigma leads to a loss of honor, respect, and dignity, as Nigerians are frequently perceived and treated as scammers, fraudsters, and con artists, inflicting severe harm to Nigeria's international reputation.

Ramon Olorunwa Abbas, also known as Hushpuppi, Hush, or Ray Hushpuppi, a one-time Instagram influencer from Nigeria and now a convicted criminal, received an 11-year sentence in the United States[80]

His conviction was for conspiring to wash the proceeds of various frauds, including business email compromise schemes, which swindled a U.S. law firm of close to $40 million,

[79] National bureau of statistics 'Nigeria Launches its Most Extensive National Measure of Multidimensional Poverty',17 November 2022 available at 2022 Multidimensional Poverty Index (MPI) - National Bureau of Statistics >accessed 13 May 2024

[80] Ibid
Faith karimi.'He flaunted private jets and luxury cars on Instagram. Feds used his posts to link him to alleged cyber crimes' 12 July 2020 available at https://www.cnn.com/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html .accessed >25 Feb 2024

misappropriated $14.7 million from an overseas bank, and attempted a heist of $124 million from an English soccer team.[81] Financially, cybercrime has severely wounded Nigeria's economy, with the nation reportedly losing around $9.3 billion to such crimes.[82]

This loss is compounded by reduced consumer trust and hindered foreign investments. Frank and Odunayo[83]highlighted the enormous $80 billion annual loss to software piracy, a rapidly expanding scam mainly executed by the youth[84]

The EFCC revealed that 80% of its convictions are cybercrime-related. Abdulrasheed Bawa,the Executive Chairman,[85] pointed out that Nigeria's shift to an "e-society" has inadvertently boosted cybercrime, making electronic transactions such as e-payments and e-banking more susceptible to cyber threats.

2.7 Conclusion

In conclusion, this chapter has shed light on the complex landscape of cybercrime in Nigeria, exploring its various forms, underlying reasons, and significant impacts. By delving into conceptual clarifications, historical examples, and the specific context of Nigeria, we have gained a deeper understanding of the challenges posed by cyber threats in the digital age. It is evident that cybercrime not only inflicts financial and societal harm but also undermines trust, security, and progress. Moving forward, addressing these challenges will require a multi-faceted approach, including robust legislation, enhanced cybersecurity measures, and greater collaboration between stakeholders.

---

[81] Kayode Oyero ‘ Money laundering: US court to sentence Hushpuppi on Valentine’s Day ‘26 January 2022 Available at https://punchng.com/money-laundering-us-court-to-sentence-hushpuppi-on-valentines-day/ .Accessed>25 February 2024

[82] Adeyemi Adepetun. ‘ Nigeria responsible for $9.3b in global loss to cybercrime’ 28 October 2016 available at https://m.guardian.ng/news/nigerians-responsible-for-9-3b-in-global-loss-to-cybercrime/ accessed>25 February 2024

[83] Frank, I. & Odunayo, A.’Approaches to cyber security issues in Nigeria: Challenges and solutions’ International Journal of Cognitive Research in Science, Engineering and Bducation,(2013)1(1), 100-110.

[84] Wahab Adesina ‘ 80% of our convictions cybercrime-related — EFCC ‘ 7 October 2021 available at https://www.vanguardngr.com/2021/10/80-of-our-convictions-cybercrime-related-efcc-2/am > accessed 25 February 2024

[85] Ibid

Introduction

An illegal act must be explicitly defined and banned by law. Following the moral principle of nullum crimen sine lege (Latin for "no crime without law"), an individual cannot be punished for an action that was not prohibited by law at the time the action was committed. In the realm of cybercrime regulations, the cybercrime laws set the standards for acceptable behavior in the use of information and communication technology (ICT). These laws not only establish penalties for cybercrimes but also aim to protect ICT users, prevent harm to individuals, data, systems, and infrastructure, and uphold human rights. They enable the investigation and prosecution of online crimes and promote international cooperation on cybercrime issues. By defining rules of conduct for online activities, cybercrime laws help reduce risks and mitigate harm caused by cybercrimes. It is crucial for illegal acts to be clearly defined and prohibited by law to ensure accountability. Many countries have developed specific laws to address the evolving landscape of cybercrimes, which encompass traditional crimes adapted to cyberspace as well as new offenses made possible by digital technologies and the Internet.

Cyber Laws in Nigeria

In Nigeria, the primary law for combating cybercrime is the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. Before this law, there was no specific legal framework for cybersecurity in the Nigerian digital economy, leading to a gap in law enforcement. The Cybercrime Act of 2015 has equipped Nigeria better to fight cybercrime activities.However, discussing the Cybercrime Act 2015 wouldn't be complete without shedding light on the key laws that were in place to tackle cybercrimes before its enactment. These laws include the Economic and Financial Crimes Commission (Establishment) Act, 2004; the Advanced Fee Fraud and other Related Offences Act, 2006; the Money Laundering (Prohibition) Act, 2011,

as amended in 2013; the Nigerian Evidence Act; the Criminal Code Act; and the Terrorism (Prevention) Act, 2013.

It is imperative to note that the Cybercrime Act 2015 has been updated with significant amendments under the Cybercrime (Prohibition, Prevention, etc.) Amendment Act, 2024, which refined and expanded certain sections to address emerging threats and enhance regulatory mechanisms.

THE ECONOMIC AND FINANCIAL CRIME COMMISSION ACT

Before the Cybercrimes Act of 2015 came into effect, the Economic and Financial Crimes Commission (EFCC) Act, also known as the EFCC Act, served as the primary law for combating and prosecuting cybercriminals due to its extensive provisions concerning cyber/internet crimes.

The Economic and Financial Crime Commission Act hereinafter referred to as EFCC Act was first enacted in 2003 and amended in 2004. The act establishes the legal framework for the Commission's formation, the Act specifies the Commission's major responsibilities, which encompass investigating a wide range of financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, and contract scams[86]. The Economic and Financial Crime law in Nigeria specifically addresses issues related to internet service providers and cyber cafes, but it does not encompass the comprehensive scope of computer misuse and cybercrime.

The EFCC Act seemed to have made very elaborate provisions towards cyber security by creating a wide scope of cyber and internet crimes to which the Act applied. This provision

[86] Section 6 (a) B) EFCC Act.

and powers to prosecute those crimes and many more had helped the commission in making some laudable achievements in the fight against various types of cybercrime.

This provision formed the foundation for several cases involving the commission, including the well-known case of Federal Republic of Nigeria v. Chief Emmanuel Nwude & ors.[87].

In another case discussed below within the EFCC as an agency for cyber security, in the matter of FRN V. Emmanuel Nwude, the accused individuals faced a 57-count charge, including defrauding for an amount of US $181.6 million. They were convicted on all counts and received appropriate sentences; their assets were forfeited to the federal Government, and the scam proceeds were recovered and returned to the rightful owners. The Act also clearly outlines the offenses that fall under its jurisdiction.[88] It's evident that the EFCC Act, while not specifically designed for cyber security, contains extensive provisions for that purpose. However, the Act does have its shortcomings. It states that the Commission established under the Act will have authority over the coordination and enforcement of all economic and financial crimes laws,[89] potentially leading to power struggles with other law enforcement agencies like the Nigerian Communication Commission responsible for enforcing the Cybercrime Act, 2015. Additionally, the Act lacks detail in outlining the specific acts and activities that constitute cybercrimes.

ADVANCED FEE FRAUD AND OTHER RELATED OFFENCES ACT 2006

[87] Suit No CA/245/2005
[88] Section 14, 15, 16, 17 & 18 of the EFCC Act
[89] Section 6 (c) EFCC Act

The law aims to tackle Advance Fee Fraud and other related offenses. It states that anyone who deceives someone else with the intent to defraud, leading to the transfer of property or obtaining property through false means, is breaking the law under this Act.

According to the law, it doesn't matter where the victim is located; as long as someone deceives another person through false pretenses to gain a benefit, they are held accountable under this act.[90] If found guilty, the offender could face imprisonment ranging from seven to twenty years without the option of a fine[91]. Additionally, engaging in illegal financial transactions is also considered an offense under this act. If a financial institution or corporation is involved, they may face a fine of One Million Naira, If unable to pay the fine, their assets equivalent to the fine could be seized by the Federal Government. Directors, secretaries, or officers of these entities could face imprisonment from five to ten years[92]

The law outlined in section 12 [93]is designed to oversee companies offering services via e-mail or online platforms.. These companies must collect specific information from customers or subscribers like full names and addresses. Failure to provide this information or giving false details could lead to imprisonment for at least three years or a fine of N100,000. Companies that don't comply with these regulations may face a fine of N100,000 and could even have their equipment or facilities used for providing the service confiscated. This provision will be useful in prosecuting many cybercrimes, particularly those involving identity theft, phishing, spoofing, and other offenses where the culprits often remain anonymous and operate under false identities.

The writers believe that some areas need reviewing. The Act gives the power and responsibility of surveillance to operators like Corporations and internet service providers. While this approach may seem positive, considering that these operators interact with

[90] Section 1(2)Ibid
[91] Section 1(3)Ibid
[92] Section 7(1)(a)(b)Ibid
[93] Ibid

customers and potential criminals regularly, the possibility that some employees of these operators may have criminal tendencies and could aid criminals cannot be dismissed. For example, despite the security measures like Know Your Customer (KYC) schemes implemented by banks and financial institutions, frauds such as phishing continue to increase. It seems that bank databases are frequently breached because an insider is providing criminals with customer account information. The surveillance power should ideally be shared between the operators and the relevant law enforcement agencies.

Criminal Code Act

The Criminal Code Act of prohibits the act of stealing funds in any form. If caught, individuals can face legal consequences under this Act. Although cybercrime is not explicitly addressed, it is considered a form of theft under the law. Chapter 38[94] of the Act focuses on the acquisition of property through deceit, with Section 419[95] specifically addressing cybercrime and Section 418[96] defining offenses. In essence, Section 418 states that any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence. Also, section 419 states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

The provisions outlined are highly beneficial for prosecuting cyber criminals who engage in deceitful practices, like impersonating company Directors or falsifying corporate accounts to defraud individuals who trust them based on these misrepresentations. Regrettably, the Criminal Code, originating from the British colonial era, predates the internet era and lacks

[94] CAP C38, LFN 2004.
[95]Ibid
[96] Ibid

specific regulations addressing online scams within the section on false pretences. The outdated nature of the Criminal Code is evident in section 419, stipulating that a criminal cannot be arrested without a warrant unless caught in the act. Cyber criminals demonstrate adeptness in covering their tracks and erasing evidence of their illicit activities and transactions before law enforcement secures a warrant for their arrest.Again It's rare for cyber criminals to be caught in the act; online crimes are typically discovered after they've happened. The punishment in the Criminal Code, like three years' imprisonment or seven years if the stolen property is worth over one thousand naira, shows that the law wasn't meant for modern crimes like cybercrime. The one thousand naira limit is tiny compared to the millions stolen by these criminals daily. Also, the State is the one who complains in our justice system, so victims often get nothing in the end. This can make cybercrime victims hesitant to report the crimes they've faced.

Money Laundering (Prohibition) Act 2011

The Money Laundering (Prohibition) Act[97], also known as the ML Act, is a law that stops the cleaning of rlmoney from crimes or illegal activities. According to the ML Act, no person or company can make or get cash payments over #5 million for individuals or #10 million for companies, except through a financial institution.[98]

Under this law,, all banks and financial institutions in Nigeria must report any transaction over US $10,000 or its equivalent to the Central Bank of Nigeria, the Securities and Exchange Commission, or the EFCC in writing within 7days from the date of the transaction.[99]

[97] CAP, M18, LFN 2018.
[98] Section 1 money laundering act
[99] Section 2(1)ibid

This rule aims to prevent cyber criminals from using banks and financial institutions to aid online crimes. If individuals or companies transport cash over US $10,000 in or out of Nigeria, they must declare it to the Nigerian Customs Service.[100]

Based on what was mentioned earlier, it's evident that the Act thoroughly addresses cybersecurity and safeguards against cybercrimes, particularly within financial institutions. However, the Act doesn't establish its own enforcement agency; instead, the Economic and Financial Crimes Commission is responsible for enforcing its provisions.[101]

This writer believe this could slow down the enforcement of the ML Act. They suggest amending the EFCC Act to separate it from enforcing the ML Act and amending the ML Act to establish its own enforcement agency.

The Nigerian Evidence Act, 2011

The 2011 Evidence Act replaced the old 2004 one and allows computer and internet-generated evidence to be considered. Previously, before this new Act, electronically generated evidence couldn't be used in our courts, causing a barrier to admitting internet-generated evidence.

This situation was definitely a hindrance to the country's justice system until 2011 when it was rectified. Before 2011, the courts acknowledged computer-generated evidence, as seen in the case of Esso West Africa Inc. v. T. Oyebola[102].

The courts were hesitant, but in this instance, the Supreme Court emphasized that the law should be well-informed about contemporary business practices and should not overlook the complexities of computers.

[100] Section 2(3)ibid
[101] Section 7 EFCC Act
[102] (1969) 1 NMLR, pt. 194 at 198.

The previous issue has been fixed in the new Evidence Act. The new Act states that "in any proceedings, a statement contained in a document produced by computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible."[103]

Hence, the Evidence Act has taken a step towards allowing computer-generated evidence, meaning online information could be used to prosecute cybercriminals. Additionally, the Act defines a document broadly to include various devices like discs, tapes, and computers, [104]making it inclusive of information from computer networks and online activities.

While it's great for prosecuting crimes like cybercrimes, the Act sets out specific conditions for accepting such evidence. The Act states that computer-generated evidence can be admitted if the document was created by the computer during a period when it was regularly used to store or process information for any ongoing activity, whether for profit or not, by any entity or individual. Additionally, it must show that the computer received relevant information regularly during that time, operated correctly, and the information in the document aligns with the data the computer usually processes.[105]

In the Kabor v. Dickson case[106], the Supreme Court mentioned that simply submitting computer-generated documents isn't enough; evidence about the computer's usage must be presented to meet the requirements of section 84(2). This might be challenging for law enforcement due to limited funding and lack of expertise in navigating the process of presenting evidence through an expert. In such situations, the case could be lost due to a lack of proof.

'The Terrorism (Prevention) (Amendment) Act. 2013

[103] Section 84 (1) Evidence Act
[104] Sectiom 258 ibid
[105] Sectiom 84(2)(a-d).
[106] (2014) SC 193

This Act repealed the Terrorism (Prevention Act) of 2011 and introduced provisions for the extraterritorial application of the Act, in addition to bolstering the regulation of offenses related to terrorist financing.

Section 1 (b) of the Act provides that:

> any person or body corporate who knowingly in or outside Nigeria, directly or indirectly deals or attempts or threatens any act of terrorism,[107]commits an act preparatory to or in furtherance of an act of terrorism, omits to do anvthing that is reasonably necessary to prevent an act of terrorism,[108]assists or facilitates the acuvites of persons engaged in an act of terrorism or is an accessory to an oftence under this Act [109]paracipates as an accomplice in or contributes to the omission of any act of terrorism or offence under this Act[110]assists, facilitates, organizes or directs the activities of persons or organizations engaged in an act of terrorism[111],is an accessory to any act of terrorism or incites, promotes, or induces any other person by any means whatsoever to commit any act of terronism[112]or any other offence referred to in this Act commits an offence and is liable on conviction to maximum of death sentence[113]

The Act, while not specifically designed for cybersecurity, is a useful tool for prosecuting aspects of cybercrime related to cyber terrorism. It encompasses provisions that cover a wide range of activities, including acts of terrorism carried out online or through computer networks. The Act assigns the responsibility for prosecuting offenses to various agencies, such as the Nigerian Police Force, the Economic and Financial Crimes Commission, and the Department of State Security Services. This move is seen as a positive step, considering the government's zero-tolerance policy towards terrorism.

However, the involvement of multiple agencies in prosecuting these offenses could lead to power struggles and overlapping responsibilities, potentially hindering the Act's intended

[107] Section 1 of the Terrorism (Preventio)Act 2013
[108] Section 1(c)
[109] Sectiom 1(d)
[110] Sectiom 1(e)
[111] Section 1(f)
[112] Section 1(g)
[113] Section 1(h)

goals. A more efficient approach would involve a single, well-equipped agency handling the task.

The Cybercrimes (Prohibition, Prevention Etc Act, 2015

The Cybercrimes Act of 2015 is Nigeria's first law specifically addressing cyber security. It was passed in May 2015 to implement the 2011 ECOWAS Directive on combating cybercrime and has a broad scope.The acclaimed objectives of this Act include the provision of an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria[114].The Act was created as a response to the increasing fraudulent activities in cyberspace, where there was no specific regulatory regime before. It aims to protect vital information for national security by designating certain computer systems as Critical National Information Infrastructure. Additionally, it focuses on safeguarding intellectual property and privacy rights. The Act serves to deter various cyber activities such as cyberstalking, cybersquatting, fraud, forgery, and cyber terrorism through legislative proscriptions. Violations of these regulations can lead to a range of penalties, including fines and imprisonment.

The Act assigns the National Security Advisor (NSA)[115] and the Attorney-General of the Federation (AGF) to coordinate enforcement[116]. It also establishes the multi-agency Cybercrime Advisory Council and the National Cyber Security Fund overseen by the NSA. Section 38 mandates that service providers retain all traffic data and subscriptions for at least two years. Failure to comply with this requirement or share the information with law enforcement agencies can lead to a fine of 7 million naira.

[114] Section 1 of the Cybercrime Act,2015
[115] Section 41 Ibid
[116] Section 41(2)Ibid

Section 39[117] of the Cybercrimes Act mandates that service providers must aid authorities in collecting or recording data upon a court order. Additionally, under section 40[118], they are obligated to help law enforcement in identifying offenders, tracing crime proceeds, and terminating services used for offenses. Notably, the Act imposes harsh consequences, like life imprisonment, for crimes targeting critical national infrastructure that lead to fatalities, as well as different punishments for less serious offenses.[119]

Accordingly,, hackers who illegally access computer systems or networks may face a fine of up to N10 million or up to 5 years in prison, depending on the intent of the hack. The same penalties apply to internet fraudsters who engage in fraudulent activities through electronic messages or unauthorized use of computer data.[120]

The Act indeed addresses identity theft, stipulating a penalty upon conviction of 7years imprisonment or a fine of 5 million, or both fine and imprisonment.[121]

It also outlaws cyber-stalking and cyber-bullying as well, with penalties that vary depending on the severity of the offense. Offenders can face fines starting from N2 million or imprisonment for at least 1 year, up to a maximum of 10 years or a fine of N25 million, or both fine and imprisonment[122]

The Act ensures that service providers must handle traffic data and subscriber information while respecting individuals' right to privacy. Additionally, the Act permits the interception of electronic communication through a court order if there are reasonable grounds to suspect that the content is needed for a criminal investigation.[123]

---

[117] Ibid
[118] Ibid
[119] Section 5(3) Ibid
[120] Section 14(2)Ibid
[121] Sectiom 22(1)Ibid
[122] Section 24(1)1(2) Ibid
[123] Sectiom 39 Ibid

Section 50 of the Act gives the Federal High Court jurisdiction over offenses under the Act. The case can be initiated in any Federal High Court in Nigeria, irrespective of where the offense occurred. This rule conflicts with the ruling in the Ibori v. Federal Republic of Nigeria case by the Court of Appeal.[124]

In the case, it was determined that a defendant should be tried where the incident leading to the trial occurred. Section 52 of the Act specifies that offenses covered by the Act are extraditable under the Extradition Act.[125]

Section 53 stipulates that evidence from a foreign country can be utilized in Nigerian court proceedings if authenticated by a judge, magistrate, justice of peace, or a seal from a foreign government Ministry or Department. Furthermore, Section 56 mandates the National Security Adviser to maintain a 24-hour contact point for countries with agreements or treaties with Nigeria.

The Act presents various challenges that warrant attention. Firstly, the Act lacks a clear enforcement mechanism, leading to ambiguity in reporting violations. Decentralizing enforcement responsibilities could enhance clarity in this regard. Secondly, conflicts with existing laws, such as differing burden of proof standards, may create legal uncertainties. The Act's overlap with regulations on banks and service providers could further complicate legal interpretations. Lastly, the Act's provisions for safeguarding National Information Infrastructure are pivotal, but the absence of published designations in the Federal Gazette poses a challenge to its foundational principles.

The Cybercrime (Prohibition, Prevention, etc.) Amendment Act, 2024

To keep pace with the evolving landscape of cyber threats, the Cybercrime (Prohibition, Prevention, etc.) Act, 2015, was amended in 2024.President Bola Tinubu signed the

[124] [2009] 3 NWLR (Pt. 1127) 94
[125] See Cap E25 Laws of the Federation of Nigeria, 2004.

Cybercrime Act 2024 into law on February 28, 2024[126]. The Cybercrimes (Amendment) Act comprises thirteen (13) sections, modifying 11 sections of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.[127] As stated in the Explanatory Memorandum of the Cybercrimes (Amendment) Act, its objective is to include certain consequential terms that were unintentionally left out in the Cybercrimes Act. Yet, upon closer examination of the Cybercrimes (Amendment) Act, it becomes apparent that it goes beyond simply inserting omitted words; it introduces new provisions that hold substantial importance for Nigeria's cybersecurity landscape.[128]

Key amendments include clarifications regarding contractual transactions with electronic signatures[129], the establishment of Sectoral National Computer Emergency Response Teams (CERTs) and Security Operations Centers (SOC)[130], and the revision of vague language regarding offensive message[131]. The language in Section 24(1) of the Cybercrimes Act was notably vague and ambiguous. Civil society organizations believe that this vagueness allowed state authorities to misuse the provision to prosecute journalists, bloggers, and media practitioners. Fortunately, Section 5 of the Cybercrimes (Amendment) Act has removed this unclear language and replaced it with more precise and definitive terms.

Furthermore, financial institutions are now mandated to verify customer identities using National Identification Numbers[132], while service providers must safeguard data according to the Nigeria Data Protection Act[133]. Additionally, a levy on electronic transactions[134] by

---

[126] Onuzure Dania,'Cybercrime implementation mustn't subvert Constitutional right lawyers', 2024.available at https://punchng.com/cybercrime-act-implementation-mustnt-subvert-constitutional-rights-lawyers/?amp> accessed 29 May 2024

[127] Imoleayo Oyedeyi, 'Amended Cybercrime Act dangerous, may influence police clapdown on journalists, orhers-lawyer' 2024. Available at https://punchng.com/amended-cybercrime-act-dangerous-may-influence-police-clampdown-on-journalists-others-lawyer/?amp > accessed 29 May 2024

[128] Ibid

[129] Section 2 (b) of the Cybercrimes(prohibition, prevention etc) (Amendment) Act 2024

[130] Ibid Section 3

[131] Ibid Section 5

[132] Section 8 of the Cybercrimes(prohibition, prevention etc) (Amendment)Act 2024

[133] Ibid Section 9

[134] Ibid Section 11(a)

specified businesses aims to fund cybersecurity efforts, with penalties for non-compliance.[135] Notably, the Act eliminates the provision for canceling international passports as a penalty for cybercrime convictions[136]. These amendments collectively aim to enhance cybersecurity measures, clarify legal provisions, and impose stricter penalties for cyber offenses, reflecting Nigeria's commitment to a safer digital environment.

However, the amendment process has attracted some criticism. There are concerns that the amendments were made hurriedly and without sufficient transparency[137] . Questions have been raised about when the bill was sponsored and whether there was adequate public debate and scrutiny of its provisions. [138]Some believe that the National Assembly, under Senator Godswill Akpabio, rushed the bill into law primarily to generate more revenue for the government, despite the severe economic difficulties faced by many Nigerians[139].

Critics argue that imposing additional levies in this economic climate is insensitive and burdensome for citizens who already endure significant financial strain[140]. There is also concern about the allocation of these funds. Initially, the plan was to direct the generated levy to a fund under the Office of the National Security Adviser. However, this office, as currently constituted, is not established by any specific Nigerian law, raising questions about the legitimacy and transparency of such an allocation[141]. Responding to the criticism, President Tinubu suspended the implementation of the 0.5% cybersecurity levy[142], highlighting the

---

[135] Ibid Section 11(b)
[136] Ibid Section 12
[137] Imoleayo Oyedeyi, 'Amended Cybercrime Act dangerous, may influence police clapdown on journalists, orhers-lawyer' 2024. Available at https://punchng.com/amended-cybercrime-act-dangerous-may-influence-police-clampdown-on-journalists-others-lawyer/?amp > accessed 29 May 2024
[138] Ibid
[139] Ibid
[140] [140] Imoleayo Oyedeyi, 'Amended Cybercrime Act dangerous, may influence police clapdown on journalists, orhers-lawyer' 2024. Available at https://punchng.com/amended-cybercrime-act-dangerous-may-influence-police-clampdown-on-journalists-others-lawyer/?amp > accessed 29 May 2024
[141] Ibid
[142] Olalekan Fakoyejo, 'it's official:Tinubu suspends 0.5% cybersecurity levy'.2024. Available at https://www.thecable.ng/its-official-tinubu-suspends-0-5-cybersecurity-levy/> accessed 29 May 2024

impact of public opinion and the ongoing debate about the best approach to funding cybersecurity initiatives.

The Constitution

The 1999 Constitution (as amended) serves as the primary guide for governing the internet in Nigerian legal practice. Section 37 specifically safeguards the right to privacy, encompassing personal spaces, communication, and telegraphic exchanges.

Legal issues and challenging combating cybercrime

cybercrime persist in Nigeria, despite the existing legislative framework such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015. However, recent amendments and the enactment of the Cybercrime Act of 2024 aim to address these shortcomings and enhance cybersecurity measures in the country. One of the primary issues remains the difficulty faced by authorities in apprehending and prosecuting cybercriminals, despite the significant annual financial losses exceeding $500 million[143] incurred by businesses and individuals due to cybercrime. In the Explanatory Report of the Council of Europe's Convention on Cybercrime, the following statement was made:[144]

“One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subjeet of a criminal

investigation, there by destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation” [145]

---

[143] Omogbolagun T. “https://punchng.com/senate-laments-nigerias-loss-of-500m-annually-to-cybercrime/?amp accessed >17th April 2024

[144] European Treaty Series No.185 Held in Budapest September ,2001

[145] 'Paragraph 133 of the Explanatory Report to the Council of Europe's Convention on Cybercrime

In 2023 The Federal government decries rising of cybercrime , the Chairman of the Economic and Financial Crime Commission disclosed that the anti-graft agency had secured 1084 cyber crime convictions so far in 2023.while this statistics is a clear indication that a lot has to be done in combatting cybercrime in the nation and there is an urgent need for intensified efforts in this regard.[146] The Cybercrime Act of 2024 introduces updated provisions and measures to strengthen cybersecurity, enhance law enforcement capabilities, and streamline procedures for prosecuting cybercriminals.[147] Despite these legislative efforts, ongoing collaboration between government agencies, law enforcement authorities, and cybersecurity experts is essential to develop comprehensive strategies for combating cybercrime effectively.

The mask of anonymity of the cybercriminals

One of the big challenges in prosecuting cybercrime is identifying the actual criminals because online users' identities are often unknown. The internet is open to users worldwide, making it difficult to establish clear rules for identifying internet users and their intentions. So each person on the internet has a unique online identity that might not reflect their real self. This means that people can create fake identities online, making it hard to figure out who they really are. This freedom on the internet has made it easier for cybercriminals to hide their true identities by using various devices, making it tough to track them down. During an inquiry, a device's IP address can be traced back to a specific location; however, the challenge arises when the true identity of cyber offenders does not necessarily have to be disclosed to the Internet service provider.A significant development in combating cybercrime in Nigeria is the mandatory use of the National Identification Number (NIN) for various

[146] Odeniyi S. 'FG decries rising cybercrimes,EFCC secures 1084 Convictions'2023.available at https://punchng.com/fg-decries-rising-cybercrimes-efcc-secures-1084-convictions/?amp accessed >17 th April 2024

[147] Section 3 of the Cybercrime(prohibition, prevention etc.)(Amendment)Act 2024

online activities[148]. The NIN is a unique identifier assigned to Nigerian citizens and legal residents, which is now required for activities such as obtaining SIM cards, accessing financial services, and registering for certain online services. This requirement helps in reducing anonymity by linking online activities to verified identities. This measure, combined with other provisions of the Cybercrime Act of 2024, strengthens the overall framework for combating cybercrime in Nigeria.

Despite these advancements, the inherent anonymity provided by the internet continues to pose a significant obstacle. Therefore, ongoing efforts to develop advanced technological tools and international cooperation remain essential to overcome these challenges.As the obstacle of maintaining anonymity among cybercriminals complicates the prosecution process significantly in Nigeria.[149]

Inadequate enforcement of laws and regulations

Another significant issue hindering the prosecution of cybercrimes in Nigeria is the inadequate l enforcement of existing laws by relevant government agencies. In Nigeria, the Cybercrimes Act 2015 serves as the comprehensive law designed to investigate and prosecute cybercrime perpetrators. However, there appears to be a very minimal enforcement of this legislation, which has impeded its effectiveness in combating cybercrimes. This issue is particularly evident in Section 47 of the Act.[150] The Attorney-General (AG) of the federation has the power to guarantee the successful prosecution of cybercrime offenses. However, there is still a lack of prosecutorial guidance to clarify the ambiguity linked to Section 47 of the Act.[151] So, in Section 47 of the Act, it clearly states that law enforcement officers are part of the cybercrime institutions authorized to prosecute cybercrimes in Nigeria. However, there still seems to be a slow response to the cybercrime issue. The Police and the Economic

[148] Section 8 of the Cybercrimes(prohibition, prevention etc) (Amendment)Act 2024
[149] Mohammed Chakwi (2006). JInonymiry in Cyoerspace: Finding the Balance denseen Privey ana Securty:. Uton lic.com
[150] ibid
[151] Ibid

Financial Crime Commission are currently the ones taking on these prosecutorial powers, even though they are not expressly mandated by the act. The Attorney General of the Federation, as the Chief Law Officer, should ideally have this responsibility. This gap is considered a significant reason for the slow implementation and enforcement of the Act's provisions.[152] Additionally, victims of cybercrimes find it difficult to know where to report their complaints due to the lack of specified agencies in the act, leading many offenses to go unreported and perpetrators to operate freely.

The Cybercrime Act of 2024 addresses these enforcement challenges by introducing clearer mandates and enhanced coordination among various government agencies. Notably, Section 41 of the Act has been amended to ensure the establishment of sectorial Computer Emergency Response Teams (CERT) and Security Operation Centres (SOC) that feed into the national CERT. It also mandates that all public and private organizations integrate their internet and data traffic to these sectorial SOCs to protect the national cyberspace.

Furthermore, the amended Act calls for the establishment of a National Computer Forensic Laboratory to be used by all law enforcement, security, and intelligence agencies[153]Despite these improvements, continuous capacity building, inter-agency cooperation, and public awareness remain essential to ensure robust enforcement of the laws and bring offenders to justice.

Lack of Computer Forensic Standards in Investigations:

The absence of computer forensic standards in retrieving and authenticating electronic data in criminal investigations and prosecutions has impacted the battle against cybercrime significantly. Computer forensics plays a crucial role in criminal investigations and prosecutions, especially in dealing with complex crimes like cybercrime, where forensic

[152] Section 58 ibid
[153] Section 10 of the Cybercrimes(prohibition, prevention etc) (Amendment)Act 2024

techniques are essential for successful prosecution in the court of law.[154] This is necessary because of the progress in technology and the sophisticated tools used by cybercriminals to deceive their victims. An excellent example is the challenge an investigator would encounter in collecting evidence related to hacking and identity theft without the assistance of computer forensics supported by updated tools.[155] Without this, the investigation would be hindered, leading to challenges in prosecuting the offense. The Cybercrime Amendment Act of 2024 addresses this gap by mandating the establishment of a National Computer Forensic Laboratory, as specified in the amended Section 41 of the Act. This facility is designed to support all law enforcement, security, and intelligence agencies in their investigative efforts. The Act also emphasizes the need for building capacity for the effective discharge of functions of all relevant bodies under the Act or any other law on cybercrime in Nigeria[156] Despite these advancements, ongoing efforts to update forensic tools and techniques, along with continuous training for forensic investigators, remain essential. International cooperation and adherence to global best practices in computer forensics will also help Nigeria stay ahead of evolving cyber threats.

Weaknesses in financial institutions:

Financial institutions in Nigeria are significantly impacted by cybercrimes due to certain weaknesses in the Cybercrime Act. One major issue is that the Act requires financial institutions to verify the identities of customers conducting electronic transactions on their platforms, shifting this monitoring responsibility away from law enforcement agencies. While financial institutions gather customer information, the Act needs to be enhanced to empower these institutions to effectively track and monitor cybercrimes in the digital age where many

[154] Danium. M.IL Sarki.et Al, "Forensic seience electronic evidenceand cybercrime crosecution in Nigera" InCyber Crinolous and Technoloos Assisted Crime Control: A Reader feds Ndubueze. P.N Zaria: Abroado Bello University Press (2018)op. 369-382

[155]See Section 6.8 and 20 Cybererime (Prevention & Probibition) Act 2015

[156]Ibid

transactions occur outside traditional banking settings[157].Recent amendments to the Cybercrime Act, particularly Section 44, have introduced a levy of 0.5% of all electronic transaction values by specified businesses. The funds from this levy are intended to support cybersecurity efforts, and the Office of the National Security Adviser is tasked with administering the levy fund, ensuring proper records, and monitoring compliance. Businesses that fail to remit this levy face fines and potential operational license withdrawal[158]

However, enforcement and compliance remain challenges, as the Act still needs further enhancements to fully empower financial institutions. Effective tracking and monitoring of cybercrimes require more robust frameworks, especially given the increasing complexity and volume of online transactions. The collaboration between financial institutions and law enforcement agencies must be strengthened to ensure that cybercrimes are effectively tracked and addressed.

The issue of Jurisdiction

Jurisdiction is crucial as it serves as the foundation for any legal decision and delves deep into the core of any case presented in court. If a court lacks jurisdiction, it also lacks the essential authority to hear the case. The Court of Appeal described jurisdiction as the lifeline of a court because no court can handle a case if it lacks jurisdiction.[159]A critical question arises regarding whether cybercrime offenses lack a specific crime scene, known as "locus delicti," or if they can be considered to have multiple crime scenes due to their multi-jurisdictional nature. Extradition is often viewed as a solution to address jurisdictional challenges, but it requires an extradition treaty between states to allow for the return of cybercriminals for trial. Moreover, both the requested state and the state of domicile of the criminal must ensure that the alleged offense is punishable under their respective laws before

[157] "Ogbonnaya M.'Nigeria's Financial Institutions Vulnerability to cybercrimes '(7 October 2020)available at https:/cnactairca.orm/enust-observermircmas-Ananciletsututions-vulnerablty-to.gyberconck>accessed 24 April 2024

[158] Section 11 of the Cybercrimes(prohibition, prevention etc) (Amendment)Act 2024

[159] Dairo v Union bank of Nigeria plc(2007)16 NWLR (pt.1059)99

extradition can proceed. In Nigeria, the Federal High Court can hear cases under the Cybercrime Act[160], and these offenses can be subject to extradition under the Extradition Act.[161] While no international law compels nations to extradite cybercriminals automatically, collaboration between states can improve the prosecution of cybercriminals. The FBI and EFCC collaboration in "Operation Rewired" in 2019 was highly successful in capturing cybercriminals and retrieving $251,000 from 281 arrests made in the US and other countries, with 167 arrests in Nigeria.[162]

Another successful partnership is a joint effort involving INTERPOL, Group-IB, and the Nigeria Police Force cybercrime Investigation. Together, they have apprehended three suspects in Lagos who are suspected of infiltrating government and private sector entities in over 150 countries since 2017.[163]The cybercrime Amendment Act of 2024 also emphasizes international cooperation, which can help address jurisdictional issues. The Act mandates the coordination of Nigeria's involvement in international cybersecurity cooperation to ensure the integration of Nigeria into global frameworks on cybersecurity[164]. This provision aims to facilitate better international collaboration and support the prosecution of cybercriminals across borders. Despite these successes, jurisdictional challenges remain a significant obstacle. The multi-jurisdictional nature of cybercrime necessitates stronger international legal frameworks and treaties to facilitate the prosecution and extradition of cybercriminals. Enhanced cooperation between countries and continuous efforts to align legal standards and practices are crucial in effectively combating cybercrime.

---

[160] Section 50 of the Cybercrimes (prohibition, prevention, etc) Act 2015

[161] Extradition Act, CAP E25, Volume 6, Laws of the Federation of Nigeria, 2004

[162]Akinkumi Obakeye,'Cybercrime:167 Nigerians arrested in EFCC,FBI joint operation',2019.available at https://www.channelstv.com/2019/09/10/cybercrime-167-nigerians-arrested-in-efcc-fbi-joint-operation/amp/> accessed 24 April 2024

[163] Interpol,' three arrested as Interpol ,Group -IB and the Nigeria police force disrupt prolific cybercrime group'2020.available at https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested_INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group> accessed 20 April 2024

[164] Section 10 of the Cybercrimes(prohibition, prevention etc)(Amendment)Act 2024

Measures for enhancing cybercrimes regulations

Nigeria has seen a rise in cyber-crime activities, making cybersecurity a critical issue. The government has introduced laws to tackle this problem. More action is needed to combat cyber-crime and boost cybersecurity.

In 2014, the Nigerian government created the National Cybersecurity Policy and Strategy (NCPS) to address cybersecurity[165]. The framework involves various stakeholders and provides a comprehensive approach to handling cybersecurity threats.In addition to the NCPS, the government set up the National Information Technology Development Agency (NITDA) to enforce cybersecurity policies and regulation.[166] NITDA is responsible for upholding cybersecurity standards, creating guidelines, and raising awareness about cybersecurity across the nation.

Furthermore, the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024 reflects the ongoing efforts of the Nigerian government to strengthen cybercrime regulations, emphasizing the evolving nature of cybersecurity challenges and the need for proactive measures.

The Nigerian government has made efforts to strengthen cybercrime regulations, but there is still much room for improvement in effectively combating cybercrimes in the country. Here are some of the best ways the government can enhance cybercrime regulations in Nigeria.

Increase cybersecurity Awareness: The Nigerian government should intensify its actions by emphasizing the importance of cybersecurity through campaigns that educate individuals and organizations about the risks associated with cyber-crime and the

[165] F.E Ikuero "preliminary review of cybersecurity coordination in Nigeria. Nigerian Journal of Technology.2022, 41(3)pp.521-526 available at <https://www.ajol.info/index.php/njt/article/view/235311/222306 accessed >20 April 2024

[166] James ishaku,' securing the cyberspace,Gateway to digital economy-DG NITDA.'2021. available at https://nitda.gov.ng/securing-the-cyber-space-gateway-to-digital-economy-dg-nitda/4624/> accessed 20 April 2024

necessity of implementing strong cybersecurity measures. This initiative aligns with the objectives outlined in the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024, which underscores the significance of proactive measures in combating cybercrimes. By raising cybersecurity awareness, the Nigerian government can ensure that individuals and organizations understand the risks of cyber-crime, which in turn can lead to a more informed and compliant approach to cybersecurity regulations. When people are aware of the threats posed by cyber-crime, they are more likely to support and adhere to regulations aimed at combating such crimes, ultimately strengthening the overall cybersecurity framework in the country.

Strengthening Partnerships: It is crucial for the government to work closely with private sector entities and international allies to exchange information and pool resources in the fight against cyber-crime. The Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024 recognizes the significance of collaboration in combating cybercrimes and emphasizes the need for partnerships to enhance cybersecurity measures.[167] For instance, collaboration with tech companies like Microsoft and Google can provide valuable insights into emerging cyber threats, while partnerships with organizations like Interpol and the FBI can facilitate joint operations to track down cybercriminals operating across borders. Additionally, collaboration with international agencies like Interpol, as seen in the recent successful collaboration between the FBI and EFCC in "Operation Rewired," can significantly enhance efforts to combat cybercrimes on a global scale. By implementing these strategies, Nigeria can strengthen its cybercrime regulations and better protect its citizens from online threats.

Invest in cybersecurity infrastructure: To enhance its cybersecurity capabilities, the Nigerian government should allocate resources to build robust cybersecurity

[167] Section 10 of the Cybercrimes(prohibition, prevention etc)(Amendment)Act 2024

infrastructure. This includes establishing specialized cybersecurity training facilities to educate professionals on the latest cyber threats and defense strategies. Additionally, setting up incident response centers equipped with advanced technology can ensure swift and effective responses to cyber incidents. Investing in cybersecurity research and development centers will foster innovation in cybersecurity solutions tailored to Nigeria's specific cyber landscape. For example, creating partnerships with universities to conduct research on emerging cyber threats can lead to the development of cutting-edge cybersecurity tools and techniques to safeguard against cybercrimes.

Enhance cybersecurity Laws: The government should consider revising and enhancing current cybersecurity regulations to ensure they remain relevant and robust in combating both present and future cyber threats, as highlighted by the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024. This legislation reflects the ongoing efforts to adapt regulations to the evolving cyber landscape and strengthen legal mechanisms for addressing online offenses like harassment. It’s crucial to continuously review and improve cybersecurity laws to effectively safeguard against cybercrimes.

Invest in Cybersecurity Expertise: The Nigerian government should focus on advancing cybersecurity expertise within the nation by allocating resources to cybersecurity education and training initiatives. By investing in programs that enhance cybersecurity skills, the government can bolster its ability to combat cybercrimes effectively. For instance, establishing specialized cybersecurity courses in universities and offering training workshops for law enforcement officials can significantly strengthen the country's cybersecurity capabilities. These efforts would not only improve the overall cybersecurity landscape but also aid in the development of more robust cybercrime regulations that are better equipped to address modern cyber threats

To strengthen cybercrime regulations in Nigeria, it's crucial to take additional steps beyond current legislative measures, compliance efforts, and regulations. As they say, "A chain is only as strong as its weakest link," highlighting the importance of bolstering every aspect of cybersecurity to create a formidable defense against cyber threats and ensure a safer digital environment for all.

Conclusion: In concluding Chapter 3 on evaluating cybercrime regulations in Nigeria, it's essential to reflect on the current laws effectiveness, identify legal challenges, and suggest measures for improvement. By assessing the existing framework, recognizing obstacles, and proposing enhancements, we pave the way for a stronger legal landscape to combat cyber threats effectively. This thorough evaluation sets the stage for proactive steps to strengthen cybersecurity practices and safeguard digital spaces in Nigeria.

CHAPTER FOUR

COMPARATIVE ANALYSIS OF THE NIGERIA LEGAL FRAMEWORK ON CYBERCRIME WITH OTHER JURISDICTIONS

4.1 Introduction

In this chapter, a comparative analysis of cybercrime regulations will be conducted, examining the laws in the United States and the United Kingdom alongside those in Nigeria. By analyzing the cybercrime laws in these countries, the project aims to utilize the experiences and best practices from the US and UK to fill the gaps in the laws regulating cybercrime in Nigeria. Additionally, the role of international standards and cooperation in shaping effective cybercrime regulations will be explored, emphasizing the importance of global alignment and collaboration in combating cyber threats.

4.2 Cybercrime Laws in the United States

In the United States, the primary regulatory mechanisms addressing cybercrime are the Computer Fraud and Abuse Act (CFAA) and the Cybersecurity Information Sharing Act (CISA). These laws form the backbone of the country's efforts to combat cyber offences a and enhance cybersecurity.

Enacted in 1986, the Computer Fraud and Abuse Act (CFAA), also known as 18 U.S.C. 1030, is a cornerstone of U.S. cybersecurity legislation. It outlines several significant offenses to address the diverse range of cyber threats. Key provisions of the CFAA include unauthorized access to obtain information; which criminalizes accessing a computer without authorization or exceeding authorized access to obtain information from any protected computer[168], Knowingly accessing a computer without authorization or exceeding authorized access with the intent to obtain classified information that could harm national security[169], intentional

[168] 18 U.S.C. § 1030(a) (1)
[169] 18 U.S.C. S1030(a)(1)

transmission of a program, information, code, or command that results in damaging a protected computer,[170] trafficking of computer passwords[171],extortion involving computers[172].

The Computer Fraud and Abuse Act (CFAA) has undergone numerous amendments to keep pace with the evolving landscape of cybercrime. Between 1988 and 2008, the CFAA was amended nine time[173] reflecting the need to address new and emerging threats in cyberspace. The Act employs a three-tier system for enforcing violations, ensuring that penalties are commensurate with the severity of the offense[174]. Simple violations of the CFAA are treated as misdemeanors under both state and federal law. Individuals found guilty of these minor infractions can face imprisonment for up to one year and monetary penalties of up to $100,000[175]. Organizations found guilty of similar violations can be fined up to $200,000[176].

For more serious offenses, the CFAA imposes stricter penalties. Violations that fall into this second tier can result in imprisonment for up to five years.[177]Additionally, individuals may be fined up to $250,000, while organizations may face penalties up to $500,000. This tier of enforcement is designed to address more significant breaches of cybersecurity, such as repeated unauthorized access or actions that result in substantial harm or financial loss.

The most severe penalties under the CFAA are reserved for the gravest violations. Offenders in this third tier can be sentenced to up to ten years in prison[178]. Monetary penalties for these severe offenses can reach $250,000 for individuals and $500,000 for organizations.

The Cybersecurity Information Sharing Act (CISA), enacted in 2015 as part of the Consolidated Appropriations Act, aims to bolster cybersecurity by facilitating information

[170]18 U.S.C. § 1030(a) (5)
[171] 18 U.S.C. §1030(a) (6)
[172] 18 U.S.C. § 1030(a) (7)
[173] Caseguard,'The Computer Fraud and Abuse Act of 1986' available at CaseGuardhttps://caseguard.com › articles › th...The CFAA, Computer Fraud, Federal Government Regulations >accessed 23 May 2024
[174] Ibid
[175] 18 U.S.C. § 1030(a) (2)
[176] Ibid
[177] 18 U.S.C S 1030 (a)(4)
[178] 18 U.S.C. § 1030(b)

sharing between the government and private sector. CISA encourages collaboration, provides legal protections for sharing cybersecurity information, and promotes the adoption of best practices and standards. Critical sections of CISA include provisions which outlines government dissemination of cybersecurity information[179], governs private and public sector sharing with the government[180], offers liability protections for monitoring and sharing activities[181], and , which emphasizes the voluntary nature of the information-sharing framework[182].

The CISA complements the Computer Fraud and Abuse Act (CFAA) by providing a framework for the voluntary sharing of cybersecurity threat information between government agencies and private sector entities. While the CFAA focuses on criminalizing unauthorized access to computer systems and addressing cyber offenses, CISA enhances these efforts by facilitating collaboration and information sharing to prevent and respond to cyber threats effectively. Together, these legislative measures work in tandem to strengthen cybersecurity measures and protect critical infrastructure in the United States.

Another law in the United States that is utilized to address computer-related offenses is the Wiretap Act. This federal law, modified in 1986 by the Electronic Communications Privacy Act, Safeguards the confidentiality of wire, oral, and 'electronic communications, encompassing computer network communications within its scope[183] It is both procedural and substantive.[184]

It prevents not just law enforcement; But 'any person ' from engaging in an unlawful interception or sharing and using unlawfully intercepted content. [185]

---

[179] Section 103 of the CISA 2015
[180] Ibid section 105
[181] Ibid section 106
[182] Ibid Section 108
[183] Title 18 United States Code SS 2510-2522. The Wiretap Act
[184] Jarret. op. cit
[185] Wiretap Act. Section 2511 11

The prohibition crux of the Wiretap Act is found in Section 2511(1)(a), which prohibits 'any person' from intentionally intercepting, or attempting to intercept, any wire, oral or electronic communication. In contrast, if an action is unintentional and happens due to carelessness or error, it's not considered intentional.

Another federal law in the US concerning cybercrime is the Identity Theft Act[186]. This law criminalizes various behaviors involving fake ID documents or the improper use of identification details. Another US law related to this is the Access Device Fraud Act[187]

Prosecutors often file charges under Section 1029 in various phishing scenarios, where a defendant uses deceptive emails to acquire bank account details, and in "carding" situations, where a defendant deals with stolen bank account or card information[188]The penalties for breaking Section 1029 can lead to up to 10 or 15 years of imprisonment depending on the specific subsection breached[189]

There's also the CAN-SPAM Act of 2003[190], which provides a method for addressing individuals responsible for sending numerous unsolicited commercial emails, commonly referred to as 'spam. 'While the Act mainly relies on civil and regulatory measures for enforcement, it has also introduced various new criminal charges. Section 1037 provides as offences transmission of multiple commercial emails by (i) accessing a protected computer, without authorization, to send them or (ii) sending them through a protected computer with the intent of hiding their origin or (iii) materially falsifying header information or (iv) falsifying registration information for five or more email accounts or two or more domain names or (v) falsely representing oneself as the registrant of five or more intellectual property addresses (or conspiring to do so). [191]

---

[186] Identity Theft: Title 18 United States Code S 1028(a)(7)
[187] Access Device Fraud: Title 18 United States Code, S 1029
[188]Jarret., op. cit at 102-103
[189] Ibid Section 1029 (c)(1)(B)
[190] CAN-SPAM Act : 18 U.S.C S 1037
[191] Ibid

The punishment for breaking Section 1037 varies based on aggravating circumstances and past convictions, with penalties ranging from one year to five years. [192]

The enforcement of these laws is primarily handled by federal agencies such as the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), and the Cybersecurity and Infrastructure Security Agency (CISA). These agencies work collaboratively with state and local law enforcement, as well as international partners, to combat cybercrime.

4.3 United Kingdom

In the United Kingdom, the major cybercrime regulatory mechanisms are the Computer Misuse Act 1990 and the Data Protection Act 2018.

These frameworks are crucial for addressing cybercrime and ensuring the protection of personal data and the integrity of computer systems. The Computer Misuse Act enacted in 1990 and later amended in 2006 and 2008[193]is a key piece of legislation that was introduced to address the growing issue of cybercrime. The law establishes three primary offenses: (i) unauthorized access to computer material, (ii) unauthorized access to a computer system with the intention to commit or aid in further offenses, and (iii) unauthorized modification of computer material. [194]

The maximum penalties for these crimes vary from six months in prison and/or a 500 Euros fine to ten years in prison and/or an unlimited fine. The recent Police and Justice Act[195] includes changes to the CMA in the 'Miscellaneous Part 5 Computer Misuse amendments' section. For instance, Clause 39 increases the maximum prison sentence for hacking into computer systems from five years to ten years.

---

[192] Ibid Section 1037 (b)

[193] Lexisnexis, 'Computer Hacking and Misuse under the Computer Misuse Act 1990' available at LexisNexishttps://www.lexisnexis.co.uk › legalComputer hacking and misuse under the Computer Misuse Act 1990>accessed 23 May 2024

[194]CMA 1990, section 3

[195] (Commencement No 9)Order 2008

In 2015, Section 41 of the Serious Crime Act ushered in a significant change by introducing the new provision, section 3ZA[196] to the Computer Misuse Act 1990. This addition specifically addresses unauthorized actions that result in, or pose a threat of, substantial harm to computer systems. Similarly The Data Protection Act 2018 (DPA 2018) stands as a cornerstone of privacy legislation in the United Kingdom, offering comprehensive provisions to safeguard individuals' rights and regulate the handling of their personal information. At its core, the DPA 2018 aims to empower individuals by granting them greater control over their personal data[197]

One of its fundamental provisions is the delineation of data subject rights, ensuring that individuals have the ability to access[198], rectify[199], and erase[200] their personal data held by organizations.

Furthermore, the Act introduces stringent requirements for organizations to conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities.[201]

Additionally, the DPA 2018 mandates timely reporting of data breaches to the Information Commissioner's Office (ICO) and affected individuals, ensuring transparency and accountability in the event of security incidents.[202]

In contrasting the cybercrime laws and enforcement in the United States (US) and the United Kingdom (UK) with those in Nigeria, stark differences emerge. These differences encompass the stringency and comprehensiveness of laws, levels of public awareness, effectiveness of prosecution, the cultural perceptions of cybercrime and the cross border management and

[196] CMA 1990,Section 3ZA
[197] Gov.Uk, 'Data protection Act' available at https://www.gov.uk/data-protection#:~:text=Everyone%20responsible%20for%20using%20personal,used%20for%20specified%2C%20explicit%20purposes > accessed 23 May 2024
[198] DPA 2018,Section 45
[199] Ibid section 46
[200] Ibid section 47
[201] Ibid section 64
[202] Ibid Part 3

extradition. Understanding these contrasts is essential for highlighting the challenges and potential areas for improvement in Nigeria's approach to combating cybercrime.

The US and UK have developed stringent and comprehensive cybercrime laws that provide clear guidelines for identifying, prosecuting, and penalizing cybercriminals. In contrast, Nigeria's regulatory frameworks, while present, are less stringent and comprehensive. The Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 serves as Nigeria's primary legislation addressing cybercrime. However, enforcement of this law is inconsistent, and gaps in the legal framework hinder its effectiveness. The limited scope and implementation challenges of Nigeria's cybercrime laws underscore the need for more robust and enforceable legislation to effectively combat cybercrime in the country.

The 2024 amendments to the Cybercrimes Act aim to address some of these gaps and improve the robustness of Nigeria’s cybercrime legislation. The amendments include provisions that are particularly relevant to the prosecution of cybercrimes. For instance, the requirement for cyber incidents to be reported within 72 hours of detection, as opposed to the previous 7 days of occurrence[203], is designed to ensure quicker response times, which is crucial for effective law enforcement and prosecution. Additionally, the Act now includes public and private organizations, alongside financial institutions, broadening the range of entities that must comply with the law and can be held accountable for cybercrimes.[204]

While these amendments represent significant steps towards strengthening Nigeria’s cybercrime laws, the effectiveness of these changes will depend on their implementation and enforcement.

[203] Sectiom 21(1)(b) of The Cybercrimes(prohibition, prevention etc)(Amendment)Act,2024
[204]Ibid Section 22(1)

Public awareness and education about cybercrime are crucial in fostering a proactive approach to cybersecurity. In the US, organizations such as the Cybersecurity and Infrastructure Security Agency (CISA)[205]and the National Cyber Security Alliance (NCSA) play a pivotal role in promoting cyber hygiene and awareness. Initiatives like National Cybersecurity Awareness Month educate the public and businesses about cyber threats and protective measures. Similarly, the UK's National Cyber Security Centre (NCSC) provides extensive resources and guidelines to enhance public and corporate understanding of cybersecurity, thereby fostering a culture of vigilance and preparedness[206]. In Nigeria, public awareness and education about cybercrime are significantly lower. Limited outreach and educational initiatives contribute to a general lack of understanding and preparedness among the populace and businesses. This gap in awareness exacerbates the vulnerability of Nigerian individuals and organisations to cyber threats, highlighting the need for enhanced public education and awareness campaigns. The 2024 amendments to the Cybercrimes (Prohibition, Prevention, Etc.) Act also underscore the importance of public-private partnerships and capacity building for effective cybersecurity management[207]. These amendments include provisions for establishing sectoral Computer Emergency Response Teams (CERTs) and Security Operations Centers (SOCs)[208], which are intended to integrate public and private sector efforts in combating cyber threats.

[205] CISA,' CISA Cybersecurity Awareness Program' available at https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program> accessed 23 May 2024

[206] Matt Zbrog, National cybersecurity Awareness month 2022:an expert advocacy guide' available at https://www.forensicscolleges.com/blog/resources/national-cybersecurity-awareness-month> accessed 23 May 2024

[207] Section 41 (1)(d-j) of The Cybercrimes(prohibition, prevention etc)(Amendment)Act,2024

[208]Ibid Sectiom 41(1)(d)

Furthermore, the Act emphasizes the need for continuous capacity building for relevant security, intelligence, law enforcement, and military services[209]. By ensuring these agencies are well-equipped and knowledgeable about the latest cyber threats and defense mechanisms, Nigeria can enhance its overall cybersecurity posture. Nonetheless, bridging the gap in public awareness and education remains a critical challenge that requires concerted efforts from both the government and private sector to develop and implement comprehensive cybersecurity awareness programs.

Similarly, The effectiveness of prosecution and enforcement in the US and UK is evidenced by their track record in handling high-profile cybercrime cases. In the US, the Department of Justice has successfully prosecuted numerous cybercriminals. Notable examples include the conviction of Russian hacker Roman Seleznev for his involvement in a massive credit card fraud scheme [210] In the UK, law enforcement agencies have made significant strides in prosecuting cybercriminals, exemplified by the successful takedown of the Dark Overlord hacking group[211] which was responsible for numerous data breaches and extortion attempts.

Conversely, Nigeria faces substantial challenges in the prosecution and enforcement of cybercrime laws. The idolization of cybercriminals in Nigerian society undermines efforts to combat cybercrime effectively. The case of Ramon Olorunwa Abbas[212]known as Hushpuppi, is a prominent example. Hushpuppi, involved in extensive online fraud and money laundering activities, gained notoriety and admiration on social media for his lavish lifestyle funded by

---

[209] Ibid Section 41(1)(g)

[210] US attorney's office,'Russian cyber-criminal sentenced to 14 years in prison for role in massive online identity theft and bank fraud conspiracy' available at https://www.secretservice.gov/newsroom/releases/2017/12/russian-cyber-criminal-sentenced-14-years-prison-role-massive-online#:~:text=25%2C%202016%2C%20a%20federal%20jury,run%20concurrent%20to%20his%20sentences.>accessed 23 May 2024

[211] Kayla Deruiter 'member of the dark over lord hacker group caught and charged for cybercrime' October 28 2020 available at https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/elementor-9661/> accessed 23 May 2024

[212] United States of America v. Abbas,No.2:20-CR-00322-ODW(C.D.Cal.Jul.27,2021)

criminal activities[213].This cultural phenomenon glorifies cybercrime, making it difficult to deter potential offenders and enforce laws effectively.

Moreover, the involvement of law enforcement officials in cybercrime further complicates the situation in Nigeria. The case of Abba Kyaria[214] senior police officer implicated in aiding Hushpuppi, highlights deep-rooted issues within the system. Kyari's alleged involvement in helping Hushpuppi evade justice and his subsequent indictment in the US underscore the difficulties Nigeria faces in establishing effective cybercrime enforcement. Although the Cybercrimes (Prohibition, Prevention, Etc.) Act aim to address these issues, overcoming cultural attitudes that glorify cybercrime and addressing corruption within law enforcement remain crucial for these legislative improvements to be effective.

Cross-border cybercrime management and extradition are critical aspects of combating cybercrime, given the global nature of the internet and cyber threats. The US and UK have established mechanisms to address these challenges effectively. Both countries actively participate in international cooperation through organizations such as INTERPOL and the European Union Agency for Cybersecurity (ENISA)[215]. They have also signed numerous bilateral and multilateral agreements to facilitate the extradition of cybercriminals. For instance, the US has successfully extradited cybercriminals like Alexey Belan[216] from foreign jurisdictions, demonstrating its robust extradition framework.

In the UK, the Extradition Act 2003 and cooperation with European Union member states under the European Arrest Warrant (EAW) system enhance the country's ability to address

---

[213] Karimi.F and Madowo.O, 'A man who flaunted private jets and luxury cars on Instagram gets 11 years imprisonment gets 11 years in prison for Money laundering' November 8 2022,available at https://amp.cnn.com/cnn/2022/11/08/us/instagram-star-ray-hushpuppi-sentenced-cec> accessed 23 May 2024

[214] Ameh Ejekwonyilo,'Court grants Abba kyari bail' available at https://www.premiumtimesng.com/news/headlines/696746-court-grants-abba-kyari-bail.html#:~:text=The%20Federal%20High%20Court%2C%20Abuja,importation%20of%20cocaine%20and%20obstruction.> accessed 23 May 2024

[215] Sean Lyngaas,'U.S warns Countries not to manipulate the extradition process' for Cybercriminals ,November 19 2018 available at CyberScoophttps://cyberscoop.com › u-s-warn...U.S. warns countries not to 'manipulate the extradition process' for cybercriminals>accessed 23 May 2024

[216] Ibid

cross-border cybercrime[217] The UK's extradition agreements with various countries enable efficient prosecution of cybercriminals who operate internationally. In contrast, Nigeria faces significant challenges in dealing with transboundary cybercrime and extradition. Although Nigeria has signed international agreements and participates in regional initiatives like the African Union Convention on Cyber Security and Personal Data Protection, the practical implementation of these agreements is often hindered by bureaucratic inefficiencies and lack of resources. The case of Hushpuppi's extradition[218] to the US underscores the complexities involved. While Nigeria cooperated with US authorities in extraditing Hushpuppi, such high-profile cases are exceptions rather than the norm, indicating the need for more streamlined and effective extradition processes.

While the amended Cybercrime Act 2024 introduces provisions aimed at enhancing Nigeria's involvement in international cybersecurity cooperation, such as establishing platforms for public-private partnerships (PPP)[219]and integrating Nigeria into global cybersecurity frameworks[220]the practical impact of these new provisions remains to be seen. Despite the positive intentions of the 2024 amendment, there is a significant gap between the legislative framework and its implementation on the ground. Bureaucratic inefficiencies, resource constraints, and challenges in coordination still hinder effective cross-border cybercrime management and extradition in Nigeria. To bridge this gap, there needs to be a concerted effort to enhance the operational capabilities of enforcement agencies, streamline bureaucratic processes, and ensure adequate resources are allocated for cybercrime initiatives.

4.4 The Role of International Standards and Agreements in Cyber Space

[217] NCA,extradition arrangements with EU countries' available at National Crime Agencyhttps://www.nationalcrimeagency.gov.uk › ...Extradition arrangements with EU countries> accessed 23 may 2024

[218] Vanguard, ' Hushpuppi:Extradition request by U.S govt.not in good faith-Abba kyari tells court https://www.vanguardngr.com/2022/06/hushpuppi-extradition-request-by-u-s-govt-not-in-good-faith-abba-kyari-tells-court/amp/> accesssed 23 May 2024

[219] Section 41(1)(h) of the Cybercrime (prohibitions, prevention etc.)(Amendment)Act 2024

[220] Ibid section 41(1)(I)

Global agreements play a vital role in addressing cybercrime within cyberspace by establishing a regulatory framework for countries involved in these agreements. These agreements bind countries to adhere to the rules and regulations outlined in the treaties, conventions, and protocols. The following are some of the globally accepted treaties, conventions, and protocols impacting the majority of countries;

The agreement known as The Budapest Convention on Cybercrime: The Budapest Convention, also referred to as the Convention on Cybercrime[221],is the primary global agreement created to fight against cyber attacks. It was formulated by the Council of Europe, consisting of forty-one nations, in Strasbourg, France with the involvement of observer states from the Council of Europe, such as Canada, Japan, South Africa, and the United States.[222] This convention was signed in Budapest in 23rd of November,2001 and became effective in 2004. It was established to address the increasing worry about the insufficiency of laws concerning certain activities happening over computer networks. Approximately 68[223] countries have endorsed the Budapest Convention, with ten international organizations (such as the Commonwealth Secretariat, European Union, INTERPOL, International Telecommunication Union, Organization of American States, UN Office on Drugs and Crime, and more) engaging in the Cybercrime Convention Committee as members or observers.

This international legislation holds significant importance as it obligates countries similarly to a treaty. The responsibility of a state to fulfill its commitments under a treaty is explicitly outlined in Article 26 of the Vienna Convention on the Law of Treaties, which enforces the principle of pacta sunt servanda; every active treaty is obligatory for the involved parties and must be executed by them in good faith.[224] Treaties are the sole mechanism available for

[221] Budapest Convention on Cybercrime.Available on: https://www.coe.int accessed 27th April 2024
[222] Ibid
[223]https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en accessed >April 27th 2024
[224] Olawuvi, D. 'The Princioles of Nigerian Environmental Law/ (2013, Business Perspectives Publishing) at o 150

adjusting international law to new circumstances and reinforcing the authority of the rule of law among states.[225]

The convention primarily focuses on (i) harmonizing the domestic criminal law aspects of offenses and related provisions in the realm of cybercrime, (ii) establishing the necessary domestic criminal procedural law powers for investigating and prosecuting such offenses, along with other offenses carried out through a computer system or involving electronic evidence, and (iii) creating a rapid and efficient system for international cooperation.

Article 1 of the convention lays out definitions for four key terms crucial to the treaty. Firstly, the treaty defines a 'computer system' as a device comprising hardware and software designed for automatic processing of digital data. Regarding the second term, 'computer data,' it specifies that the data must be in a format directly processable by the computer system, meaning the data must be electronic or in a form that can be processed directly. The third term, 'service provider,' encompasses a broad range of entities that fulfill specific roles concerning the communication or processing of data on computer systems. This definition encompasses not only public or private entities but also includes those that store or handle data on behalf of public or private entities. And finally,, "traffic data" includes computer data linked to a communication via a computer system, generated by a system in the communication chain, disclosing details like the start, end, route, time, date, size, duration, and service type of the communication.[226]

The treaty mandates that countries (meaning states that have ratified it) must enact laws and take actions to make it a criminal offense under their own laws, when done on purpose, to aid or support the commission of crimes against the confidentiality, integrity, and availability of

225 Brierly, J., 'The Law of Nations: An Introduction to the International Law of Peace (Oxford University Press, 6* ed.1963) p 57

226 https://www.refworld.org/legal/agreements/coe/2001/en/90189 accessed> 27th April 2024

computer data and systems, as well as offenses involving copyright and related rights with the intention of committing such offenses.[227]

According to Article 11, ratifying states must follow the convention honestly and incorporate all the specific crimes outlined in the treaty. These crimes include :

-Accessing a computer system, in whole or part, without right, with the intention of acquiring computer data or for other deceitful purposes, especially in connection to a computer system linked to another one[228]. The term 'without right' refers to actions taken without permission, whether it's not authorized by law, contract, or any other established legal defenses. If there is proper authorization to access the computer system or data, this rule does not apply.

-Unauthorized interception using technical methods of private transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system transmitting such data.[229]

-Unauthorized actions such as harming, deleting, corrupting, changing, or removing computer data are covered in the convention[230]. However, a party can choose to specify that the action must result in significant harm. This clause can be applied to prosecute criminal activities involving the deployment of harmful malware and viruses to destroy computer data.

-Interfering with the proper operation of a computer system without authorization by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.[231]

The second key section of the Convention mandates that countries must establish specific procedures and mechanisms to simplify the investigation of cybercrime or any offenses committed using a computer or where evidence may be in electronic form. This part

[227] Convention on Cybercrime, Article 11
[228] Convention on Cybercrime. Article 2
[229] Convention on Cybercrime, Article 3.
[230] Convention on cybercrime, Articie 4
[231] Convention on Cybercrime, Article 5

necessitates ratifying states to implement legislative and other actions required to empower their authorities to conduct investigations related to the crimes outlined in the Convention.[232]

The third major section of the Convention outlines how countries that are part of the agreement will support one another in investigating cybercrimes and other offenses that involve electronic evidence.[233]

Nigeria signed the Budapest Convention on Cybercrime on July 6, 2022

This move signifies Nigeria's commitment to aligning its legal frameworks with international standards for combating cybercrime and fostering international cooperation in cyberspace

4.5 The United Nations (UN):

The United Nations (UN) with headquarters in New York, USA, is dedicated to global cybersecurity. The UN has set up expert groups and hosted conferences on Information and Communication Technology (ICT) and cyber threats. In 2012, the then UN Secretary-General, Ban Ki-moon, appointed a group of 15 experts from the five permanent members of the UN Security Council and countries like Argentina, Australia (the chair), Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to carry out a mandate from the UN General Assembly to explore potential cooperative measures in addressing current and future threats linked to the use of information and communication technologies (ICTs) (as mentioned in Wolter, 2020).

Additionally, as part of the United Nations' dedication to ensuring global cybersecurity, in 2018, the United Nations Office of Drug and Crime (UNODC) organized an International Academic Conference on Linking Organized Crime and Cyber Crime in Chuncheon, Republic of Korea. Experts from around the world, including academics and practitioners, were invited to the two-day conference, which was done in collaboration with Hallim

[232] Convention on Cbercrime, Articles 14-21
[233] Covention on Cvbercrime. Articles 23-35

University in Chuncheon, Republic of Korea. Another initiative was the launch of the Global Cybersecurity Index (GCI) by the UN International Telecommunications Union (ITU) to assess the state of cybersecurity worldwide.

4.5 Computer and Computer-Related Crimes Model Law:

The Commonwealth Secretariat created a "Model Law on Computer and Computer-Related Crime" for the 53 member countries of the Commonwealth in October 2002. This Model Law broadened the range of criminal responsibility for crimes related to the internet and computer systems, including the misuse of unauthorized computer-related tools and activities. When it comes to cybercrime, the Model Law also brought in the concept of dual criminality. This means that if someone commits a crime outside their own country, they can be prosecuted if their actions would be considered illegal under the laws of the country where the crime occurred. This principle of dual criminality can lead to charges or extradition. Some member countries have used the Model Law as a basis for creating their own domestic cyber laws.

The Group of Eight, also known as G8, is composed of eight countries. The main focus of the G8 was on prosecuting high-tech criminals and enhancing technical and legal measures to address global computer crimes during the Denver Summit in 1997.[234]

At the Okinawa Summit 2000, the Okinawa Charter on Global Information Society adopted the principles of international collaboration and harmonization for cybercrime. The Group of Eight agreed on importance and principles for the protection of privacy, free flow of information, and security of transactions.

[234] https://blog.ipleaders.in/regulatory-framework-for-cyber-crimes/

The United Nations Convention Against Transnational Organized Crime (UNCTOC) was approved by the United Nations in 2000. The Palermo Convention mandates that member states establish local criminal laws aimed at organized criminal organizations, along with updated protocols for extradition, mutual legal aid, and collaboration among law enforcement agencies. While the treaty doesn't explicitly address cybercrime, its guidelines are highly relevant in this context.

All these guidelines work together to build a solid base for tackling issues in the online world. They encourage countries to cooperate, align their laws, and agree on the rules that govern online behavior. By teaming up to combat cybercrime and its effects on communities, these global standards and deals contribute to a safer and more robust online environment for everyone. Looking ahead, ongoing teamwork and adjusting to new risks will be vital to safeguarding the safety and security of the worldwide digital realm.

4.6Conclusion

The comparative analysis of cybercrime regulations in the United Kingdom, the United States, and Nigeria reveals distinct approaches to addressing cyber threats. While the UK and US boast established frameworks, Nigeria’s legal system is still evolving.

Despite differences, Nigeria can benefit from international standards. The recent amendments to the Cybercrime Act in 2024 signify progress toward aligning regulations with global initiatives. Continued efforts and participation in international collaboration can enhance Nigeria’s capacity to combat cybercrime and safeguard its digital infrastructure.

Overall,As discussed earlier, international standards and agreements play a pivotal role in shaping cyberspace. By adhering to these standards and leveraging international agreements,

Nigeria can bolster its cybersecurity capabilities and contribute to global efforts against cyber threats.

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

5.1 Summary

This research work, "Assessment of Cybercrime Regulations in Nigeria," provides a comprehensive evaluation of the current state of cybercrime regulations in the country. The study began with a literature review on cybercrime, examining existing research and scholarly works on the subject. This review highlighted prevalent types of cybercrimes such as phishing, identity theft, ransomware attacks, and online fraud. Understanding these various forms of cybercrime allowed for a critical assessment of Nigeria's regulatory framework and its effectiveness in addressing these threats.

Through the analysis of historical examples, causes, impacts, and existing cyber laws, the research identified significant challenges and gaps within Nigeria's regulatory framework for combating cybercrime. The findings underscore the necessity of revising the Cybercrime Act of 2015 and other related laws to effectively address the evolving nature of cyber threats. Key recommendations include enhancing collaboration among law enforcement agencies, allocating additional resources and training for personnel, and increasing public awareness initiatives to strengthen enforcement and prevention efforts.

The recent amendments introduced by the Cybercrime Amendment Act 2024 represent a significant step towards addressing the identified challenges.

Provisions within the amendment enhance collaboration among law enforcement agencies, introduce new enforcement mechanisms, and allocate additional resources for cybersecurity efforts. These changes align closely with the recommendations outlined in this study, reflecting a proactive approach to strengthening Nigeria's cybercrime regulatory framework.

A comparative analysis of cybercrime regulations in Nigeria, the US, and the UK provided valuable insights into best practices that Nigeria could adopt. Learning from the experiences of these countries can help Nigeria improve its cybercrime response strategies. Additionally, active participation in international initiatives and adherence to global standards are essential for Nigeria to combat cybercrime effectively. Collaborating with international partners and organizations offers access to expertise and resources critical to supporting Nigeria's efforts.

In conclusion, this study highlights the pressing need for a robust and adaptive cybercrime regulatory framework in Nigeria, supported by international cooperation and informed by global best practices. The recent amendments introduced by the Cybercrime Amendment Act 2024 represent a significant step forward, but ongoing vigilance and adaptation are essential to stay ahead of evolving cyber threats.

5.2 Recommendations

From the findings of the project, it is recommended as follows for enhanced cybercrimes regulatory efficiency:

1. Improved international collaboration with other countries for enhanced cross border prosecution of cyber criminals.
2. Swift and effective prosecution of Cybercriminals, supported by the enhanced enforcement mechanisms introduced by the Cybercrime Amendment Act 2024, to reduce the impunity with which the crime is perpetrated in Nigeria.
3. Naming, Shaming, and tracing revenues confiscated from Cybercriminals to discourage the crime.
4. As indicated in the comparative analysis of cybercrime in the US and UK,the Nigeria cybercrime Act should be urgently reviewed and updated to reflect the evolving nature of

cyber threats. The recent amendments introduced by the Cybercrime Amendment Act 2024 should be considered in this review process.

5. Invest in robust cybersecurity infrastructure for both the public and private sectors. This includes securing critical national infrastructure and adopting best practices for data protection and privacy.
6. The public must be thoroughly educated on effective methods to protect computer systems and data. This includes promoting the use of strong, unique passwords and reliable antivirus software to safeguard personal and business data. For instance, teaching people to utilize comprehensive security measures such as firewalls, encryption, and two-factor authentication can significantly reduce the risk of cyber threats.
7. Create user-friendly and efficient mechanisms for reporting cybercrimes, aligning with the provisions introduced by the Cybercrime Amendment Act 2024 to streamline reporting processes and facilitate prompt response by law enforcement agencies.
8. Encourage ongoing research into cybercrime trends and innovative solutions. By staying informed about new developments in cybersecurity, Nigeria can better adapt its strategies to evolving threats.
9. The Cybercrime Act ought to include clauses for compensatory damages and other types of relief for individuals impacted by cybercriminal actions, mirroring the regulations outlined in the United States under Subsection 1030(g) of the Computer Fraud and Abuse Act. These actions would offer victims a way to pursue compensation for their damages and assist them in recuperating from the consequences of cybercrime.
10. Regularly hosting seminars and workshops is essential to educate the public about the importance of safeguarding their personal information. These events can provide valuable insights into the latest threats and best practices for data protection.

11. Both financial institutions and individuals must prioritize the consistent and proper use of firewalls to safeguard against cyberattacks. Firewalls act as a critical barrier, helping to block unauthorized access and filter out potentially harmful malware or malicious code.
12. The government should prioritize the creation of job opportunities and provide platforms for youth to gain entrepreneurial skills. By investing in these areas, the government can empower young people to establish their own careers and pursue legitimate avenues of income.
13. Equip law enforcement agencies with specialized training and resources to effectively investigate and prosecute cybercrimes, supported by the provisions introduced by the Cybercrime Amendment Act 2024 to enhance law enforcement capabilities.
14. It is crucial for Nigeria to conduct a comprehensive review of the Cybercrime Act of 2015, as amended by the Cybercrime Amendment Act 2024 to ensure alignment with global best practices and emerging cyber threats
15. Establish a comprehensive national cybersecurity strategy that outlines clear objectives, responsibilities, and timelines for combating cybercrime.

5.3 Conclusion

Based on the findings of this study, it is evident that cybercrime poses a significant threat to Nigeria's economy and national security. The misuse of computer technology not only jeopardizes public safety but also has severe repercussions for individuals and businesses. However, Nigeria faces challenges in effectively combating cybercrime, including a weak legal framework and inadequate enforcement measures.

The recent amendments introduced by the Cybercrime Amendment Act 2024 represent a crucial step towards addressing these challenges. By enhancing collaboration among law enforcement agencies, introducing new enforcement mechanisms, and allocating additional

resources for cybersecurity efforts, the amendment strengthens Nigeria's ability to combat cyber threats. Moreover, the amendments provide a framework for international cooperation in prosecuting cybercriminals, aligning with the recommendations outlined in this study.

However, to fully address the threat of cybercrime in Nigeria, sustained efforts are required. A radical review of the Cybercrime Act, incorporating the insights provided by the Cybercrime Amendment Act 2024, is essential.

This review should be supported by transnational prosecution of cybercriminals, facilitated by well-equipped law enforcement agencies and a proactive judiciary. Only through comprehensive legal reforms and effective enforcement measures can Nigeria effectively tackle cybercrime and safeguard its citizens and businesses from the growing threat posed by cybercriminal activities.