AN EXPLORATORY ANALYSIS OF THE EFFICACY OF NIGERIA'S CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT 2015: LEGAL FRAMEWORKS, CHALLENGES, AND PROSPECTS FOR COMBATING CYBERCRIME

SUBMITTED

BY

OKIBE, EMMANUEL SUNDAY
(2019/LW/12433)

TO

THE DEPARTMENT OF LAW, FACULTY OF LAW
ALEX EKWUEME FEDERAL UNIVERSITY, NDUFU-ALIKE, IKWO, (AE-FUNAI)
EBONYI STATE

SUPERVISOR
OLEBARA, OGUGUO PASCHAL ESQ.

OCTOBER, 2024

TITLE PAGE

AN EXPLORATORY ANALYSIS OF THE EFFICACY OF NIGERIA'S CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT 2015: LEGAL FRAMEWORKS, CHALLENGES, AND PROSPECTS FOR COMBATING CYBERCRIME

DECLARATION

I, Emmanuel Okibe, hereby solemnly declare that this research work, titled **An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks Challenges, and Prospects for Combating Cybercrime**, submitted in partial fulfilment of the requirements for the award of LL.B, is an original and authentic production of my intellectual endeavours.

I attest that:

1. This research work has not been previously submitted, published, or disseminated in any form.
2. All sources utilized in this research have been properly acknowledged, cited, and referenced in accordance with established academic conventions.
3. This work does not infringe upon any copyright, patent, trademark, or other intellectual property rights.
4. This research was conducted in compliance with applicable laws, regulations, and ethical standards.

I hereby assume full responsibility for the accuracy, integrity, and validity of this research.

Signature: _____

Date: _____

Name: _____

Matric Number: _____

APPROVAL AND CERTIFICATION

PURSUANT TO THE REQUIREMENTS of Alex Ekwueme Federal University, Ndufu-Alike, Ikwo, Ebonyi State, and the Faculty of Law therein, it is hereby certified that the research work titled **An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks Challenges, and Prospects for Combating Cybercrime**, submitted by **Emmanuel Okibe** in partial fulfillment of the requirements for the award of LL.B, has been examined and approved as meeting the standards of scholarship and research.

NOW, THEREFORE, BE IT RESOLVED that the research work titled **An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks Challenges, and Prospects for Combating Cybercrime**, is hereby approved:

OLEBARA, OGUGUO PASCHAL ESQ	**DR K.G ONYEGBULE**
(SUPERVISOR)	**(COORDINATOR)**

ASSO. PROF. ESENI AZU UDU
(DEAN OF FACULTY)

EXTERNAL EXAMINER

DEDICATION

In loving memory of Harmony Peace Ogbonna, my coursemate, friend, and sister. Your love and legacy leave an indelible mark on my heart. Dedicated to your eternal spirit!

.

ACKNOWLEDGEMENTS

I hereby acknowledge the contributions and support of the following individuals, whose roles were instrumental to my academic journey and the completion of this research.

I extend sincere appreciations to Olebara, Oguguo Paschal Esq., my project supervisor, for his expert guidance and invaluable insights, Dr Goodluck Kelechi Onyegbule, Head of Department, for his leadership and mentorship through the beginning to the end of our project work and Asso. Prof. Eseni Azu Udu, Dean of the Faculty of Law, for his fatherly roles and unwavering lectures that shaped us all.

My heartfelt gratitude goes to my brother, Joseph Okibe, whose financial support enabled me to pursue my education. I am also indebted to Faith Ederisi, my online friend and pillar of strength, whose support transcended borders. My appreciations also go to Okam Ifesinachi Joy, a true friend in need and indeed. I fondly remember Harmony Peace Ogbonna, my late friend, sister, and coursemate, whose friendship and camaraderie left an indelible mark on my academic journey.

TABLE OF CASES

LIST OF STATUTES

A

Advance Fee Fraud and Other Fraud Related Offences Decree No.13 of 1995 Act CAP. A6 L.F.N. 2004

Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006

African Union's Convention on Cyber Security and Personal Data Protection, 2014

B

Banks and Other Financial Institutions Act, 1991. Cap. B3, Laws of the Federation of Nigeria, 2004.

Banks and Other Financial Institutions Act, 2020, No. 5, A653.

Budapest Convention on Curtailing the Menace of Cybercrime 2001

C

Charter of the United Nations, 1945.

Computer Fraud and Abuse Act (CFAA) of 1986

Computer Misuse Act 1990 (CMA)

Constitution of the Federal Republic of Nigeria (As Amended) 1999

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 2007

Criminal Code Act, Cap. 77 Laws of the Federation of Nigeria, 1990

Criminal Code Act, Cap. C38 Laws of the Federation of Nigeria, 2004.

Cybercrime (Prohibition, Prevention, etc.) Act 2015

Cybercrimes Act 19 of 2020

E

Economic and Financial Crimes Commission (EFCC) (Establishment) Act, 2004

Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime Within ECOWAS

Electronic Communications and Transactions Act 25 of 2002

European Union Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography

Evidence Act, 2011. No. 18, Acts of the National Assembly of the Federal Republic of Nigeria, 2011.

F

Failed Banks (Recovery of debts) and Financial Malpractices in Banks Act 1994

M

Miscellaneous Offences Act

Money Laundering (Prohibition) (Amendment) Act, 2012

Money Laundering (Prohibition) Act, 2011

Money Laundering Act, 2004

N

National Information Infrastructure Protection Act of 1996

National Information Technology Development Agency (NITDA) Act, 2007

Nigerian Communications Act, 2003

Nigerian Criminal Code Act CAP C 39 Laws of the Federal Republic of Nigeria 2004

P

Penal Code (Northern States) Federal Provisions Act, Cap P.3 Laws of the Federation of Nigeria 2004.

Police and Justice Act of 2006

S

South Africa, ECT Act (Electronic Communications and Transactions Act No 25 of 2002.

Stanford Draft International Convention in order to avoid needless debates 1999

Substantial Crime Act of 2015

U

United Nations Convention on the Use of Electronic Communication in International Contracts, 2005

United Nations Convention on the Use of Electronic Communication in International Contracts, 2002.

United Nations Conventions on the Rights of the Child 1989

United Nations General Assembly, Resolution 56/183

USA PATRIOT Act 2001

W

West African States (ECOWAS) Directive C/DIR.1/08/11 2011

LIST OF ABBREVIATIONS

A.T.M.	Automated Teller Machine
C.D.	Compact Disk
C.I.A.	Central Intelligence Agency
E.F.C.C.	Economic and Financial Crimes Commission
E.U.	European Union
G.A.O.	Government Accountability Office
I.C.A.N.N.	Internet Corporation for Assigned Names and Numbers
I.C.C.C.	Internet Crime Complaint Center
I.C.T.	Information and Communication Technology
I.D.	Identity
I.T.U.	International Telecommunication Union (ITU)
L.A.	Los Angeles
N.A.S.A.	National Aeronautics and Space Administration
N.C.C.	Nigerian Communications Commission
N.I.T.D.A.	National Information Technology Development Agency
P.O.S.	Point of Sale
PW2	Prosecution Witness 2
S.A.B.R.I.C.	South African Banking Risk Information Centre
S.A.P.S.	South African Police Service
SMEs	Small and Medium-Sized Enterprises
U.K.	United Kingdom
U.N.D.O.	United Nations Office on Drugs and Crime
U.S.A	United States of America

TABLE OF CONTENTS

CHAPTER THREE

Legal Regime and Institutional Framework for Combating Cybercrime In Nigeria

ABSTRACT

One of the most creative and practical inventions of humankind is the development of the internet, computers, and mobile phones. The benefits of these technological advancements are immeasurable. For example, transactions between parties in different jurisdictions can be completed over the internet, and personal correspondence has become easier than it was in the 18th and 17th centuries when letters were used slowly. However, with the convenience of the internet and technology also comes the risk of cyberattacks and data breaches. As more and more sensitive information is shared online, individuals and companies are increasingly vulnerable to hackers and cybercriminals. In a similar spirit, technological advancements have brought about immeasurable harm, raised the frequency of crimes, broadened the scope of illegal activity, and produced a brand-new class of crimes known as cybercrimes. Nigeria, as a country experiencing rapid technological growth, has not been immune to the rise of cybercrime. In response to this growing threat, the Nigerian government enacted the Cybercrime (Prohibition, Prevention, etc.) Act in 2015. This legislation aims to provide a legal framework for combating cybercrime in Nigeria by defining offences, outlining penalties, and establishing procedures for investigation and prosecution. However, the effectiveness of this law in addressing the dynamic nature of cybercrime remains a subject of debate among legal scholars and practitioners. To allow for a detailed examination of the legal framework itself, focusing on the text of the Act and how it compares to international best practices, this research adopted the doctrinal methodology to analyze the key provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, and evaluate its effectiveness in combating cybercrime in Nigeria. The study found that while the Act introduces important provisions such as criminalizing cybercrimes, providing for international cooperation, and establishing the National Cybersecurity Fund, there are still challenges in its implementation and enforcement. These challenges include a lack of adequate resources and expertise within law enforcement agencies, as well as a lack of awareness and understanding among the general public about cybercrime and how to report it. It is concluded, therefore, that the Act does not address emerging cyber threats which are becoming increasingly prevalent. It is recommended that there should be a continuous review and amendment of the Act to keep up with the rapidly evolving nature of cybercrimes and technology.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Ontological concept held by scholars over the years has been that human evolution in time and space is inevitable and that technology will continue to advance at a rapid pace.[1] In today's world, we are witnesses to this inevitable evolution as the digital landscape becomes more complex and interconnected. Irrespective of how empirical this may seem, human activities continue to increase, and in this increment lies a pressing need to navigate the complexities of the digital age. This is evident enough in Premium Times news report on the statement of Nigeria's Senate President**,** Godswill Akpabio, who expressed his worry over the huge financial losses Nigeria suffers as a result of cybercrime activities in the country. He asserted that:

> 'In this age of rapid technological advancement and widespread internet usage, cybercrime has emerged as a grave menace to our society, economy and personal security. It is imperative to strengthen the existing laws on cybercrime prohibition and prevention. In the past, certain individuals with misguided intentions exploited our weak cybercrime laws, thereby tarnishing the reputation of our country. They engaged in a wide array of illegal activities, such as hacking, identity theft, fraud, harassment and cyber terrorism. These crimes not only inflicted significant financial losses upon our country, but also invaded our privacy, disrupted critical infrastructure, and eroded trust in our digital systems'[2].

Suffice that to be what it may, it should be noted, therefore, that with the help of technology, nations have come together to form the global village that is today our world.[3] And this interconnectedness has greatly impacted the way we communicate, trade, and interact with one

---

[1] A Somit and SA Peterson (eds.), *The Dynamics of Evolution* (Cornell University Press, 1992) 35

[2] Premium Times News Report (2023) 'Nigeria losing huge resources to cybercrime – Akpabio'. Available at <https://www.premiumtimesng.com/news/more-news/645665-nigeria-losing-huge-resources-to-cybercrime-akpabio.html?tztc=1> accessed on 17 April 2024.

[3] F Okeshola and A Adeta, 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria Kaduna State, Nigeria'. *American Journal of Contemporary Research* [2013] (3) (9) 98.

another. Today, the majority of nations rely on the internet to complete significant business deals that have an influence on their economies. Indeed, the present notion of the information society has developed as a result of the integration of information and communication technology (ICT) into many facets of daily life[4]. To uphold this assertion, Data Reportal in their publications stated that, globally, there are currently approximately 5.31 billion mobile phone connections and 4.95 billion internet users[5]. As per a statistic released by the International Telecommunication Union (ITU), Nigeria had over 45 million internet users as of 2011. This accounts for 26.5% of the country's total population.[6] According to current numbers given by Internet World Stats, Nigeria ranks seventh in terms of countries with the biggest number of internet users in the world, with 115.99 million total internet users as of the end of 2021.[7] This figure is expected to increase to more than 143.26 million internet users by 2026.[8]

Summarily, the whole essence of the foregoing is that, in his present stage of evolution, man has approached and has come to live in the information era, which depends more on ideas, knowledge, and practical applications than it does on coal or steel for progress. One may now have contact with almost anyone on the planet via cyberspace, and doing business has gotten a little bit easier. The frequent electronic delivery and purchase of goods and services has had a profound impact on sectors including banking, travel, and journalism.[9] Indeed, the concept of a safe cyberspace is now crucial to both national security and economic growth. It is clear that the

---

[4] International Telecommunication Union (ITU), 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) September Report, available at <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> accessed 14 May 2024

[5] DataReportal, 'Digital 2022: Global Overview Report', available at <https://datareportal.com/reports/digital-2022-global-overview-report> accessed 14 May 2024.

[6] International Telecommunication Union (ITU), at *ibid* note 4

[7] Statista, 'Number of Internet Users in Nigeria from 2017 to 2026', available at: <https://www.statista.com/statistics/183849/internet-usersnigeria/> accessed 14 April 2024.

[8] *Ibid*

[9] M Olusola 'Cyber Crimes and Cyber Laws'. *The International Journal of Engineering and Science* [2013] (2) (4) 19.

importance of regulating and preventing cybercrime is more vital now than ever before. With the increasing reliance on cyberspace for communication and business transactions, it is essential to review the legal framework in place to protect individuals and businesses from cyber threats. One such piece of legislation is the Cybercrime (Prohibition, Prevention, etc.) Act 2015 in Nigeria, which aims to address the growing threat of cybercrime in the country.

All the greater, despite the benefits of the information age and new trade instruments, cyberspace is still a dangerous place for crime, personal privacy, political and socioeconomic stability, and national security. With its increasing and underlying benefits, there are prices to pay for the increasing convenience of the internet. To Ashaolu, the growth of the internet and increased accessibility to computer technology has not only opened up new avenues for business ventures but have also made it easier for people engaged in illicit activity to prosper.[10] Kshetri did not fail to also assert that, the growing insecurity of the digital world is a result of the relationship between organised crime and the internet.[11] A number of clever crimes that were previously outside the purview of our criminal code have been linked to the introduction of the internet.[12] This has made it necessary for several nations to pass legislation designed to lessen the impact of crime in cyberspace. The goal of Nigeria's Cybercrime (Prohibition, Prevention etc.) Act 2015 is to outlaw, deter, and punish cybercrimes in the nation, which has developed into a global hub for illegal activity on the internet.[13]

---

[10] O Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber security in Nigeria'. *Academic Journal* [2014] (6) (3) 116

[11] N Kshetri, 'Pattern of Global Cyber War and Crime: A Conceptual Framework'. *Journal of International Management* [2005] (11) (4) 541

[12] D Ashaolu, 'Combating Cybercrimes in Nigeria' in D Ashaolu (ed.) *Basic Concepts in Cyberlaw* (Velma Publishers 2012) 46.

[13] CF Izuakor, 'Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context'. *ISSA Journal* [2021] 28-29.

Based on the above highlights, this study aims to critically analyze the effectiveness of the Cybercrime (Prohibition, Prevention, etc.) Act 2015 in combating cybercrimes in Nigeria. By examining the provisions of the Act and comparing them to international best practices, this study seeks to identify any gaps or weaknesses that may hinder its implementation. Hence, the research will explore the challenges faced by law enforcement agencies in enforcing the Act and propose recommendations for improving Nigeria's legal framework for combating cybercrime.

1.2 Statement of the Problem

The Cybercrime (Prohibition, Prevention, etc.) Act 2015, Nigeria's primary legislative instrument for combatting cybercrime, exhibits significant shortcomings in its conceptualization, design, and implementation, thereby undermining its efficacy in addressing the complex and evolving nature of cyber threats. The problem is compounded by:

- Ambiguities and inconsistencies in key provisions, hindering effective enforcement and interpretation
- Inadequate safeguards for protecting victims' rights and interests
- Limited mechanisms for facilitating international cooperation and mutual legal assistance
- Potential infringements on human rights and fundamental freedoms
- Insufficient adaptability to emerging technologies and cyber threats, among others.

This research seeks to critically examine the Act's deficiencies and propose comprehensive reforms to strengthen Nigeria's legal framework for combatting cybercrime, ensuring a more effective, efficient, and rights-respecting approach to mitigating the risks and consequences of cybercrime.

The Cybercrime Act 2015, despite its noble intentions, has been criticized for its narrow scope, outdated provisions, and inadequate penalties, rendering it ineffective in addressing the dynamic and borderless nature of cybercrime. The Act's focus on punishment rather than prevention, coupled with its failure to provide adequate resources and support for law enforcement agencies, has hindered its ability to effectively combat cybercrime. Furthermore, the Act's lack of clarity on key concepts, such as "cybercrime" and "computer systems," has led to confusion and inconsistencies in its application, resulting in a fragmented and ineffective approach to cybercrime prevention and control. This research aims to critically evaluate the Act's provisions, identify areas of improvement, and propose comprehensive reforms to strengthen Nigeria's legal framework for combatting cybercrime.

The research questions that will guide this analysis include:

1. What are the specific types of cybercrimes prohibited under the Cybercrimes Act 2015, and how have they evolved since the Act's inception in 2015?
2. To what extent has the Cybercrimes Act 2015 been effective in preventing and prosecuting cybercrimes in Nigeria, and what challenges remain in mitigating these threats?
3. What are the primary challenges and limitations faced by prosecutors in Nigeria when pursuing cybercrime cases, and how can these obstacles be addressed through policy or legislative reforms?
4. How do legislative frameworks and enforcement mechanisms for cybercrime prevention in Nigeria compare to those in other jurisdictions, and what lessons can be learned from these comparisons?

5. Drawing on lessons from selected jurisdictions, what strategic reforms in legal frameworks and governance structures are required to enhance Nigeria's cybercrime resilience and effectively mitigate emerging cyber threats?

1.3 Aim and Objectives of the Study

The main objective of the study is to carry out an exploratory analysis of the efficacy of Nigeria's cybercrime (prohibition, prevention, etc.) act 2015: legal frameworks, challenges, and prospects for combating cybercrime. The specific objectives of the study are:

1. To identify and examine the specific types of cybercrimes prohibited under the Cybercrimes Act 2015 and analyze their evolution since the Act's inception in 2015.
2. To assess the effectiveness of the Cybercrimes Act 2015 in preventing and prosecuting cybercrimes in Nigeria and identify remaining challenges in mitigating these threats.
3. To investigate the primary challenges and limitations faced by prosecutors in Nigeria when pursuing cybercrime cases and recommend policy or legislative reforms to address these obstacles.
4. To compare and contrast legislative frameworks and enforcement mechanisms for cybercrime prevention in Nigeria with those in other jurisdictions, and identify lessons learned from these comparisons.
5. To investigate and identify strategic reforms in legal frameworks and governance structures necessary to enhance Nigeria's cybercrime resilience, drawing on lessons from selected jurisdictions, and to develop evidence-based recommendations for effective mitigation of emerging cyber threats.

1.4 Scope and Limitations of the Study

This study aims to conduct an exploratory analysis of the efficacy of Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act 2015. The scope of this research encompasses an examination of the legal frameworks established by the Act to prevent and prosecute cybercrimes in Nigeria. Specifically, it investigates the challenges encountered in implementing the Act, including enforcement, jurisdictional issues, and technological limitations. Additionally, the study evaluates the effectiveness of the Act in combating cybercrimes, such as online fraud, identity theft, and data breaches. Finally, it identifies future prospects for improving the Act's efficacy, including proposed amendments, international cooperation, and capacity building.

This study is subject to several limitations. Firstly, the research relies on secondary data sources, including existing literature, case laws, and reports from law enforcement agencies. Secondly, the geographical scope is limited to Nigeria's Cybercrime Act 2015 and its application within the country's jurisdiction. Thirdly, the study concentrates on the period since the Act's enactment in 2015 to the present day. Furthermore, the exploratory nature of this study precludes an exhaustive examination of all aspects of the Act's efficacy. The study may also not capture the perspectives of all stakeholders, including law enforcement officials, legal practitioners, and cybersecurity experts. Another limitation is the rapidly evolving nature of cybercrime, which may affect the study's findings. Lastly, limited access to sensitive information, such as confidential law enforcement records or cybersecurity reports, may constrain the research.

To maintain focus and feasibility, this study delimits its scope by excluding an in-depth analysis of international cybercrime laws and frameworks. It also does not examine the economic impact of cybercrime on Nigeria's economy. Furthermore, the study focuses primarily on the legal

aspects of cybercrime prevention and prosecution, acknowledging areas for future research and potential expansion.

1.5 Significance of the Study

This study has both theoretical and practical significance. Theoretically, this study contributes to the existing literature on cybercrime laws in Nigeria by providing a critical analysis of the Cybercrime Act of 2015. This analysis delves into the strengths and weaknesses of the Act, shedding light on its effectiveness in combating cybercrime in the country. The study will also help to deepen our understanding of the legal framework for combating cybercrime in the country and sheds light on the effectiveness of the current legislation in addressing cyber threats.

Practically, the findings of this study can be used by policymakers, law enforcement agencies, and other stakeholders to improve the implementation of cybercrime laws and enhance cybersecurity measures in Nigeria. By identifying gaps and areas for improvement in the existing legal framework, this study can help to strengthen the country's defences against cyber threats and protect its citizens from online criminal activities.

1.6 Research Methodology

This study seeks to evaluate the effectiveness of the Cybercrime Act in addressing the growing threat of cybercrime in Nigeria. To do this, this study will adopt a doctrinal approach in analyzing the Cybercrime (Prohibition, Prevention, etc.) Act 2015 in Nigeria. This is because the doctrinal or library-based research is the most popular methodology used by legal researchers. Doctrinal study seeks to determine what the law is in a certain circumstance. It is focused with

the analysis of legal doctrine, including how it was formed and applied.[14] As is generally known, this is completely theoretical research, consisting of either simple research targeted at locating a single declaration of the law or legal analysis with more complicated logic and depth. To Salim, Zuryati and Zainal, it is library-based study that aims to determine the "*one right answer*" to certain legal challenges or questions.[15] Thus, the goal of this methodology is to conduct targeted queries in order to discover specific bits of information. The reason why the doctrinal research method was adopted for this study is because it allows for a comprehensive analysis of the Cybercrime Act 2015 in Nigeria and also allows for a thorough understanding of the legal principles and concepts that underpin the legislation, providing valuable insight into its practical application.

At the other hand, both primary and secondary data will be collected. Primary data will be gathered through the consultation of relevant statutes and case laws. Secondary data, on the other hand, will be collected from various sources such as online sources, academic journals, government reports, and news articles to provide a broader context and support the findings. The research methodology adopted for this study aims to provide a comprehensive and nuanced analysis of the Cybercrime (Prohibition, Prevention, etc.) Act 2015 in Nigeria, with the goal of identifying any gap or area for improvement in the country's legal framework for combating cybercrime.

[14] MD Pradeep, 'Legal Research- Descriptive Analysis on Doctrinal Methodology.' *International Journal of Management, Technology, and Social Sciences (IJMTS)* [2019] (4) (2) 95-103. DOI: http://doi.org/10.5281/zenodo.3564954.
[15] Salim Ibrahim Ali, Zuryati Mohamed Yusoff, and Zainal Amin Ayub, 'Legal Research of Doctrinal and Non-Doctrinal,' *International Journal of Trend in Research and Development* [2017] (4) (1) 493.

1.7 Chapter Analysis

Chapter one of this work started with introduction to the study of cybercrime, providing an overview of the legal frameworks, challenges, and prospects for combating this growing threat in the digital age. The statement of the problem highlighted the increasing prevalence of cybercrime and the need for effective strategies to address it. The aim and objectives of the study outlined the specific goals of the research, while the scope and limitations clarified the boundaries of the study. The significance of the study underscored the importance of understanding and addressing cybercrime in today's interconnected world. The research methodology section detailed the approach and methods used to investigate and analyze cybercrime trends and responses. Chapter analysis provided insights of what to expect in each chapter of the study, guiding the reader through the organization and structure of the research.

The next chapter of this work provides a comprehensive overview of the key concepts related to cybercrime, such as the definition of crime, cybercrime and history and evolution of cybercrime. Additionally, it delves into the theoretical foundations that underpin the study of cybercrime, including the social control theory, asset building theory, identity empowerment theory and positivist theory. The chapter concludes with a detailed review of existing literature on cybercrime, highlighting the current state of research in this field and identifying gaps that this study aims to address.

Chapter three provides an in-depth analysis of the legal frameworks and institutional setup in Nigeria for combating cybercrime. The National Legal Regime highlights the specific laws and regulations in place to address cybercrimes within the country. The Continental and Sub-Regional Legal Regime section explores how Nigeria collaborates with other African countries

to combat cyber threats. The International Legal Regime section discusses Nigeria's role in global efforts to address cybercrimes. The chapter concludes with an examination of the institutional framework in Nigeria dedicated to combating cybercrimes, outlining the key agencies and their roles in this endeavor.

Chapter four goes on to discuss the prohibited offences outlined in the Cybercrimes Act 2015 and the challenges faced in prosecuting cybercrimes in Nigeria. It also compares the legislative frameworks and enforcement mechanisms of selected jurisdictions in preventing cybercrimes. The chapter concludes by emphasizing the need for a paradigm shift in legal approaches and governance, drawing lessons from countries such as the USA, UK, and South Africa. The chapter highlights the importance of updating laws and policies to effectively combat cybercrimes in an increasingly digital world.

The final chapter of the study provides a comprehensive summary of the findings, highlighting the key points discussed throughout the research. Based on the analysis of the data, several recommendations are put forth to improve the effectiveness of Nigeria's Cybercrime Act in combating cybercrime. Additionally, the chapter discusses the contributions of the study to existing knowledge in the field and suggests areas for further research to enhance understanding of cybercrime prevention and prosecution. In conclusion, the study emphasizes the importance of a strong legal framework and collaborative efforts in combating cybercrime in Nigeria.

.

CHAPTER TWO

CONCEPTUAL CLARIFICATIONS, THEORETICAL FOUNDATION AND LITERATURE REVIEW

2.1 Conceptual Clarifications

At this point, we will be looking at the concept of crime, cybercrime and the history and evolution of cybercrime for a better understanding of the concepts.

2.1.1 Conceptualizing Crime

There are numerous responses to the question, "What constitutes a crime?" To a practising lawyer, a crime is anything banned under the criminal law—the criminal law being that area of law dealing with governmental punishment. However, as numerous legal scholars note[16], not all state penalties—civil fines and civil contempt of court, for instance—fall under the purview of the criminal code. The adjectival events of the criminal code, or the ways that criminal and civil proceedings are unique from one another, provide a more accurate litmus test for the extent of the legislation. In short, when something is covered by criminal proceedings, it becomes a criminal restriction. The scope of criminal law can only be defined in adjectival terms since the content of those objects subject to criminal prohibition (crime) varies far too widely[17].

Criminologists offer another perspective on the question, "What is a crime?" They stress how important it is to have a larger social environment. Crimes are not merely legal constructs, such as a negative covenant or a *cestui qua* trust. Rather, there is an important social component to

[16] E.g. G Williams, 'The Definition of Crime'. *Current Legal Problems* [1955] (107) 130; A Simester and G Sullivan, *Criminal Law: Theory and Doctrine* (3rd edn.: Oxford University Press, 2007) 3-4.
[17] See G Williams, above n. 13 and D Ormerod, *Smith and Hogan Criminal Law* (11th edn.: Oxford University Press 2005) Ch. 2, especially 9–10, 16–17. On the procedural aspects of criminal law, see also A Ashworth, 'Is the Criminal Law a Lost Cause?' *LQR* [2000] (116) 225, at 230–232.

criminal law. A defendant found guilty of a crime is not only held accountable for breaking a legal rule following a successful prosecution; rather, she is judged guilty of the charge brought against her. These are terms with social connotations. Hence, in social life, the criminal code plays a crucial condemning role by designating certain behaviours as especially unacceptable, necessitating the mobilisation of the governmental apparatus to combat them[18].

Legal definition of crimes states that crimes are typically described as acts or omissions that are prohibited by law and can be punished by jail and/or fines. Common instances include murder, robbery, burglary, rape, drunk driving, child maltreatment, and failure to pay taxes. However, as some distinguished criminologists[19] have lately stated, the key to understanding crime is to concentrate on the underlying characteristics of all criminal behaviours rather than on specific criminal acts. Instead of attempting to explain individual crimes such as homicide, robbery, rape, burglary, embezzlement, and heroin usage, we must determine what they all have in common. Much previous crime research has been confused by its emphasis on politico-legal rather than behavioural definitions.

The behavioural definition of crime focuses on criminality, which is a specific personality profile that leads to the most serious types of crimes. All criminal behaviours entail the use of force, deception, or stealth to get material or symbolic resources. According to Gottfredson and Hirschi[20], criminality is a type of strategic behaviour characterised by self-centredness, disregard for the pain and needs of others, and a lack of self-control. Criminality is more appealing to

[18] For a recent overview, see L Zedner, *Criminal Justice* (Oxford University Press 2004) Ch. 2; and for doctrinal accounts particularly sensitive to these issues, see A Ashworth, *Principles of Criminal Law* (5th edn.: Oxford University Press 2005), 1–6 and Simester and Sullivan, above n 13 at 1–5.
[19] J Sampson Robert and W Byron Groves, 'Community Structure and Crime: Testing Social-Disorganization Theory'. *American Journal of Sociology* (1989) (94) 774-802.
[20] Hirschi Travis and Gottfredson Michael, 'Age and the Explanation of Crime'. *American Journal of Sociology* [1983] (89) 552-584.

impulsive people because it provides quick gratification through relatively simple tactics. These strategies are often hazardous and thrilling, requiring little expertise or planning. They frequently inflict pain or distress to sufferers and provide little or no long-term advantages since they interfere with professions, families, and connections.

2.1.2 The Concept of Cybercrime

The Cybercrime Act 2015 failed to define "cybercrime," however attempt will be made here to define it. Cybercrime may be described as an act that involves the use of computers, network or electronic information technology devices or the internet to perpetuate criminal activities like illegal access to data,[21] data interference,[22] system interference,[23] computer related fraud and forgery,[24] misuse of devices for crime,[25] illegal interception, intellectual property violations, terrorism and viral attacks. Any crime committed in the cyberspace is a cybercrime; or put in a more succinct way, any crime committed by using computer as a tool for the perpetration of the offence can generally be described as a cybercrime. Such act includes hacking, cracking, stalking, squatting, phishing, identity theft, impersonation, spoofing, software piracy, credit card fraud and viral attacks through the use of computers.[26]

There is no universal definition of cybercrime, mainly because it means different things to different people. It therefore depends on the context in which the term is being used. Cybercrimes evolve as technological developments improve, presenting new opportunities;

---

[21] See *sections 6, 28(3), 5* and *31* of the *Cybercrimes (Prohibition, Prevention etc.) Act 2015*.
[22] *ibid section 16.*
[23] *ibid sections 8 and 16*
[24] *ibid sections 13 and 14.*
[25] *ibid sections 18, 24* and *25*
[26] E Onoja, *Fundamental Principles of Nigerian Criminal Law* (Green World Publishing Company Ltd 2015) 607-608.

hence definitions keep evolving. For instance, David Wall[27] classified cybercrime into four main groups: cyber-trespass, cyber-deception/theft, cyber-pornography and obscenity, and cyber-violence. Wall stated that cyber-trespass involves unauthorized crossing of already established boundaries in cyberspace like software piracy. Cyber-deception/theft, on the other hand, consists of using cyberspace to steal or cause harm. A good example is identity theft using ICTs. Cyber-pornography and obscenity involve cases where sexually explicit materials are traded in cyberspace, example, child internet pornography or abuse. Cyber-violence consists of using cyberspace or ICTs to instigate violence that has an ensuing impact on the people's lives; an example that suffices here is cyber-terrorism. Cyber-violence could be carried out by an individual or a social/political group against others. In the context of Nigeria, the definitions that fit the Nigerian cybercrime mold the best involve cyber-trespass and cyber-deception/theft, because they are the most common types of cybercrimes committed by Nigerian fraudsters. While researchers have not established the prevalence of cyber-pornography and cyber- violence in Nigeria, these areas should nevertheless be addressed through legislation. The prevalent and pervasive growth of terrorism across the world and Nigeria indicates cyberterrorism should be comprehensively addressed in the laws and policies of Nigeria.

Other researchers have also attempted to conceptualize cybercrime in various ways. According to Renu[28], cybercrime refers to a wide variety of criminal activities involving the use of computers and Internet technology. Cybercrime can also be classified in three ways: crimes where a computer is the primary instrument of crime, crimes where a computer is attendant to

[27] DS Wall, 'Cybercrimes and the Internet', In DS Wall (Ed.), *Crime and the Internet* (Routledge 2001) 1-18.
[28] P Renu, 'Impact of cybercrime: Issues and challenges,' *International Journal of Trending Scientific Research and Development* [2019] (3) (3) 1569-1572.

the offense, and crimes where the crime target is a computer[29]. Indeed, McGuire and Dowling[30] classified cybercrime into two types: "cyber-enabled crime" and "cyber-dependent crime". Cyber-enabled crimes are traditional cybercrimes that are facilitated using a computer. This includes credit card fraud, identity theft, mail fraud, and electronic information theft for profit, drug trafficking, voyeuristic activities, stalking, harassment, Internet scams, or other menacing behavior. Cyber-dependent crimes, on the other hand, are crimes that cannot take place without cyber-technology. For example, cybercriminals can use malware to cause extensive damage to databases of companies. They can cripple infrastructural facilities of countries using the ICTs. They can hack computers of individuals and agencies to steal, destroy, or distort information.

Yet still other scholars have postulated various definitions of cybercrime in their desire to establish a common ground. Hassan, Lass and Makinde[31] defined cybercrime as a process that involves the use of computers and the Internet by individuals to commit crimes. It could also reasonably include a wide variety of criminal offenses and activities that can be narrowed down to any illegal actions directed through electronic operations targeting the security of computer systems and the data processed by them.[32]

While no one description or perspective offers a better definitional fit than another, the various classifications demonstrate the difficulty of defining the term. Instead, it is perhaps necessary to focus on a particular perspective that explains cybercrime from a law enforcement perspective, focusing on jurisdiction and response. Therefore, one useful classification of cybercrime for

[29] R Sarre, LYC Lau and LYC Chang, 'Responding to Cybercrime: Current Trends. Police Practice and Research,' *An International Journal* [2018] (19) (6) 515-518.
[30] M McGuire and S Dowling, Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications,' *Home Office Research Report* [2013] 75.
[31] AB Hassan, FD Lass and J Makinde, 'Cybercrime in Nigeria: Causes, Effects and the Way Out,' *ARPN Journal of Science and Technology* [2012] (2) (7) 626-636.
[32] OJ Olayemi, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria,' International Journal of Sociology and Anthropology [2014] (6) (3) 116-125.

criminal justice purposes was provided by Kremling and Sharp-Parker[33].They argued that a definition of cybercrime should be addressed within the context of jurisdiction and the laws that address prevention and responses to the crime. In this light, categorizations and contexts are essential as they allow governments and law enforcement organizations to devise strategies and tactics to protect, prevent, respond, and recover from various types of cybercrime using definitions that are clearly spelt out with consequences for each offense.

2.1.3 The History and Evolution of Cybercrime

The origin of cyber crime is difficult to determine, but it can be traced back to the first major attack on a digital network in 1971. John Draper, a phone phreak, discovered a whistle that produced the same tones as telephone switching computers of the time, leading to increased instances of wire fraud[34]. In 1973, a teller at a local New York bank used a computer to embezzle over $2 million dollars. In 1978, the first electronic bulletin board system came online and quickly became a preferred method of communication for the cyber world[35].

In 1981, Ian Murphy, popularly known as Captain Zap, was the first person convicted of a cyber crime. He was alleged to have hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times. In 1983, the movie War Games released, which depicted a teenage boy who hacks into a government computer system through a back door and nearly

[33] J Kremling and AM Sharp-Parker, *Cyberspace, Cybersecurity and Cybercrime* (Sage 2018).
[34] Vuk Mujovic, 'Evolution of Cybercrime: Where Does Cybercrime Come from? The Origin & Evolution of Cybercrime,' (2018). Available at: <https://www.le-vpn.com/history-cyber-crime-origin-evolution/> accessed on 28 July 2024.
[35] *Ibid*

caused the world to World War III. In 1988, Robert T. Morris released a self-replicating worm that infected more than 600,000 networked computers[36].

The first large-scale case of ransomware was reported in 1989, where the virus held computer data hostage for $500. In 1993, Kevin Paulson was caught and convicted for hacking into the phone systems, taking control of all phone lines going into an LA radio station to guarantee winning a call-in contest. He was eventually caught and sentenced to 5 years in Federal penitentiary and was the first to have a ban on Internet use included in his sentence.

In 1994, the World Wide Web was launched, allowing black hat hackers to move their product info from the old bulletin board systems to their own websites. A student in the UK used the information to hack into Korea's nuclear program, NASA, and other US agencies using only a Commodore Amiga personal computer and a "blue boxing" program found online[37].

In 1996, CIA Director John Deutsch testified to Congress that foreign-based organized crime rings were actively trying to hack US government and corporate networks. The US GAO announced that its files had been attacked by hackers at least 650,000 times, with at least 60% of them being successful. In 1999, the Melissa Virus was released, becoming the most virulent computer infection to date and resulting in one of the first convictions for someone writing malware.[38]

Cyber crime began to take off in the early 2000s when social media came to life, creating a flood of personal information and the rise of ID theft. The number and types of online attacks increase

---

[36] *Ibid*
[37] Moga Ezekiel, Salihu Abdullahi Galle and Abdulkarim Rukayyat, '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.
[38] *Ibid*

exponentially, with the latest wave establishing a global criminal industry totaling nearly a half-trillion dollars annually. Those involved in this act are popularly known as 'Yahoo boys.' I assume this name was created out of the fact that yahoo was the first trending email platform in the early 2000s. Due to how expensive getting a laptop or a desktop computer was, most cybercrimes in the early time were performed in the cybercafe. Government on its part made use of Nigeria police force as an agent expected to solve this problem by arresting anyone found guilty of being a 'yahoo boy'.[39] However, despite the efforts of law enforcement, the 'Yahoo boys' have continued to adapt and evolve their methods, making it difficult to track and apprehend them. As technology has advanced, so too have their tactics, allowing them to operate on a global scale with relative ease.

2.2 Theoretical Foundation

To Grant and Osanloo, the theoretical framework is the 'blueprint' or guide for research.[40] It is a framework based on an existing theory in a field of inquiry that is related to and/or reflects the hypothesis of a study. In line with that, we will at this point review the relevant theories applicable to the present research and discuss how they will inform our study.

2.2.1 The Social Control Theory

The Social Control Theory, by Travis Hirschi in 1969, without the influence of positive, social control institutions such as mosques, churches, schools, family and workplaces, many people would ordinarily want to commit cybercrimes. Tania posited that children and youths should be

[39] (PDF) Cybercrime in Nigeria: Evolution and Forms. Available at <https://www.researchgate.net/publication/368757425_Cybercrime_in_Nigeria_Evolution_and_Forms> accessed 7 Jul 2024.

[40] C Grant and A Osanloo, 'Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for 'House'', *Administrative Issues Journal: Connecting Education, Practice and Research* [2014] 12-22. DOI: 10.5929/2014.4.2.9

given a substitution to a life of crime which is important to social control theory.[41] The Federal Government, the National Assembly and other policymakers should promote political, social and economic stability so that the people would not be pressurised into cybercrime in Nigeria due to unemployment, poverty, weak institutions, and negative peer influence are among which are the causes of cybercrime in Nigeria.[42] Desperate and vulnerable individuals are victims of cybercriminals antics.[43]

The implicit idea of the theory posits that individuals are more likely to engage in criminal behaviour when they feel disconnected from society and its norms. In the context of cybercrime, this theory suggests that individuals who lack strong social bonds and relationships may be more inclined to participate in illegal online activities. By analyzing the Cybercrime (Prohibition, Prevention, etc.) Act 2015 through the lens of the Social Control Theory, we can better understand how the legal framework in Nigeria addresses the root causes of cybercrime and aims to deter individuals from engaging in such activities through effective prevention and punishment measures.

2.2.2 Asset Building Theory

The proponents of this theory assert that one of the reasons individuals engage in criminal behaviour is due to a lack of resources, and by providing them with legitimate ways to build assets, it can deter them from turning to illegal activities. By promoting financial literacy, entrepreneurship, and access to economic opportunities, individuals are given the chance to improve their financial situations legally. This theory suggests that by addressing the root causes

---

[41] U Tania, *Criminology Theories: The Varied Reasons Why People Commit Crime*. Available at: <www.blog.udemy.com> accessed August 12, 2024.
[42] JO Aransiola and SO Asindemade, 'Understanding Cybercrime Perpetrators and the Strategic they Employed in Nigeria,' *Cyberpsychology, Behaviour and Social Networking* [2011] (14) (12) 759-763.
[43] *Ibid*

of criminal behaviour, such as poverty and a lack of resources, society can effectively combat cybercrime and other criminal activities. Also, by creating a legal framework that supports asset building and economic empowerment, countries like Nigeria can reduce the prevalence of cybercrime and promote a safer online environment for their citizens.

This theory evolved as from policymakers who were specifically interested in exploring asset accumulation strategies to reduce poverty which is the major course of criminal activities[44]. The rationale for building assets through mechanisms other than income support stems in part from what Sen[45] identifies as strengthening human and economic capabilities[46]. Asset-building policy was developed to influence and improve many aspects of individual and household welfare including knowledge, resources, and functioning skills[47].

The asset-building paradigm, commonly referred to as capacity building, can be scrutinized through a multifaceted lens. A pivotal dimension of this approach is rooted in the notion of human assets or capital, which encompasses the intangible resources and capabilities that individuals possess. According to Becker[48], human capital is the range of personal assets and resources belonging to an individual, such as skills, education, and intellectual ability, that influence future financial and psychological outcomes. He posits that human capital constitutes a staggering 75 percent of total wealth, underscoring its paramount importance in the global economy. Consequently, cybercriminals seek to illicitly acquire valuable assets by engaging in various forms of cyber malfeasance, including identity theft, phishing scams, and hacking. These

[44] M Sherraden, J Curley and M Grinstein-Weiss, *Wealth Creation and Rural America* (National Rural Funders Collaborative 2003) 34.
[45] A Sen, *Commodities and Capabilities* (North-Holland Publishing Company, 1985) 56.
[46] A Sen, 'Capability and Well-being,' in M Nussbaum and A Sen (eds.), *The Quality of Life* (Clarendon Press 1993) 30-53.
[47] *Ibid*, at note 10
[48] G Becker, *Human Capital* (Bureau of Economic Research 1964) 47.

illegal activities allow them to gain access to valuable personal information and financial resources, which they can then use for their own benefit. As technology continues to advance, the threat of cybercrime becomes more prevalent, making it crucial for individuals and organizations to invest in cybersecurity measures to protect their assets from being compromised. At the other hand, also, cybercriminals who possess high levels of human capital may be more successful in carrying out their illegal activities, as they have the skills and knowledge necessary to navigate the complexities of the digital world. This underscores the importance of investing in education and training to build human capital and prevent cybercrime.

Another dimension of capacity building is the growth of tangible and financial capital. Sherraden[49], whose work has been instrumental in advancing this concept, proposes that building financial assets has far reaching effects on the current well-being of individuals, in addition to the well-being of future generations[50]. Thus, building financial assets is the main reason for cybercrime. Furthermore, the acquisition of financial assets can lead to economic stability and security for individuals and their families. By accumulating wealth through legitimate means, individuals are less likely to resort to criminal activities such as cybercrime in order to meet their financial needs. In this way, the promotion of asset building can serve as a preventative measure against cybercrime, as individuals have less incentive to engage in illegal activities when their financial needs are met through lawful means. Ultimately, the emphasis on building financial assets can contribute to a reduction in cybercrime rates and promote a more secure and stable society.

[49] M Sherraden, 'Rethinking Social Welfare: Toward Assets,' *Social Policy* [1988] (18) (3) 37-43.
[50] M Sherraden, *Assets and the Poor: A New American Welfare Policy* (ME Sharpe 1991) 86.

2.2.3 Identity Empowerment Theory

The theory suggests that individuals who feel empowered by their identity are less likely to engage in criminal behaviour. This is because they have a strong sense of self-worth and are less likely to seek validation through illegal activities.

The theory in question was initially posited by Hall, who served as its primary proponent and laid the foundational groundwork for its development.[51] The theory explained and described critical and social processes that increase the probabilities and possibilities of peoples' wellbeing and optimal functioning. The theory assumed that empowered individuals with well known identity make meaningful commitments and undertake effective goal oriented activities they choose for themselves, rather than resorting to crimes. The theory posited that people's behaviour and quality of life and general society can be changed by increasing their awareness of the strength of social influences within the environment. The theory asserted that all people can make some constructive change to enhance and improve their situations by taking control of their own identities and asserting themselves in a positive way. This theory emphasizes the importance of individuals recognizing their own power and agency in creating positive change, rather than relying solely on external forces. By understanding and embracing their own identities, individuals can work towards empowering themselves and others to combat cybercrime and other challenges in Nigerian society. Based on this theory, people's collective empowerment, which results from their awareness and actions in relation to themselves and the community, manifests in the form of self help projects, which include cybercrime.

[51] HW Hall, *Neighborhoods: Their Place in Urban Life* (Sage Publication 1990).

In the context of cybercrime, the Identity Empowerment Theory suggests that individuals who are aware of the risks and consequences of cybercrime are more likely to take preventive measures and report suspicious activities. This theory highlights the importance of education and awareness in combating cybercrime, as well as the role of individuals in protecting themselves and their communities from online threats. By understanding and embracing their digital identities, people can become empowered to take control of their online safety and security.

2.2.4 Positivist Theory or Legal Positivism

Positivism arises as a new concept for understanding many scientific difficulties and serves as a framework for human thought in all aspects of existence. Initially, positivism as a school was developed by Auguste Comte, a French social philosopher. Neff while restating the position of Comte, stated that human mind passes through numerous theological, philosophical, and positive stages[52]. Protevi, also upheld this view by going further to state that, according to Comte, positivism believes that what is true or accurate is only a positive or actual field of knowledge, specifically when the scientific method is used in that field of expertise[53]. Positivism is a novel element of epistemic logic that emphasises science as a determining factor in establishing validity.

Auguste Comte expounded that during the theological stage, ideas—ideas that originate from God and are not perceived by the senses—dominately impact human cognition. At the metaphysical level, natural rules are the source of human thought. During the positive phase, concepts derived from something beyond the reach of the senses have started to give way and are

[52] C Neff and A Sthepenn, 'Short History of International Law, in D dalam Malcolm Evan ', *International Law* (1st Edn. Oxford University Press 2003).
[53] Protevi John, *The Edinburgh Dictionary of Continental Philosophy* (Edin-burgh University Press 2005).

grounded in verifiable facts. The goal of juridical positivism is to portray the legal system as merely an empirical fact, a sensuous fact[54]. This line of reasoning leads to legal issues that are restricted to empirical data. The law is reduced to a single item that is only perceptible to the senses. This way of thinking thus solidifies the notion of a set of norms that are factually established by the appropriate authority and that are subject to enforcement. As a result, this theory concentrates on the legal ramifications of the official state regulations.

Austin also assumes that the legal system is real and applicable, not because it has a factual basis in social life, or because the law exists in society, or even because the law is not a mirror problem of justice and morals, but because it has a positive shape from the appropriate institution. The legal justification is based on formal-legalism, both as a kind of ruler's command, as Austin proposed, and as the derivation of grundnorm, which is at the heart of Kelsen's teaching. The most fundamental aspect of this legal positivist theory is that it examines the law in terms of its juridical form rather than its material content[55]. John Austin was a significant follower of positivism in the history of thought, particularly his analytical legal positivism. It starts with the basic premise that there is a power that gives orders.

[54] David Plunkett, 'Robust Normativity, Morality, and Legal Positivism' in David Plunkett, Scott Shapiro & Kevin Toh (eds), *Dimensions of Normativity: New Essays on Metaethics and General Jurisprudence* (Oxford University Press 2019).

[55] See Tom Campbell, *Prescriptive Legal Positivism: Law, Rights and Democracy* (Cavendish Publishing 2004) on "Prescriptive" Legal Positivism, according on which "Legal Positivism" is a normative view about what law ought to be. We set this aside, along with descriptive formulations of positivism that are (at least partly) epistemological instead of purely metaphysical. For discussion and references for such formulations, see Samuele Chilovi & Daniel Wodak, 'On the (in) significance of Hume's Law', *Philosophical Studies* (2021).

However, to Friedmann and Wolfgang[56], Austin asserts that in order for something to be deemed a law, it must contain certain characteristics, such as belief, the existence of sovereign authority, an order, the requirement to obey duties, and penalties for flagrant violators.

The goal of positivism is to disprove the doctrine of natural law. Rather than moral assertions, positivism is a doctrine founded on social realities[57]. The tenet of positivism is that laws are only valid when they are based on social truths, which are established or declared explicitly by people in positions of power—in this example, the governor, judges, lawmakers, and others. Furthermore, positivism makes it clear that morality and the law are two distinct domains[58]. There are various theoretical aspects to consider while understanding legal positivism, which is a current that carries empirical legal theories. These theories include Kelsen's pure theory, pragmatic positivism, analytical jurisprudence, and analytical legal positivism.

Applying Positivist theory to the fight against cybercrime in Nigeria reveals the critical role of effective legislation and institutions in protecting citizens from online harm. This is because when individuals perceive cybercrime as a low-risk, high-reward endeavor, they're more likely to engage in malicious activities. Factors driving this behavior include economic desperation, social pressure, and psychological thrill-seeking. In Nigeria, where cybercrime affects countless lives, understanding these motivations behind cybercrime is crucial. The Cybercrime (Prohibition, Prevention, etc.) Act 2015 serves as a vital legal instrument, outlining offenses and penalties to deter potential perpetrators. However, truly combating cybercrime requires more than legislation alone. It demands a comprehensive approach, addressing socio-economic factors like poverty

[56] Friedmann Wolfgang, *Legal Theory* (Stevens & Son Limited 1953) L dalam Bernard Tanya dkk, Teori Hukum: Strategi Tertib Manusia dalam Lintas Ruang dan Generasi (Genta Publishing 2013).
[57] *Ibid.*
[58] *Ibid.*

and unemployment, which drive individuals to cybercrime. It requires empowering citizens through education and awareness, fostering a culture of cybersecurity and responsibility. Effective law enforcement, international cooperation, and institutional capacity-building are also essential.

By examining cybercrime through a Positivist lens, we will come to the comprehension of the complex interplay that inherently occurs between the legal norms, the institutional frameworks, and the diverse human behaviors in a given society. This understanding is needed as it informs evidence-based policies, ensuring a safer online environment for Nigerians and contributing to global efforts to mitigate cybercrime threats.

2.3 Literature Review

Numerous scholars have carried out researches on topics related to this present study. Below are the reviews of some of the related literatures:

The work of Abayomi is worthy of review as it is relevant to this present study. His research was on "Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement."[59] According to him, Nigeria has experienced a significant surge in cybercrime over the past decade, attributed to the transformative impact of the digital revolution and the country's robust economic growth. He argued that the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, was timely, given the inadequacies of traditional criminal laws in addressing cybercrimes, which target intangible assets such as information and technology. His paper critically examined Nigeria's legal framework for combating cybercrimes and identified various

[59] B Abayomi Sogunle 'Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement', *Journal of Law and Judicial System* [2021] (4) (1) 1-11. DOI: <https://doi.org/10.22259/2637-5893.0401001> accessed on 12 September, 2024.

challenges. While his work offered suggestions for a more structured approach to combating cybercrime, it lacked concrete examples of successful implementation in other countries, potentially limiting the practicality of his recommendations. This study aims to address this gap by conducting a comparative analysis of cybercrime laws and their enforcement in different jurisdictions, providing empirical evidence to inform effective strategies for combating cybercrimes in Nigeria.

Aamo Iorliam underscored "Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime,"[60] where he explored the use of digital surveillance to identify and analyze fraud in Nigeria's cyberinfrastructures. It was found that Nigeria's porous cyberspace enabled 3,500 cyberattacks in 2017, resulting in $450 million losses, which compromised the digital economy, trust in online commerce, and military intelligence. The Nigerian Army's Cyber Warfare Command was established in 2018 to combat terrorism and banditry, but digital surveillance tools are needed to detect and prevent cyber-enabled crimes. The book discusses network traffic analysis, mobile forensic tools, and digital surveillance software, highlighting its benefits in combating internet-aided crimes. However, it fails to critically examine the Cybercrime Act 2015, neglecting to ensure the legal and ethical use of digital surveillance tools. This research fills this gap by examining the intersection of digital surveillance software and existing cybercrime laws in Nigeria, exploring challenges and opportunities for law enforcement agencies.[61]

[60] Iorliam Aamo, *Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime* (Springer International Publishing 2019) 1-55.
[61] *Ibid*

Clough, in his book "Principles of Cybercrime,"[62] stated that digital technology has revolutionised the way we socialise and conduct business. A nuanced exploration of the symbiotic relationship between technological advancements and cybercrime reveals that innovative opportunities for legitimate users are often mirrored by illicit exploits. As criminals leverage new technologies for fraudulent activities, child pornography, stalking, copyright infringement, and computer attacks, the imperative for dynamic legal frameworks becomes increasingly evident. Clough's treatise on cybercrime prosecution in select Anglo-American jurisdictions offers a valuable foundation, yet its scope is limited by the omission of comparative analyses from diverse legal traditions. This research endeavors to bridge this knowledge gap by undertaking a cross-jurisdictional examination of cybercrime prosecution, thereby illuminating the complexities and opportunities inherent in developing a globally effective response to cybercrime.

The research work of Kesiena URHIBO “Combating and Addressing the Menace of Cybercrime in Nigeria: An Overview of Applicable Laws”[63] is also relevant to this present study. To him, in Nigeria, technological advancements in data processing, information communication technology, and the internet pervade all aspects of human activity. It has also created an environment in which social outcasts can commit cybercrime and fraud against online users. The finding in his work is that the rise of cybercrime in Nigeria has been aided by the fact that it requires little to no resources to begin with and can be carried out in a variety of locales with no geographical restrictions. This has sparked heated debate over whether Nigeria has enough laws in place to investigate and prosecute cybercriminals effectively and quickly. To that aim, his paper

[62] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2015) 3-486.
[63] Kesiena URHIBO ‘Combating and Addressing the Menace of Cybercrime In Nigeria: An Overview of Applicable Laws’, *African Journal of Criminal Law and Jurisprudence (AFJCLJ)* [2021] (6) (1) 109-124

advocates for the enactment of successful legislation to eliminate or limit cybercrime in Nigeria to an absolute minimum. A gap in the literature regarding cybercrime in Nigeria has also been identified, as most studies focus on the prevalence of cybercrime rather than the effectiveness of current laws and regulations in combating it. This gap leaves room for further research to explore the potential impact of stronger legislation on reducing cybercrime rates in the country. It is this gap that informed the present study.

In their research work, "Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations."[64] Izevbuwa and Rita posited that the advent of the internet, computers, and mobile phones has transformed various aspects of life, including transactions and personal correspondence, but also exacerbated harm, crime frequency, and illegal activities. They highlighted the emergence of cybercrimes as a significant threat to national security, necessitating robust legislation and procedural measures to combat them. In Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, was enacted to investigate and prosecute cybercriminals. Their study employed doctrinal methodology to analyze the Act's key provisions and ancillary legislation, assessing their effectiveness and offering solutions to combat cybercrime. However, their work lacked in-depth analysis of implementation challenges and capacity building for law enforcement agencies. This present research addresses these gaps, providing a more comprehensive approach to combating cybercrime in Nigeria.

[64] Izevbuwa Osaretin George and Rita Abhavan Ngwoke 'Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations', *Journal of Law, Policy and Globalization* [2022] (119) 1-17. DOI: 10.7176/JLPG/119-01.

Olanrewaju and Abraham underscored 'A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria,'[65] and stated that the digital age has introduced new ways to commit crimes, necessitating the development of strategies to combat digital or cybercrime. Their discovery revealed that in Nigeria, there has been a significant increase in internet-based advance fee fraud, hacking into emails and websites, and infringements on privacy rights. Going further, they posited that the Cybercrimes (Prohibition and Prevention, etc.) Act, 2015, was introduced as a first step to combat cybercrime, but it is insufficient to address the complexities of technological progress. The Act aims to provide Nigerian authorities with a cohesive legal, regulatory, and institutional framework for outlawing, prevention, detection, prosecution, and punishment of cybercrimes. The findings show that the Act has certain gaps, particularly in its scope for protecting Critical National Information Infrastructure and failing to provide a comprehensive framework. Their proposal suggests amending the Act to include non-Critical National Information Infrastructure regions. The lacuna in their work ranges from the fact that they failed to address the issue of international cooperation in combating cybercrimes to the lack of specific penalties for offenders. Additionally, their proposal does not provide a clear plan for monitoring and enforcing the amended Act once it is implemented. This present research will examine these lacunae with a view to filling them.

More to the above, Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi wrote on "Cybercrime, Digital Forensics and Jurisdiction,"[66] and stated that the objective of law is to protect society from harm by defining what conduct is unlawful and prescribing the

[65] Olanrewaju Adesola Onadeko and Abraham Femi Afolayan 'A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria' *A Paper Presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL)* at Halifax, Nova Scotia, Canada [2016] 1-11.
[66] M Chawki, A Darwish, MA Khan and S Tyagi, *Cybercrime, Digital Forensics and Jurisdiction* (Springer International Publishing 2015) 1-145.

punishment for such behaviour. The internet's ubiquity and anonymity have created a virtual landscape where the rule of law is often challenged, and chaos prevails. The increasing recognition of intangible materials' economic value has led to cybercrime being viewed as a valuable asset. The interdisciplinary fields of Cybercrime, Digital Forensics, and Jurisdiction collectively enhance understanding and mitigation of cyber threats, empowering stakeholders to combat cybercrime and foster a secure digital environment. However, their work overlooks the ethical implications of digital forensics and the challenges of maintaining privacy and civil liberties. Furthermore, the role of international cooperation and information sharing in combating cybercrime across borders warrants further exploration. This research aims to address these gaps by examining the institutional and legal frameworks for combating cybercrime in Nigeria, analyzing the effectiveness of current legislation, and assessing its impact on cyber threat mitigation.

Hu, Chen, and Bose in their paper, "Cybercrime Enforcement Around the Globe,"[67] compares law enforcement approaches to cybercrime in several nations, including the United States, the United Kingdom, Australia, China, and Europe. The researchers conducted a comprehensive analysis of cybercrime incidents reported in various countries, focusing on illicit activities such as credit card fraud, social networking crimes, internet child pornography, and juvenile delinquency. Their examination of global punishment disparities revealed that European countries and the United States tend to impose harsher penalties, whereas China adopts a more lenient approach for the first three types of offenses. Notably, all countries exhibit lenient penalties for youthful delinquency. However, their study overlooks the underlying causes of

[67] Y Hu, X Chen and I Bose, 'Cybercrime Enforcement Around the Globe,' *Journal of Information Privacy and Security* [2013] (9) (3) 34–52. Available at: <https://doi.org/10.1080/15536548.2013.10845684> accessed on 2 October 2024.

these criminal activities and fails to offer preventive solutions, leaving a gap in understanding the complexities of cybercrime. This present study seeks to address this knowledge gap by exploring the root causes of cybercrime and potential preventive measures.

Henry Osborn Quarshie underscored "Cyber Crime in a World without Borders,"[68] and stated that a world controlled by computers and computer networks has been made possible by technology. He views the contemporary world as a dynamic, machine-driven landscape. This borderless realm, created by humans, is known as cyberspace - a virtual universe facilitated by computer networks. He notes that cybercrime in this globalized environment eliminates the need for physical presence at the crime scene. However, his work overlooks the full extent of cyber threats and regulatory mechanisms. This study will examine the various types of cybercrimes in the online world, as outlined in the Cybercrime (Prohibition, Prevention, etc.) Act 2015, and address the regulatory gaps in this domain.

Oluwatomi Ajayi's work on "Internet Technologies and Cybersecurity Law in Nigeria"[69] is relevant to this present study. This seminal work provides a comprehensive examination of the Nigerian context of cybercrimes, cybersecurity threats, and responses, underscoring the vulnerabilities of personal information in the digital age. The author astutely emphasizes the paramount importance of cybersecurity as technology increasingly permeates every aspect of human existence, introducing unprecedented opportunities and novel threats. However, his work leaves a notable gap in the analysis of the ethical implications of cybersecurity practices and policies in today's interconnected world. This study aims to address this lacuna by conducting a critical investigation of the ethical dilemmas faced by individuals, organizations, and

[68] Henry Osborn Quarshie 'Cyber Crime in a World without Borders', *Texila International Journal of Academic Research* [2017] (4) (2) 1-7. DOI: 10.21522/TIJAR.2014.04.02.Art007
[69] A Oluwatomi Ajayi, *Internet Technologies and Cybersecurity Law in Nigeria* (Malthouse Press 2024) 7-344.

governments in the digital era, thereby providing a nuanced understanding of the complex issues at play.

Felix and Mark in their work on "Handbook on Nigerian Cybercrime Law,"[70] stated that given its emerging nature and potential to challenge law enforcement, understanding cybercrime is crucial. To them, in Nigeria, law enforcement agencies and the Ministry of Justice at both federal and state levels are establishing dedicated units to address cybercrime. Educational institutions are also incorporating cybercrime into their curricula to raise awareness. Their book provides an introductory examination of the relationship between law and cybercrime from a Nigerian perspective, offering a foundational understanding of the concept and its implications for legal frameworks and enforcement strategies. The potential gap in this study is the lack of in-depth analysis of specific cybercrime cases in Nigeria and how they were handled by the legal system. By providing case studies and real-life examples, readers would be able to better understand the challenges and successes faced in combating cybercrime in the country. This present study aims to address this gap by delving deeper into the practical application of laws and enforcement mechanisms in response to cybercrime incidents in Nigeria.

"Cybercrime: Key Issues and Debates" by Alisdair Gillespie[71] provides a comprehensive examination of cybercrime, exploring its conceptualization, historical development, and jurisdictional implications through a multidisciplinary approach combining legal, criminological, and sociological perspectives. Gillespie's findings highlight cybercrime's rapid evolution, jurisdictional challenges, inadequate international cooperation, and growing concerns about online privacy and human rights, leading to recommendations for improved international

[70] E Felix Eboibi and K Mark Amakoromo, *Handbook on Nigerian Cybercrime Law* (Justice Jeco Printing and Publishing Global 2018).
[71] A Alisdair Gillespie, Cybercrime: Key Issues and Debates (Routledge 2016)

cooperation, harmonized laws, public awareness campaigns, cybersecurity investments, and balanced security measures. Gillespie's work serves as a foundation for further research, policy development, and practical applications, but leaves room for exploration of country-specific cybercrime legislation and effectiveness. This gap is addressed by this present research, "An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act 2015," which examines Nigeria's cybercrime framework, assesses its effectiveness, identifies challenges, and provides recommendations. This present study fills a significant geographical gap in the literature, evaluating cybercrime governance in a developing country and informing policy decisions and legislative reforms.

CHAPTER THREE

LEGAL REGIME AND INSTITUTIONAL FRAMEWORK FOR COMBATING CYBERCRIME IN NIGERIA

3.1 National Legal Regime

This section will provide an overview of the legal regime in Nigeria that addresses cybercrime.

3.1.1 Cybercrimes (Prohibition, Prevention, Etc) Act 2015

Prior to 2015, Nigeria's legal framework was devoid of specific legislation tailored to combat cybercrimes, leaving a significant void in the country's ability to effectively address and prosecute online offenses.[72] The existing legal framework, comprising the Criminal Code,[73] Penal Code,[74] and the Advance Fee Fraud Act, was utilized to address cybercrime-related offenses. However, these laws were criticized for their inadequacy in explicitly defining cybercrimes, resulting in the police treating cybercriminals as ordinary fraudsters due to the absence of a tailored legal regime and jurisprudential foundation. The necessity for more robust legislation was emphasized in 2014 by the Office of the National Security Adviser, culminating in the enactment of the Cybercrime (Prohibition, Prevention) Act in May 2015.[75]

---

[72] KG Akintola, RO Akinyede and CO Agbonifo, Appraising Nigeria Readiness for Electronic Commerce Towards Achieving Vision 20:2020, *International Journal of Research and Review in Soft and Intelligent Computing* [2020] (9) (2) 331-340.

[73] The Nigerian Criminal Code Act CAP C 39 Laws of the Federal Republic of Nigeria 2004 never envisaged cybercrime as a special and specific crime. Section 419 criminalizes the conduct whereby a person by any pretence 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.

[74] Penal Code (Northern States) Federal Provisions Act, Cap P.3 Laws of the Federation of Nigeria 2004.

[75] The Act came into force on May 15, 2015, after the Presidential Assent in March 2015. It establishes the legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and related crimes.

The Cybercrime (Prohibition, Prevention) Act constitutes Nigeria's inaugural comprehensive legal and regulatory framework, enacted to govern online conduct and prohibit cybercrime.[76] Its punitive nature is a response to the escalating cybercrime threat in Nigeria, which has reached alarming proportions. Consequently, the Act establishes a unified, efficient, and robust legal, administrative, and regulatory system in Nigeria, facilitating the prevention, investigation, detection, prosecution, and punishment of cybercrime and related offenses[77]. Notably, the Act provides a foundational framework for cybersecurity, enhancing the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights, and the preservation and safeguarding of critical national information infrastructure[78]. The objectives stipulated in *Section 1* of the Act are congruent with those outlined in the Act's explanatory memorandum. Furthermore, *Section 2* of the Act explicitly states that 'the provisions of this Act shall apply throughout the Federal Republic of Nigeria.' This provision effectively preempts the 36 State Houses of Assembly from legitimately enacting cybercrime legislation in their respective states, as the Federal Legislative arm has already exercised its authority in this domain. This constitutional arrangement appears to have reinforced the doctrine of covering the field, as enshrined in *Section 4(5)* of the Nigerian Constitution 1999 (as amended). This doctrine dictates that in the event of a conflict between a state law and a federal law, the latter shall take precedence, rendering the former void to the extent of its inconsistency[79].

[76] FE Eboibi, 'A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015 (which was forthcoming in 2017) Computer Law and Security Review: *The International Journal of Technology Law & Practice* on a detailed review of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act 2015.
[77] See the explanatory memorandum of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015.
[78] *Section 1 Ibid.*
[79] *Section 4(5) of the Constitution of the Federal Republic of Nigeria 1999 (as amended).*

The Cybercrime (Prohibition, Prevention) Act is systematically structured into 59 Sections, 8 Parts, and 2 Schedules, facilitating a comprehensive and nuanced approach to cybercrime regulation. The Act's organizational framework is delineated as follows: *Part I* comprises *sections 1 and 2*, which delineate the object and application of the Act, thereby establishing its foundational scope and jurisdiction. *Part II*, spanning *sections 3 and 4*, specifically addresses the protection of critical national information infrastructure, underscoring the Act's emphasis on safeguarding vital national assets. *Part III of the Cybercrime (Prohibition, Prevention) Act* presents a comprehensive framework for addressing an array of cybercrime-related offences and penalties.[80] This section meticulously delineates a range of illicit activities, including offences against critical national information infrastructure,[81] unlawful access to a computer,[82] and registration of cybercafé,[83] as well as system interference[84] and interception of electronic messages, e-mails, and electronic money transfers.[85] Furthermore, it encompasses tampering with critical infrastructure,[86] willful misdirection of electronic messages,[87] unlawful interceptions,[88] computer-related forgery,[89] computer-related fraud,[90] theft of electronic devices,[91] network data and system interference,[92] and cyber terrorism.[93] Notably, this section also addresses fraudulent issuance of e-instructions,[94] identity theft and impersonation,[95] child

[80] See the explanatory memorandum of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015
[81] *Section 5 of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.*
[82] *Section 6 Ibid.*
[83] *Section 7 Ibid.*
[84] *Section 8 Ibid.*
[85] *Section 9 Ibid.*
[86] *Section 10 Ibid.*
[87] *Section 11 Ibid.*
[88] *Section 12 Ibid.*
[89] *Section 13 Ibid.*
[90] *Section 14 Ibid.*
[91] *Section 15 Ibid.*
[92] *Section 16 Ibid.*
[93] *Section 18 Ibid.*
[94] *Section 20 Ibid.*
[95] *Section 22 Ibid.*

pornography and related offences,[96] cyberstalking,[97] cybersquatting,[98] racist and xenophobic offences,[99] importation and fabrication of e-tools,[100] manipulation of ATM/POS terminals,[101] and dealing in card of another,[102] all of which are codified in *sections 5 to 36* of the Act. The subsequent parts of the Act delineate specific responsibilities and procedures. *Part IV (sections 37-40)* outlines the duties of financial institutions and service providers, establishing clear guidelines for their roles in preventing and reporting cybercrime. *Part V (sections 41-44)* focuses on administration and enforcement, detailing the mechanisms for implementing the Act's provisions. *Part VI (sections 45-49)* addresses the critical processes of arrest, search, seizure, and prosecution, providing a framework for effective law enforcement. *Part VII (sections 50-56)* encompasses jurisdiction and international cooperation, facilitating collaborative efforts to combat cybercrime across borders. *Part VIII (sections 57-59)* addresses miscellaneous issues, including regulations, interpretation, and citation, ensuring clarity and consistency in the Act's application. Additionally, the First Schedule lists the members of the Cybercrime Advisory Council, while the Second Schedule identifies businesses subject to levies for the National Cyber Security Fund, as stipulated in *section 44(2)(a)* of the Act.[103]

3.1.2 The 1999 Constitution of the Federal Republic of Nigeria (As Amended)

The Act incorporates vital provisions safeguarding privacy rights, protecting both private individuals and public officials from cybercrime, including illicit computer hacking and online

[96] *Section 23 Ibid.*
[97] *Section 24 Ibid.*
[98] *Section 25 Ibid*
[99] *Section 26 Ibid.*
[100] *Section 28 Ibid.*
[101] *Section 30 Ibid.*
[102] *Section 34 Ibid.*
[103] See Ikenga KE Oraegbunam and E Boniface Ewulum, 'Assessing the Nigerian Cyber-Security Law and Policy for Protection of Critical Infrastructure for National Development' in GN Okeke et al. (eds) *Law, Security and National Development* (Amaka Dreams Ltd. 2017) 62-87.

harassment. The *Nigerian Constitution of 1999 (as amended)* further reinforces these protections, guaranteeing and securing the right to privacy, telephone communications, and related rights.[104] Consequently, when law enforcement agencies seek to access information from an individual's cell phone, email, or other electronic devices in the course of a telecom service provider's cybercrime investigation, the Constitutional right to privacy must be duly considered. Moreover, the Act and its provisions should be interpreted and applied in conjunction with the Nigerian Constitution, ensuring a harmonious and rights-respecting approach to cybercrime regulation. The Constitution serves as a crucial check on the application of its provisions, necessitating caution in Nigeria when balancing the defense of fundamental human rights and internet use. Although *section 45(1)(b)* of the Nigerian Constitution appears to safeguard the rights and freedoms of others, the Supreme Court's ruling in *Rasome Kuti v. Attorney General of the Federation*[105] clarifies that this section does not apply in all cases. As astutely noted by Justice Kayode Esho JSC, 'Fundamental Rights are superior to ordinary laws and precede the political society itself. They are essential conditions for a civilized existence...' This landmark decision underscores the primacy of fundamental rights in Nigeria's legal framework, emphasizing the need for careful consideration in their application, particularly in the context of internet use and cybercrime regulation

The Nigerian Constitution has significant implications for protecting individuals from unwarranted searches and seizures by law enforcement agencies. It mandates that officers obtain a search warrant before accessing areas where individuals have a reasonable expectation of privacy, including computers, records, and personal information stored on devices. The Constitution safeguards individuals' privacy rights regarding their devices, but these rights are

[104] *Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).*
[105] (1985) LPELR – SC.123/1984.

limited to property they own, possess, or manage. A search warrant must be meticulously detailed, specifying the area to be searched and the objects to be seized, thereby restricting the investigation to suspected illegal activity. Notably, exceptions to the explicit procedures outlined in sections 39 and 45 of the Act are not permissible, ensuring that the protection of individual rights remains paramount.

3.1.3 Economic and Financial Crimes Commission (EFCC) (Establishment) Act, 2004

The Economic and Financial Crimes Commission (EFCC) was established by the EFCC Act of 2002, with the primary objective of combating economic and financial crimes in Nigeria. Following the repeal of the initial Act, the *EFCC (Establishment) Act of 2004* was enacted, conferring upon the Commission special powers to investigate individuals, companies, or organizations suspected of committing economic or financial crimes, in contravention of the Act or other statutes.[106] Notably, *Section 7(2) of the EFCC (Establishment) Act, 2004*, empowers the Commission to coordinate and implement provisions of other enabling legislative frameworks, thereby playing a pivotal role in addressing the challenges of cybercrime in Nigeria. This mandate underscores the EFCC's critical function in combating financial and economic crimes, including those perpetrated through cyber means.

It is reasonable to infer from the above paragraph that the EFCC (Establishment) Act 2004, in conjunction with the Advance Fee Fraud and Other Fraud Related Offences Act 2006, vests the EFCC with the authority to investigate and prosecute individuals suspected of perpetrating cybercrimes in Nigeria, including internet and online advance fee fraud. A notable illustration of

[106] *Section 7* of the Economic and Financial Crimes Commission (EFCC) (Establishment) Act, 2004.

this mandate is the case of *Harrison Odiawa v. Federal Republic of Nigeria*,[107] wherein the EFCC charged the defendant with 58 counts of offences, including conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering, and possession of documents containing false pretences, all contrary to the Advance Fee Fraud and Other Fraud Related Offences Act. This case exemplifies the EFCC's proactive stance in combating cyber-enabled fraud and its commitment to holding perpetrators accountable under the relevant statutory frameworks. During the trial, the prosecutor presented testimony that the defendant and his accomplices had sent a solicitation email to Mr. George Robert Blick, an American citizen residing in Virginia, United States, purporting to seek a foreign contractor to assist in transferring $20.5 million USD. The nominal complainant, Mr. Blick, made a series of payments to the defendant, as agreed upon by the parties. However, subsequent to these transactions, all communication between the parties ceased. It was only then that Mr. Blick realized he had fallen victim to an alleged internet fraud scheme, perpetrated by the defendant and his cohorts, resulting in the loss of his hard-earned funds. This narrative underscores the deceptive tactics employed by the defendants to exploit their victim, highlighting the insidious nature of cyber-enabled financial crimes. Consequently, Mr. Blick submitted a petition to the EFCC, leading to the defendant's arrest. Upon conclusion of the trial, Oyewole J. delivered a verdict, stating: "The evidence presented by the prosecution unequivocally shows that the accused and his cohorts shared a common intention to defraud Mr. George, and, acting in concert, they successfully obtained various sums of money from him, as specified in counts 2, 8, 10, 12, 14, 18, 20, 22, 24, and 28. The accused is hereby found guilty as charged, with the prosecution having proven its case beyond a reasonable doubt."[108] Dissatisfied with the judgment, the defendant appealed to the Court of Appeal, which subsequently dismissed

[107] (2003-2010) ECLR 19-99; (2008) All FWLR (pt. 439) 436; (2008) LPELR-CA/L/124/2006.
[108] The defendant was also found guilty of the offences of conspiracy, forgery, uttering and for being in possession of documents containing false pretences.

the appeal and upheld the trial court's judgment, conviction, and sentences. This case starkly illustrates the pernicious nature of cybercrime in Nigeria, highlighting the need for sustained efforts to combat this menace.

3.1.4 Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006

The Advance Fee Fraud and Other Fraud Related Offences Act[109] criminalizes "advance fee fraud," commonly referred to as "419".[110] This legislation prohibits various forms of cyber-enabled fraud, including collecting money from unsuspecting individuals through false pretenses. The Act forbids the following methods of gaining money through false pretence and it includes obtaining property by false pretence,[111] use of premises for fraudulent activities,[112] fraudulent invitation,[113] attempts,[114] laundering of funds obtained through unlawful activity,[115] conspiracy, and aiding and abetting.[116] In the case of *Mike Amadi v. Federal Republic of Nigeria*,[117] the Appellant (Mike Amadi) was charged by the EFCC before the Lagos State High Court with, inter alia, attempting to obtain $125,000.00 USD from Fabio Fajans in connection with a forged Central Bank of Nigeria payment schedule containing false pretenses by demanding money to process a $2.5 million USD transfer, contrary to *sections 5(1), 8(b), and 1(3) of the Advance Fee*

[109] The concept 'advance fee fraud' expressly implies all fraudulent activities perpetrated with the aim and intent of obtaining money from another person by false pretence. On the other hand, by virtue of section 20 of the Advance Fee Fraud and Other Fraud Related Offences Act, 2006, false pretence refers to 'a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.'

[110] '419' originates from section 419 of the Criminal Code Act, Cap. 77 Laws of the Federation of Nigeria, 1990 and it is the first Nigerian criminal statutory provision to punish the act of obtaining money by false pretence. Same statutory provision is replicated in section 419 of the Criminal Code Act, Cap. C38 Laws of the Federation of Nigeria, 2004.

[111] *Section 1 and 2* of the Advance Fee Fraud and Other Fraud Related Offences Act, 2006.

[112] *Section 3 Ibid.*

[113] *Section 4 Ibid.*

[114] *Section 7 Ibid.*

[115] *Section 5 and 6 Ibid.*

[116] *Section 8 Ibid.*

[117] (2008) 12 SC (Pt. III) 55; 36.2 NSCQR 1127; (2008) LPELR-SC.331/2007.

Fraud and Other Fraud Related Offences Act Cap. A6 Vol. 1, Laws of the Federation of Nigeria 2004, now 2006. On May 20, 2005, the High Court found him guilty and sentenced him to 16 years imprisonment. Aggrieved with the judgment, the Appellant appealed to the Court of Appeal, which affirmed the High Court's judgment. The Appellant further appealed to the Supreme Court, which dismissed the appeal, upholding and affirming the judgments and sentences of the High Court and the Court of Appeal.

Furthermore, the Act imposes certain obligations on electronic communication service providers, such as telecommunication service providers, internet service providers, telephone and internet café operators, with the intention of intercepting and/or preventing the use of the internet and telecommunication facilities in advance fee scams. For example, the Act requires any person or organization offering an electronic communication service or remote computing service to obtain the full name, residential address in the case of an individual, and corporate address in the case of corporate bodies from the customer or subscriber via e-mail or any other form.[118] Failure to comply with the identifying information provision by a subscriber/customer or service provider is unlawful.[119]

3.1.5 Money Laundering (Prohibition) (Amendment) Act, 2012

The clandestine nature of cybercrime operations often yields substantial financial proceeds, which pose a challenge for criminals to utilize for high-end acquisitions without arousing suspicion. To circumvent this issue, illegal gains must be laundered to assume a legitimate

[118] *Section 12(1)* of the Advance Fee Fraud and Other Fraud Related Offences Act, 2006.
[119] *Section 12(2) Ibid* – where the section states that 'any customer or subscriber who (a) fails to furnish, the information specified in subsection (1) of this section; or (b) with the intent to deceive, supplies false information or conceals or disguises the information required under this section, commits an offence and is liable on conviction to imprisonment for a term of not less three years or a fine of ₦100,000; section 12(3) in addition to the above penalty makes service providers to forfeit the equipment or facility used in providing the service.

appearance, thereby facilitating money laundering. Historically, the majority of illicit funds have been laundered through financial networks in prominent global financial centers.[120] The money laundering process comprises three distinct phases: placement, wherein cash is introduced into the financial system; layering, involving complex transactions to obscure the illegal source; and integration, where wealth is generated from the illicit funds' transactions.[121] Notwithstanding existing legislative frameworks, money laundering persists unabated within the banking sector, likely attributable to the fact that certain individuals with controlling stakes and interests in banks engage in such practices. Moreover, the fees generated from these fictitious transactions contribute to increased bank profits, thereby enhancing their balance sheets and maintaining shareholder confidence.[122] In some instances, money launderers acquire controlling stakes in distressed banks, while cash-intensive enterprises remit high commissions to banks for facilitating these transactions, leading to a lack of scrutiny regarding the origin of these funds.[123] Regulatory agencies have been known to exhibit a lack of vigilance in addressing such non-compliance, despite their explicit mandates to enforce anti-money laundering regulations.[124]

In response to the persisting anomaly, the Money Laundering Act, 2004 was enacted to address the issue, but was subsequently repealed by the Money Laundering (Prohibition) Act, 2011. The latter was further amended by the Money Laundering (Prohibition) (Amendment) Act, 2012, expanding the scope of money laundering offenses and enhancing consumer due diligence measures. The Act explicitly prohibits the laundering of proceeds from crimes, drug trafficking, and other illicit activities. Although cybercrime is not explicitly mentioned, *section 15* of the Act

[120] FE Eboibi, 'Money Laundering in Nigeria: Implications for National Development'. *Umaru Musa Yar'Adua University Law Journal* [2014] (1) (1) 136-159.
[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] *Ibid.*

appears to encompass proceeds from cybercrime perpetrated by cybercriminals. Notably, the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 has criminalized cybercrime, suggesting that perpetrators may engage in organized criminal groups to commit cybercrime, fraud, and forgery, as covered under *section 15(6)*. Consequently, cybercrime can be construed as falling within the purview of "any other criminal act specified in this Act or any other law in Nigeria." Thus, proceeds generated from cybercriminal activities are deemed illegal, and their laundering constitutes a violation of the money laundering provisions, thereby contravening the law. In accordance with *section 15(2)* of the Act, individuals convicted of this offense are liable to a prison term ranging from 7 to 14 years.[125] In cases where the perpetrator is a corporate entity, conviction entails a fine equivalent to at least 100% of the illicitly acquired funds and properties, coupled with the potential revocation of their operating license.[126] Furthermore, if the corporate entity persists in committing the offense for which it was initially convicted, regulatory authorities may be compelled to rescind or revoke their certificate or license,[127] underscoring the severity of the legal repercussions for engaging in money laundering activities related to cybercrime.

3.1.6 Nigerian Communications Act, 2003

The Nigerian Communications Act, enacted in 2003, aimed to establish a comprehensive regulatory framework for the Nigerian communications sector, addressing pertinent issues.[128] Notably, the Act encompasses provisions related to cybercrime. Specifically, it mandates telecommunication companies to ensure their networks and facilities are not utilized for illicit

[125] *Section 15(3) Ibid*.
[126] *Section 15(4) Ibid*.
[127] *Section 15(5) Ibid*.
[128] *Section 1* of the Nigerian Communications Act, 2003.

activities. *Section 146 (1)* of the Act explicitly states that licensees must employ all necessary measures to prevent the commission of any offense under Nigerian statutes.[129] The detection and prevention of "the commission of any offence under any law in operation in Nigeria" encompasses cybercrime offences, as stipulated in the Cybercrimes (Prohibition, Prevention, Etc) Act 2015, which has been in effect since May 15, 2015. Telecommunication service providers are also required to comply with directives from the Nigerian Communications Commission (NCC) or other relevant authorities, on valid grounds, to prevent the commission or attempted commission of an offence under any written law in force in Nigeria.[130] Failure to meet these obligations gives rise to criminal liability. However, where a telecommunication service provider acts in good faith to fulfill these obligations, they will not incur criminal liability for any resulting harm.[131] The Nigerian Communications Act vests the Nigerian Communications Commission (NCC) with significant powers to regulate telecommunication service providers' roles in maintaining public safety and responding to emergencies. Notably, the Act empowers the NCC to determine whether telecommunication service providers should adopt capabilities for permitted communication interception, in compliance with specified technical requirements.[132] This provision enables the NCC to balance the need for effective communication interception with the need to protect citizens' right to privacy. Furthermore, the NCC is authorized to issue orders mandating the disclosure of specific communications or classes of communications to approved officers during public emergencies or for public safety reasons.[133] This measure ensures that telecommunication service providers can respond swiftly to emergencies while maintaining national security. Additionally, the NCC can order telecommunication service

[129] *Section 146(1) Ibid.*
[130] *Section 146(2) Ibid.*
[131] *Section 146(3) Ibid.*
[132] *Section 147 Ibid*.
[133] *Section 148(1)(C) Ibid*.

providers to establish disaster plans for the survivability and recovery of services and network facilities in the event of disasters, crises, or civil emergencies.[134]

3.1.7 Evidence Act, 2011

The preponderance of cybercrime cases presented in judicial proceedings entails electronic and computer-generated documents in various formats. These digital artifacts constitute a distinct category of evidence, characterized by their origination, storage, or derivation from computers, computer-based devices, or electronic communication systems. A hallmark of this evidence is its intangible nature, existing in a paperless format, yet stored in tangible objects. Examples of such digital evidence include emails, mobile phone records, text messages, telephone records, digital images, and electronically processed documents stored in computer-based devices.[135] The admissibility of this evidence is a crucial consideration in cybercrime litigation, as it significantly influences the outcome of cases.

The treatment of digital evidence by counsels and courts is of paramount importance, as the admissibility of a particular piece of evidence can significantly influence the outcome of a case.[136] The Act addresses the admissibility of electronic information in cybercrime trials, acknowledging the legitimacy of electronic and computer-generated evidence in legal proceedings.[137] *Section 84* of the Act extends the definition of records to include computer-

---

[134] *Section 149 Ibid*.
[135] FE Eboibi, 'Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence'. *Nigerian Law and Practice Journal* [2011] (10) 139-160.
[136] *Ibid.*
[137] *Ibid*; *section 84 and 258* of the Evidence Act, 2011. *Section 258* provides thus: 'A document includes- (a) books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter; (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it, and (c) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced

generated documents, facilitating effective cybercrime prosecution. However, the admissibility of digital evidence in cybercrime courts is contingent upon meeting specific criteria. As stipulated in Section 84, the document in question must have been produced by a computer operating regularly and properly, storing and processing information for the purpose for which the document was generated, during a specific time frame.[138]

3.1.8 National Information Technology Development Agency (NITDA) Act, 2007

In the past, the notion of cybercrime in Nigeria was considered a distant reality, akin to science fiction. However, the country now grapples with the stark reality of cyber criminality in the 21st century, which has ensnared a significant portion of the population, raising concerns about the impact on national security and social stability. Cyber criminal activities, including unauthorized access, surveillance, data interference, device interference, identity theft, and electronic fraud, are increasingly perpetrated through information technology resources.[139] To combat this, the National Information Technology Development Agency (NITDA) was established under the NITDA Act, 2007,[140] tasked with promoting and developing the use of information technology in Nigeria. Effective execution of NITDA's mandate could significantly hinder cybercriminal activities, rendering it challenging for perpetrators to exploit ICT for illicit purposes. This underscores the importance of robust institutional frameworks in mitigating cybercrime and promoting a safer digital environment.

---

from it; (d) any device by means of which information is recorded, stored or retrievable including computer output.' See also Ikenga KE Oraegbunam, 'Admissibility of Electronic Evidence under *Section 84* of Evidence Act 2011: Examining the Unresolved Authentication Problem'. *UNIZIK Law Journal* [2015] (11) 136-164. See further Ikenga KE Oraegbunam, 'Admitting Computer-Based Evidence in Nigeria: Resonances from South Africa, India and United Kingdom'. *The Nigerian Law Journal* [2017] (20) (1) 224-241.

[138] *Ibid.* See generally, *section 84(1), (2) and (4)*; see also *section 90(1)(a) and (d)* of the Evidence Act, 2011.

[139] *Ibid.*

[140] See the Explanatory Memorandum of the National Information Technology Development Agency (NITDA), Act 2007.

3.1.9 Criminal Code Act

The Criminal Code Act[141] prohibits various forms of stealing and false pretenses in Nigeria.[142] Specifically, the Act criminalizes obtaining property by false pretenses with the intent to defraud, punishable by three years' imprisonment.[143] Additionally, the Act proscribes fraudulent tricks or devices to obtain property, constituting a misdemeanor liable to two years' imprisonment.[144] These provisions prove instrumental in prosecuting cybercriminals who employ deceitful tactics, such as impersonating corporate directors or presenting fictitious accounts as genuine, with the intention of deceiving unsuspecting individuals. These misrepresentations facilitate fraudulent activities, underscoring the relevance of these legal provisions in combating cybercrime and protecting individuals from false pretenses.

The Criminal Code Act, a relic of the British colonial era, exhibits a pronounced anachronistic character, predating the advent of the internet and failing to explicitly address the nuances of internet fraud within its provisions on false pretenses.[145] This legislative lacuna is compounded by the requirement of a warrant for arrest, unless the perpetrator is apprehended in *flagrante delicto*,[146] rendering it challenging to apprehend cybercriminals who adeptly erase digital traces of their activities. The ephemeral nature of digital evidence and the ease with which cybercriminals can obfuscate their identities and activities underscore the need for a more adaptive and responsive legal framework.

---

[141] CAP. C38, Laws of the Federation of Nigeria, 2004.
[142] *Section 382-489* of the Criminal Code Act.
[143] *Section 419 Ibid*.
[144] *Section 421 Ibid.*
[145] M Chawki, 'Nigeria Tackles Advanced Fee Fraud'. *Journal of Information, Law and Technology* [2009] (1) 8. See Ikenga KE Oraegbunam, 'Combating Crimes in Cyberspace: Examining the (In)Adequacy of the Criminal Code Act and the Criminal Procedure Act'. *Ebonyi State University Law Journal* [2015] (6) (1) 2015 138-152.
[146] UV Awhefeada and OO Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria'. *Journal of Law and Criminal Justice* [2020] (8) (1) 30-49.

Moreover, the prescribed penalties, ranging from three to seven years' imprisonment, appear woefully inadequate in light of the substantial financial losses typically incurred by victims of cybercrime.[147] The disparity between the severity of the crime and the leniency of the punishment may be seen as a perverse incentive, potentially emboldening cybercriminals to exploit the vulnerabilities of the existing legal framework.

Furthermore, the criminal justice systems focus on the state as the primary complainant, rather than the victim, may discourage victims from reporting cybercrimes, as they may not receive restitution or compensation upon conviction.[148] This underscores the imperative for legislative reforms to effectively address the complexities of cybercrime, provide commensurate support for victims, and ensure that the legal framework is responsive to the evolving nature of cyber threats. In addition, there is a need for increased collaboration between law enforcement agencies, technology companies, and international organizations to effectively combat cybercrime on a global scale. By working together, these entities can share information, resources, and best practices to better identify, investigate, and prosecute cybercriminals.

3.1.10 Penal Code Act

The Penal Code Act[149] contains several provisions pertinent to cybercrime, which can be leveraged to combat this burgeoning threat. *Section 320*, for instance, criminalizes cheating by deception,[150] a tactic commonly employed in cybercrime. This provision is particularly relevant in addressing cyber terrorism and phishing, where inducement is a key element. Furthermore, *Section 362* of the Act addresses forgery, stipulating that dishonestly creating, signing, or

[147] T Oriole, 'Advanced Fee Fraud on the Internet'. *Computer Law and Security Report* [2005] (21) 241.
[148] *Ibid.*
[149] CAP P3, Laws of the Federation of Nigeria, 2004.
[150] *Section 320 (a) & (b)* of the Penal Code Act.

altering a document with the intent to deceive others into believing it is authentic or authorized constitutes a criminal offense. This provision can be utilized to prosecute cybercriminals engaging in forgery and counterfeiting.

However, it is essential to note that the Penal Code Act is an antiquated legislation, primarily applicable to the Northern region of Nigeria. Its limited scope and outdated provisions may hinder its effectiveness in addressing the complexities of modern cybercrime. Consequently, there is a pressing need for comprehensive legislative reforms to ensure a robust and adaptable legal framework capable of addressing the evolving nature of cyber threats.

3.2 Continental and Sub-Regional Legal Regime

Notably, a plethora of continental and sub-regional legal frameworks have been instituted to counter the burgeoning threat of cybercrime, including, but not limited to, the following exemplary laws:

3.2.1 The Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime Within ECOWAS

A notable sub-regional legal regime for combating cybercrime is the Economic Community of West African States (ECOWAS) Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted in Abuja in 2011 (hereinafter referred to as "The Directive"). This instrument seeks to establish a harmonized framework for criminal liability, with the ultimate objective of effectively combating cybercrime within the ECOWAS sub-region through the creation of a unified legal paradigm.[151] The Directive acknowledges the internet's role in precipitating a surge of egregious cyber-

[151] Article 2 of the Directive C/DIR.1/08/11 on Fighting Cybercrimes within ECOWAS Sixty-Sixth Ordinary Session of the Council of Ministers.

enabled activities, and accordingly, establishes a comprehensive framework to counter these threats. Key provisions include the imposition of liability on corporate entities, authorization of searches and access to computer systems by law enforcement agencies, expedited preservation of digital evidence, and facilitation of inter-member state cooperation. The Directive's scope encompasses all cyber-related offences within the Economic Community of West African States, as well as traditional criminal offences that necessitate the collection of electronic evidence for their detection and prosecution.[152] The Article stipulates that the utilization of Information and Communication Technology (ICT) to perpetrate offences, including but not limited to theft, fraud, possession of stolen goods, breach of trust, extortion, terrorism, money laundering, and organized crimes, elevates the severity of such crimes to a higher degree than their common law counterparts. This provision acknowledges the exacerbated harm and complexity occasioned by the leveraging of ICT in the commission of these offences, thereby warranting enhanced legal scrutiny and penal consequences.[153] The Article further proscribes a range of egregious cyber-enabled offences, including theft, fraud, possession of stolen goods, breach of trust, extortion, terrorism, and counterfeiting, all of which relate to computer data and software, thereby criminalizing these activities and affording protection to digital assets and computer systems.

3.2.2 The African Union's Convention on Cyber Security and Personal Data Protection

At the regional level, the African Union Convention on Cybersecurity and Personal Data Protection,[154] adopted in Malabo on 27th June 2014, underscores the commitment of member states to foster a robust information society, predicated on the principles of human rights,

---

[152] *Article 3*.
[153] *Article 24,* Aggravating Circumstances of Common Law Offences
[154] African Union, *African Union Convention on Cyber Security and Personal Data Protection,* Available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 20 April 2024.

through the harmonization of cyber legislation across Africa. The Convention's framework is articulated in two primary chapters: Chapter One addresses electronic transactions and commerce, while Chapter Two focuses on the protection of personal data. Furthermore, the Convention mandates member states to establish criminal sanctions that are efficacious, proportionate, and dissuasive, applicable to both natural and legal persons, thereby ensuring a unified and effective approach to cybersecurity and data protection.

The Convention's provisions also emphasize the importance of international cooperation, capacity building, and technical assistance to enhance the implementation of its provisions. By facilitating collaboration among member states, the Convention aims to create a harmonized and secure digital environment, conducive to economic growth, innovation, and the promotion of human rights. This regional framework serves as a vital instrument for addressing the evolving challenges of cybersecurity and data protection in Africa, and its implementation is crucial for ensuring a safe and secure digital landscape for citizens, businesses, and governments alike. The Convention also promotes information sharing and best practices to strengthen cybersecurity measures across the continent. Through regular review and updates, member states can adapt to new threats and technologies, ensuring the continued effectiveness of the Convention in safeguarding Africa's digital infrastructure.

3.3 International Legal Regime

In this section, we will explore Nigeria's international legal obligations and the institutional framework in place for combating cybercrime. Nigeria is a signatory to various international conventions and treaties that address cybercrime such as:

3.3.1 The Budapest Convention on Curtailing the Menace of Cybercrime

The Council of Europe Convention on Cybercrime, commonly referred to as the Budapest Convention, was adopted in 2001 and entered into force in 2004. This pioneering international instrument seeks to promote a unified anti-cybercrime policy among its member states, achieved through the adoption of harmonized legislation, fostering international cooperation, and deterring the misuse of computer networks and electronic information. The Convention strikes a delicate balance between the interests of law enforcement and the protection of fundamental human rights. As the first international treaty to combat cybercrime and promote cybersecurity, it serves as a paradigm for global efforts to address the evolving threats of the digital age.[155]

Notably, Nigeria is not a member of the Council of Europe and has not acceded to the Budapest Convention. Nevertheless, a critical examination of the relevant legislation reveals a substantial alignment with the Convention's provisions, underscoring Nigeria's commitment to combating cybercrime and promoting cybersecurity, despite its non-membership. This de facto conformity highlights the importance of international cooperation and harmonization in addressing the transnational nature of cyber threats.

The Convention seeks to harmonize national laws on cybercrimes, facilitating a unified approach to combat cybercrimes both domestically and internationally through enhanced international cooperation and assistance, encompassing a range of internet-related offences, including illegal interception,[156] electromagnetic emission from a computer system.[157] Data interference is characterized by the intentional and unauthorized alteration, damage, deletion, deterioration, or

[155] OJ Olujobi and OM Olujobi, 'Re-Thinking and Optimizing Nigeria's Anti-Corruption Legal Framework: Upstream Petroleum Sector Corruption Evaluation'. *Journal of International and Comparative Law* [2020] (8) 79-105.
[156] *Article 3*, Budapest Convention.
[157] *ibid*

suppression of computer data, resulting in its modification, destruction, or rendered unusable, thereby compromising the integrity and reliability of digital information.[158] The objective is to safeguard computer data and programs from intentional corruption or damage, ensuring the integrity and security of digital assets.[159] It prohibits system interference and device misuse, mandating member states to enact legislative measures that establish criminal offenses under their domestic law for intentional, unauthorized acts.[160] Critics contend that the Convention is bereft of robust enforcement mechanisms and strategies, and is hindered by jurisdictional complexities in nations where cybercriminals operate with impunity. Notwithstanding these limitations, the United States and three additional nations have ratified the Convention, underscoring their commitment to combating cybercrime.[161] The jurisdictional framework outlined in the Article is predicated on the locale where the offence of cyberterrorism is perpetrated, either entirely or partially. The Convention adopts a dual approach, leveraging both territorial and nationality models, to confer jurisdictional authority upon member states, thereby enabling them to assert legal jurisdiction over cyberterrorism offences. This allows for a more coordinated and cooperative effort in investigating and prosecuting cybercrimes across borders. By ratifying the Convention, countries are signaling their willingness to work together to address the growing threat of cyberterrorism. This unified front is crucial in combating the increasingly sophisticated tactics used by cyberterrorists to disrupt global networks and systems. By establishing clear guidelines for jurisdictional authority, the Convention helps to streamline international cooperation in addressing cyberterrorism, ultimately making it more difficult for perpetrators to evade justice.

---

[158] *Ibid, Article 4(1).*
[159] *Ibid, Article 4(2).*
[160] *Ibid, Article 6(1).*
[161] Explanatory Report of the Committee of Ministers of the Convention on Cybercrime 109th Session (Adopted on November 8, 2001).

3.3.2 The United Nations Convention on the Use of Electronic Communication in International Contracts

Pursuant to *Article 2*, the scope of the United Nations Convention on the Use of Electronic Communication in International Contracts is circumscribed, excluding applications wherein the buyer is acting in a capacity other than as a consumer. Furthermore, the instrument's efficacy is constrained by its failure to provide bespoke legal frameworks tailored to govern online transactions, thereby limiting its applicability in this realm.[162]

Notwithstanding these limitations, the Convention constitutes a seminal effort towards establishing a harmonized legal framework for electronic communication in international contracts, providing a nascent foundation for future scholarly critique, development, and refinement.[163] By acknowledging and interrogating its shortcomings, academics and practitioners can collaboratively endeavour to create a more comprehensive and efficacious legal environment that fosters innovation, growth, and trust in the digital economy.

3.3.3 The Charter of the United Nations

The United Nations Charter[164] articulates a paradigmatic framework for the international community, predicated on the establishment of conditions conducive to the perpetuation of justice, the observance of treaty obligations, and the reverence for international law. This foundational instrument seeks to foster an environment that promotes social progress and elevates standards of living. Notably, the Charter vests the Security Council with the authority to

---

[162] FM Opebiyi, 'Protecting the Interest of Buyers in Online Contracts of Sale in Nigeria: Making a Case for Legislative Intervention'. *Elizade University Law Journal* [2018] (1) 222.
[163] The United Nations, 'The United Nations Convention on the Use of Electronic Communications in International Contracts Enters into Force on 1 March 2013,' *Information Service Vienna.* Available at <https://unis.unvienna.org/unis/pressrels/2013/unisl181.html> accessed on 26 July 2024.
[164] Charter of the United Nations, San Francisco 1945.

discern and determine the existence of threats to peace, breaches of peace, or acts of aggression, empowering it to proffer recommendations or decree measures consonant with Articles 41 and 42. This dual capacity enables the Security Council to maintain or restore international peace and security, thereby ensuring the stability and tranquility of the global community.[165]

The Charter's emphasis on collective security and the maintenance of international peace and security underscores the imperative of cooperation and collaboration among nation-states. The Charter's establishment of a framework for pacific dispute settlement and aggression prevention serves as a stalwart bulwark against conflict's destabilizing repercussions, thereby fostering an environment that facilitates economic development, social justice, and the realization of human rights, ultimately promoting a harmonious and prosperous international order. As such, the Charter remains a cornerstone of international relations, providing a normative framework for the promotion of peace, security, and cooperation among nations.

3.3.4 The United Nations General Assembly Resolutions

A myriad of United Nations General Assembly Resolutions have been enacted to address the burgeoning issue of cybersecurity, underscoring the imperative of collective action in this domain. Notably, one such resolution facilitated the convening of an international group of government experts from fifteen nations, including the United States, to submit a comprehensive report. This resolution sought to foster cooperation amongst member states towards the establishment of a peaceful, secure, resilient, and open information communication technology environment, predicated on a consensus regarding norms, rules, and principles of responsible behaviour. To achieve this objective, the resolution advocated for the implementation of

[165] *Article 39 Chapter VII* regarding peace, breach of the peace and acts of aggression.

confidence-building measures, including the exchange of information and capacity-building initiatives.[166]

Furthermore, in December 2001, the General Assembly ratified Resolution 56/183, which endorsed the World Summit on the Information Society, a seminal gathering aimed at deliberating the prospects and challenges of the information society. This inaugural summit, attended by representatives from 175 nations, culminated in the declaration of principles for achieving an open information society, thereby laying the groundwork for a harmonized approach to navigating the complexities of the digital era. Notwithstanding the progress made, several contentious issues remained unresolved, including the contentious question of internet governance and the complexities of funding. Moreover, the proposals advocating for the United States to relinquish its control over the Internet Corporation for Assigned Names and Numbers (ICANN) were met with resistance and ultimately declined, thereby perpetuating the existing power dynamics and precipitating ongoing debates regarding the equitable distribution of authority and resources in the digital realm.

3.4 Institutional Framework for Combatting Cybercrime in Nigeria

3.4.1 The Economic and Financial Crimes Commission (EFCC) Institution

To combat all economic and financial-related crimes in Nigeria, the Economic and Financial Crimes Commission (EFCC) was founded as an institution under the Economic and Financial Crimes Commission Act (EFCC Act). The Act gives the Commission the authority to look into any individual, corporate body, or group that has committed any Act pertaining to financial or economic crimes.

[166] United Nations General Assembly, Resolution 56/183: World Summit on the Information Society (2001) available at <https://www.itu.int/net/wsis/documents/background.asp?lang=en&c_type=res> accessed 29 May 2024.

According to *Section 5* of the Act, the Commission is tasked with investigating all financial crimes, including advance fee fraud, money laundering, counterfeiting, and unlawful charge transfers, as well as enforcing and properly administering the Act. In consultation with the Attorney-General of the Federation, it is also tasked with prosecuting any offences related to or associated with economic and financial crimes. The "Yahoo boys," who engage in cross-border cybercrimes capable of undermining national economies, are among the criminal actions that fall under these economic crimes[167]. The EFCC has used *Section 5* as justification for a number of arrests and prosecutions, including in the Federal Republic of *Nigeria v. Chief Emmanuel Nwude & Ors* case[168]. The accused in this case was accused of committing the largest single swindle in the third world, with many more pending. As a result, the defendants were found guilty and given the appropriate sentences after being charged with 57 counts in the High Court of Lagos State, including receiving $181.6 million in money via false pretences. Their assets were forfeited to the Federal Government of Nigeria in addition to this penalty, and the owners received the money that was recovered. *Sections 14 through 18* list offences that fall under the Act's purview. This covers offences related to financial malpractice, terrorism, misleading information, and economic and financial crimes.

According to *Section 46* of the Act, "economic crime" is defined as any non-violent criminal and illicit activity carried out with the intention of illegally obtaining wealth, either alone or in concert with others, in violation of the laws currently in place that regulate the government's and its administration's economic operations. The following are prohibited: illegal arms dealing, smuggling, human tracking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices, including currency counterfeiting, theft of intellectual property

[167] O Ehimen and A Bola, 'Cybercrime in Nigeria.' *Business Intelligence Journal* [2010] (3) (1) 95.
[168] Suit No: CA/245/05.

and policy, open market abuse, dumping of toxic wastes, and any kind of fraud, narcotic drug tracking, money laundering, embezzlement, bribery, looting, and corrupt practices.

Section 7(2) of the EFCC Commission (Establishment) Act 2004 gives the Commission the responsibility of enforcing the provisions of:

a. The Money Laundering Act 2004
b. The Advance Fee Fraud and Other Related Offences Act 2006
c. The Failed Banks (Recovery of debts) and Financial Malpractices in Banks Act 1994, as amended.
d. The Banks and Other Financial Institution Act 1991 (Reenacted 2020)
e. Miscellaneous Offences Act
f. Any other law or regulations relating to economic and financial crimes including the Criminal Code orPenal Code.

It is argued that, by relying on the Advance Fee Fraud and Other Related Offences Act 2006 and other pertinent laws, the EFCC (Establishment) Act 2004 gives the EFCC the authority to look into and bring charges against those who commit cybercrimes, such as Internet or online advance fee fraud in Nigeria. For example, the accused in *Harrison Odiawa v. Federal Republic of Nigeria*[169] was charged by the EFCC with 58 counts of offences, including conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering, and possession of documents containing false pretence in violation of the Advanced Fee Fraud and Other Related Offences Act. The accused person pretended to be Abu Belgore. During the trial, the prosecution testified that the accused and his cohorts sent a solicitation e-mail to one Mr. George Robert Blick (the

[169] [2008] All FWLR (Pt. 439) 436.

nominal complainant), an American citizen resident in Virginia, USA, looking for a foreign contractor to facilitate the transfer of $20.5 million US dollars. In the aforementioned message, he was urged to react if he was interested, which Mr. George responded by e-mail, claiming that he had a United States registered corporation that could be used to collect the monies. For contractual documentation and finalization purposes, it is noted that the accused and their associates solicited various sums of money from Mr. George through email correspondence, telephone conversations, and fax transmissions. These requested amounts included payments for purported services such as document creation ($187,000 USD), bank account opening (£10,000), trust processing ($18,750 USD), ICP number issuance ($410,000 USD), petition resolution ($750,000 USD), and payments to Nigerian government officials ($250,000 USD and $350,000 USD). Additional requests were made for transportation ($300,000 Euros), machine repair ($1.5 million USD), and insurance ($1.2 million USD). Following that, the parties stopped communicating, and Mr. George realised he had been duped. He subsequently submitted a petition to the EFCC, which resulted in the accused's apprehension. Hon. Justice J.O.K. Oyewole concluded the hearing by ruling that the prosecution's evidence clearly showed that the accused and his associates had a shared goal to defraud Mr. George, and that they worked together to obtain the various sums of money listed in counts 2, 8, 10, 12, 14, 18, 20, 22, 24, and 28 from him. As a result, the accused was found guilty as charged. The accused appealed to the Court of Appeal because they were unhappy with the court's decision. The Court of Appeal upheld the trial court's verdict, conviction, and penalties while rejecting the appeal.

It is evident from the aforementioned sections that while EFCC as an institutional framework for addressing cybercrime in Nigeria efficiently addresses fraud related to the internet, it falls short in addressing cybercrimes. This is due to the fact that online fraud is but one aspect of the

problem. Internet-related fraud is included in cybercrime, which also includes other crimes including hacking, cyberstalking, and child pornography.

3.4.2 The Federal High Court

The Federal High Court is a pivotal institution in Nigeria's fight against cybercrime, providing a legal framework for prosecuting and adjudicating cybercrime cases. *Section 251(1)* of the 1999 Constitution of Nigeria grants the Federal High Court exclusive jurisdiction over matters related to cybercrime. For instance, in the case of *Economic and Financial Crimes Commission (EFCC) v. Onyekachi Emmanuel Nwagwu & 5 Others*[170], the Federal High Court convicted cybercriminals for allegedly defrauding an American citizen of $1.4 million through business email compromise and identity theft. The defendants were charged with conspiracy, cybercrime, and money laundering, highlighting the EFCC's efforts to combat online fraud and protect individuals and businesses from cyber threats.

The Cybercrime Act 2015 is the primary legislation governing cybercrime in Nigeria. The Act establishes the National Cyber Security Fund and the Cybercrime Advisory Council to oversee and coordinate cybersecurity efforts. The Federal High Court plays a crucial role in enforcing this Act, ensuring that perpetrators are brought to justice. For example, the Court has jurisdiction over cases involving identity theft, cyber-stalking, and cyber-bullying, such as the case of *Federal Republic of Nigeria v. Akeem Giwa & 2 Others* (2020)[171], where a defendant was convicted for online harassment, internet fraud and money laundering.

The Federal High Court's jurisdiction extends to various cybercrime offenses, including unauthorized access to computer systems or networks, phishing, and online scams. The Court's

[170] (2020) FHC/L/419C/2019
[171] FHC/L/292C/2020

decisions in cybercrime cases provide legal precedent, shaping Nigeria's cybersecurity landscape. Illustratively, in *EFCC v. Okechukwu Joseph* (2019)[172], the Court ruled that cryptocurrency transactions can be used as evidence in cybercrime cases.

Effective collaboration between law enforcement agencies, service providers, and the judiciary is essential in combating cybercrime. The Federal High Court's role in interpreting the Cybercrime Act 2015 and ensuring that law enforcement agencies operate within the bounds of the law is critical. By doing so, the Court safeguards individual rights while protecting Nigeria's digital economy from cyber threats. For example, the Court has ordered internet service providers to block access to websites promoting cybercrime activities.

[172] FHC/ABJ/CR/145/2019

CHAPTER FOUR

THE CYBERCRIMES ACT 2015: EVALUATING EFFECTIVENESS, GLOBAL ALIGNMENTS, AND CHALLENGES - PROSPECTS FOR FUTURE ENHANCEMENT

4.1 Cybercrime Typologies under the Cybercrimes Act 2015: An Examination of Prohibited Offenses:

There are several forms of cybercrimes that are criminalized by the Cybercrimes Act 2015. These offenses carry severe penalties, including fines and imprisonment, in order to deter individuals from engaging in these illegal activities. They are discussed below:

4.1.1 Offences against Confidentiality, Integrity and Availability of Computer Data and Systems

The ubiquity of digital technology, specifically networked communication, has rendered it an indispensable component of critical infrastructure. Consequently, the vast amount of sensitive information pertaining to government and commercial entities, stored and transmitted electronically, precipitates a heightened risk of cyber espionage. This vulnerability, to Clough, underscores the necessity for robust cybersecurity measures to safeguard against unauthorized access, data breaches, and potential national security threats[173].

Within the framework of the Act, a specific classification of offences has been established, incorporating unlawful access to computer systems[174], unauthorized interceptions of electronic communications[175], and deliberate interference with computer systems[176]. Given the pervasive

[173] Jonathan Clough, 'Cybercrime', *Commonwealth Law Bulletin* [2011] (37) (4) 671-680, at 675.
[174] *Section 6* of the Act.
[175] *Section 12* of the Act.

integration of computers into modern life and the increasing dependence of global commerce on intricate computer networks, these offences possess significant potential for detrimental consequences, thereby necessitating stringent regulatory measures and robust enforcement mechanisms.

The concept of unlawful access to a computer system is analogous to illegal entry into a physical building, and is thereby recognized as a criminal offence under the Act[177]. This unauthorized access disrupts the ability of computer operators to manage, operate, and control their systems in an undisturbed and uninhibited manner, ultimately compromising the integrity of these systems. The primary objective of prohibiting unlawful access is the preservation of computer system integrity. However, a pivotal question arises: does the unlawful access contemplated by *Section 6 of the Act*[178] constitute the ultimate goal, or does it extend to encompass subsequent offences perpetrated following initial access, such as data modification or obtainment, which potentially violate data integrity and confidentiality[179]? This inquiry is particularly pertinent, as legislative provisions often conflate unlawful access with subsequent offences. The Act unequivocally criminalizes both the act of illegal access and subsequent offenses, clarifying any potential confusion between the two. This question is pertinent due to enacted provisions sometimes conflating illegal access with subsequent offenses. However, a conjunctive reading of *Section 6* of the Act reveals that the provisions criminalize both illegal access and subsequent offense.

---

[176] *Section 8* of the Act.

[177] *Section 6(i)* provides in part: "Any person, who, without authorization, intentionally accesses, in whole or in part, a computer system or network for fraudulent purpose and obtain data that are vital to national security, commits an offence….." *section 6 (2)* says: "where the offence provided un subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program commercial or industrial secrets or classified information……"

[178] *Ibid*

[179] See Prof. Dr. Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, (September 2012), 179. Available at <www.itu.int/ITUD/Cybersecurity/legislation/html.page> accessed on October 17 2024.

Specifically, *Section 6(i)* addresses access "in whole or in part," while *Section 6(2)* imposes harsher penalties for illegal access committed with the intent to obtain computer data, etc. Moreover, the section mandates that the act of unlawful access must have been committed with the requisite intention.

The offence established by *Section 6* of the Act hinges on the notion that "access to a computer" must occur without authorization. This critical element underscores the legislative intent to safeguard computer systems from unauthorized intrusion. Notably, *Section 6* implicitly incorporates the concept of self-defence, recognizing the right of system owners to protect their digital assets from unwarranted access.

However, the provisions of *Section 6* may encounter ambiguities in scenarios where initial access was lawful, but subsequent use continues after permission has expired. This raises complex questions regarding the boundaries of authorized access and the point at which it becomes unlawful. The Act's framework must therefore be carefully interpreted to address such nuances, ensuring that the law effectively balances the need to prevent unauthorized access with the realities of dynamic access permissions.

It is pertinent to propose the incorporation of a provision analogous to *Section 5* of the "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedure Cybercrime Legislative text"[180] within the Act to mitigate existing ambiguities. *Section 5* of this legislative framework stipulates that "Illegal Remaining" constitutes an offense, wherein an individual intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in to a computer system or part

[180] *Enhancing Competitiveness in the Caribbean Through ICT Policies, Legislation and Regulatory Procedure 1980*, available at <www.itu.int/ITU-D/projects/ITU EC ACP/icb4pis/index.html> accessed on 17 October 2024.

thereof or continues to utilize a computer system, thereby rendering them liable to conviction and punishable by imprisonment for a period not exceeding (period), or a fine not exceeding (amount), or both, also encompassing "Unlawful Interception"[181].

Section 12 of the Act emphasizes the pivotal role of computer data for private users, commercial entities, and administrative bodies. Specifically, it highlights the significance of data integrity, as any deficiency or loss thereof can result in substantial financial repercussions for affected parties.

A meticulous examination of the section reveals that its scope is restricted to the interception of data via technical means. Notably, the section specifically addresses the interception of "non-public transmissions." The term "transmission" encompasses all forms of data transfer, including telephone, fax, email, and file transfer. A transmission is deemed "non-public" if the transmission process is confidential[182]. As Gercke[183] astutely observes, the determinative factor distinguishing public from non-public transmission lies not in the nature of the data transmitted, but rather in the transmission process itself. Crucially, even the transfer of publicly available information can constitute a criminal offense if the parties involved intend to maintain the secrecy of their communication's content.

---

[181] *Section 12 (i)* of the Act "Any person who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a five of not more that N5,000,000:00 or to both such fine and imprisonment. Cf with *Article 3* of the European Convention on Cybercrime, 2000, which provides: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmission of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system." (CETS No. 185) available at: <http://conventions.co.int> accessed on 15 October, 2024.

[182] Prof. Dr. Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, (September 2012) 186, available at <www.itu.int/ITUD/cyb/cybersecurity/legislation.htmlat> accessed on 15 October 2024.

[183] *Ibid*, at 186.

4.1.2 System Interference

The Act further criminalizes the intentional obstruction of lawful computer system utilization[184]. Notably, the application of this provision is circumscribed by several key criteria. Specifically, the hindering must be deemed "serious" and must be perpetrated through one of the explicitly enumerated acts. Additionally, the offender's actions must be characterized by intent or fraudulent purpose, and must lack lawful authority. Furthermore, the legislation also proscribes acts that render computer data inaccessible, thereby ensuring the protection of digital information.

However, since legal arguments may focus on the requirements to be met for determining whether or not the hindering of the computer system's functioning is serious, the requirement that the specific section can be invoked only in cases where the hindering is serious is likely to cause confusion. It is suggested that *section 8* of the Nigerian law be replaced with a clause akin to *section 7 of the 1999 Stanford Draft International Convention* in order to avoid needless debates. The relevant section offers[185]:

> '*7 (1)* A person who intentionally or recklessly without lawful excuse or justification: (a) hinders or interferes with the functions of a computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction for a period not exceeding (period), or a fine not exceeding (amount) or both in subsection (i)

[184] *Section 8* of the Act provides "Any person who, without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating; altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 to both fine and imprisonment. Contrast with *Art 5*. Of the European Convention on Cybercrime, 2000 and *section 7* of the 2002 Commonwealth Model Law, available at <www.thecommonwealth.org/sharedaspfiles/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77=86970A639805%7Computer%20Crime.pdf> (Annex1). The latter also criminalizes "reckless" acts accessed on 15 October 2024.

[185] *Section 7* of the 1999 Stanford Draft International Convention available at <http://media,hoover.org/documents/0871999825 249.pdf> accessed on 15 October 2024.

> "hinder," in relation to a computer system, includes but is not limit to: (a) cutting the electricity supply to a computer system, and (b) causing electromagnetic interference to a computer system by any means; and (c) corrupting a computer system by any means; and (d) inputting deleting or altering computer data'.

The definition of the word "hinder" in the preceding section must be incorporated into our *section 8* in order to broaden the number of acts that can have a negative impact on the operation of computer systems.

4.1.3 Content Related Offences

The Act encompasses content-related offences, specifically addressing child pornography and related transgressions[186], as well as racist and xenophobic offences[187]. These provisions underscore the legislature's commitment to combating harmful and exploitative content.

4.1.4 Child Pornography

Crimes involving child pornography have detrimental effects on society, particularly on young victims, who are particularly vulnerable in these cases[188]. Since violations in this area are commonly acknowledged as criminal acts[189], there is no question that the provisions of *section*

---

[186] *Section 23* of the Act. ." It provides in part: Any person who intentionally uses any computer system or networking in or for:- (a) Producing child pornography; (b) offering or making available child pornography (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person. (e) possessing child pornography in a computer system or on a computer data storage medium: commits an offence under the Act and…."

[187] *Section 26* of the Act. It provides in part: "Any person who with intent – (a) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network; (b) threatens through a computer system or network – (i) persons for the reasons that they belong to a group distinguished by race, colour, descent, national or ethnic origin….."

[188] Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime (UNDO), (February 2013).

[189] See 1989 United Nations Conventions on the Rights of the Child, available at <www.g8.gc.ca/genoa/july-22-01-1-e.asp> accessed on 16 October 2024; 2003 European Union Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography; available at <http://eur-;ex.europe.en/Lexuriserv/site/en/oj/2004/1013/101320040120en004400e8.pdf> accessed on 16 October 2024 and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, available at <http://conventions.coe.int> accessed on 16 October 2024.

23 are consistent with international best practices. This crime can only be committed with the necessary purpose. By establishing crimes for manufacturing, offering or making available, distributing or transmitting, procuring, and possessing, this section aims to modernise the laws pertaining to child pornography and to impose penalties on the actions of all parties involved.

The difficulties here, however, stem from the fact that different nations may have different views on the legal age of consent, whether "simple" possession should be illegal, and whether or not "materials that visually depict" should be included in the definition of child pornography as stated in our *Section 23*.

Prof. Marcon Gercke clearly captures another issue with the execution of *section 23* when he observes as follows[190]:

> 'The legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world. If offenders create content that is illegal in some countries, but not in the country they are operating from, prosecution of the offenders is difficult or impossible. There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized'.

Analogous to the above position is the vexed issue of how to enforce *section 23* without interfering with the right to freedom of expression[191]. One potential solution could involve implementing clear guidelines and regulations for the enforcement of *section 23* in a way that respects freedom of expression. Additionally, establishing a system for monitoring and addressing any potential conflicts that may arise between these two rights could help ensure a balanced approach.

---

[190] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012) available at: <www.itu.int/ITUD/Cyb/cybersecurity/legislation.htmlatpage21> accessed on 15 October 2024.
[191] Section 39(1) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).

4.1.5 Racist and Xenophobic Offences

According to *section 26* of the Act, it is illegal to purposefully distribute and make xenophobic content available to the general public via a computer system.

The Nigeria Act's failure to specify what qualifies as "racist and xenophobic material" is one of its flaws. However, it is clear from the language of section 26 that any content that encourages, supports, or incites hatred, discrimination, or violence against individuals because they are members of a group that is distinguished by race, colour, descent, national or ethnic origin, or religion, if used as a pretext for any of these factors, or a group of people that is distinguished by any of these characteristics, will be considered racist and xenophobic.[192] "It is also an offense[193] to insult the public by using a computer system or network people mentioned in the previous sentence.

Since the Act merely makes threats made "through a computer or computer network" illegal, it is argued that the word "threatens" in *section 26 (1) (b)* does not require any contact with the public.

Furthermore, insults directed "publicly through a computer system or network to persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors" are illegal under *section 26(i)(c).* This specific clause clearly does not apply to insults sent via private correspondence, such as emails, since they would not be considered public insults.

[192] section 26 (1)(b) (i) of the Act
[193] section 26 (1) (c) (i) of the Act

The Act does not, however, specify what is meant by "insult." There must be caution to ensure that the sanctity of the principles of freedom of speech as guaranteed by the constitution[194] is not violated if the term "insults" is understood to refer to any offensive or invective expression that prejudices a person's dignity and is directly related to the insulted person's membership in the group. Naturally, the court would have to define the act of insult envisioned under *section 26* of the Act carefully in order to protect the values of freedom of expression protected by the constitution.

4.1.6 Computer-related Offences

Computer-related offences, as defined under the Act, comprise criminal activities facilitated through computer use. This category encompasses computer-related forgery[195], computer-related fraud[196], and identity theft and impersonation[197], highlighting the diverse range of offences perpetrated through digital means.

4.1.7 Computer-related Forgery[198]

Section 13 of the Act addresses computer-related forgery, focusing on safeguarding data by preventing acts that yield inauthentic data. This provision extends beyond mere data manipulation, encompassing the creation of false information. Its scope ensures data integrity, shielding individuals and organizations from harmful consequences. Computer-related forgery is a serious offense that can have far-reaching consequences, threatening the credibility and

[194] *Section 39(1)* Constitution of the Federal Republic of Nigeria 1999 (as amended).
[195] *Section 13* of the Act
[196] *Section 14* of the Act.
[197] *Section 22* of the Act
[198] *Section 13* of the Act provides “A person who knowingly accesses any computer or network and inputs, alters, delete, or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible comits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less that N7,000,000 or both”.

reliability of important information. By criminalizing the creation of false data, the Act aims to protect the public from being deceived or misled by fraudulent information. This provision serves as a crucial deterrent, discouraging individuals from engaging in activities that compromise the integrity of digital data.

4.1.8 Computer-related Fraud[199]

Fraud constitutes a pervasive form of cybercrime, manifesting in various guises, including fraudulent online sales, advance fee schemes (notably, the infamous 419 scams), fraudulent investment opportunities, and unauthorized electronic fund transfers. *Section 40* of the Act specifically criminalizes intentional manipulation within data processing, aimed at facilitating illicit property transfers. Furthermore, *Sections 14(1)-(5)* of the Act stipulate that culpability requires intentional conduct, wherein intent encompasses both the manipulative act and resultant financial loss.

4.1.9 Identify Theft and Impersonation

Identity theft and impersonation constitute an egregious form of cybercrime, involving the fraudulent acquisition and exploitation of another individual's personal identity. The incorporation of *Section 22* in the Act is noteworthy, as it acknowledges the limitations of traditional criminal law in addressing the preliminary stages of identity-related offenses. Specifically, *Section 22* targets the collection, processing, and trafficking of identity information,

[199] *Section 14* of the Act. "*section 14 (1)* Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring economic benefits on himself or another person, commits an offence and shall be liable on conviction to imprisonment for a term not less than 3 years, or to a fine of not less than N7,000,000.00 or to both fine and imprisonments".

thereby bridging a critical gap in the legal framework. According to Marco Gercke[200], this provision encompasses three distinct phases:

> 'the first phase the offender obtains identity related information. This part of the offence can for example be carried out by using malicious software or phishing attacks. The second phase is characterized by interaction with identity related information prior to the use of the information within criminal offences. The third phase is the use of the identity related information in relation with a criminal offences. In most cases, the access to identity related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities'.

Section 22 of the Act provides a comprehensive framework for addressing identity theft, encompassing a broad spectrum of offences within the three phases outlined by Marco Gercke[201]. Notably, the criminalization provisions under *Section 22* are not phase-specific, indicating a nuanced approach to combating identity theft in its various manifestations. This approach allows for flexibility in prosecuting offenders who may engage in multiple phases of identity theft, ensuring that the law remains adaptable to evolving criminal tactics.

4.2 Mitigating Cyber Threats in Nigeria: An Evaluation of the *Cybercrimes Act 2015*'s Effectiveness in the Prevention and Prosecution of Cybercrimes

The *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* constitutes a robust legislative framework that comprehensively addresses the multifaceted nature of cybercrimes, proscribing detrimental behavioral patterns within the cyberspace, including cyber stalking, cybersquatting, computer-related fraud and forgery, and cyber terrorism[202]. Notably, the Act stipulates stringent

---

[200] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. available online at <www.itu.int/ITU-D/Cyb/Cybersecurity/legislation.html> accessed on 17 October 2024.
[201] *Ibid*
[202] W Brenner Susan, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Springer 2012) 123.

sanctions, encompassing monetary fines and imprisonment, for violations of these provisions, aligning with international best practices in cybersecurity regulation[203]. The explicit articulation of offenses and corresponding penalties is a significant strength of the Act, demonstrating a commitment to deter malicious activities. However, the ultimate effectiveness of the legislation hinges on the successful implementation and enforcement of its provisions. A lacklustre approach to enforcement may undermine the Act's aim. On the other hand, effective enforcement can only be performed by avoiding harassment, invasion of privacy, abuse of office, and extortion of legitimate internet users. Enforcement, on the other hand, must be distinguished by a desire for responsibility, sincerity, rigour, and steadfastness in the Act's execution and administration in order for it to be effective.

The *Cybercrimes (Prohibition, Prevention Etc.) Act of 2015* has not yet resulted in any convictions, but there are a few cases under trial over the Act's enforcement. *The Economic and Financial Crimes Commission v. Azeez Fashola (Naira Marley)* case is one example[204]. Eleven counts of offences that bordered on online fraud were brought against the defendants. The defendant committed the charges on various dates between November 26, 2018, and December 11, 2018, as well as May 10, 2019, according to the EFCC. According to the Commission, Fashola and his associates planned to swindle their victims by using various Access Bank ATM cards. The accused was also charged of possessing fake credit cards that belonged to other persons with the intention of defrauding them, which was theft. According to the anti-graft agency, the acts violated *sections 23(1)(b), 27(1), and 33(9) of the 2015 Cyber Crime (Prohibition, Prevention, etc.) Act*.

[203] Ibrahim Abubakar, 'Cybercrime Regulation in Nigeria: An Analysis of the Cybercrimes Act 2015'. *Journal of International Commercial Law and Technology* [2017] (12) (2) 43-55.
[204] The case filed at the Federal High Court has suit number FHC/L/178c/19.

At the resumed sitting on February 27, 2021, the prosecution, through its second prosecution witness (PW2), Augustine Anosike, an investigator and forensic expert with the Economic and Financial Crimes Commission (EFCC), tendered a compact disc (CD) containing extracted data, analysis, and extractions from the defendant's phone. Anosike, building on his previous testimony, revealed that forensic analysis of Naira Marley's iPhone yielded damning evidence, which was subsequently extracted, documented, and compiled onto the CD for evidentiary purposes.

In order to determine if the documents presented to the court may be used as evidence against the accused, the judge postponed the case. We anticipate that, in accordance with the recently passed *Cybercrime (Prohibition, Prevention, etc.) Act of 2015*, the court will render a decision in this matter for the first time. However, the problem of cybercrime remains unabated, notwithstanding the success of this Act. In actuality, the crime has become more complex and multifaceted. This is ascribed to Nigeria's growing "get rich quick" mentality and the absence of a worldwide census to address the threat of cybercrime. The anonymity of cybercriminals' identities continues to be one of the biggest obstacles to international attempts to stop the cybercrime epidemic. Because of the unrestricted availability of information and communication, cybercriminals are able to conceal their identities using various telecommunications devices, making it impossible to track down a user's online Internet Protocol (IP) address. The use of VPN, Psiphon, Tor, and other similar programs is a good example. Furthermore, since the identity of a cybercriminal is unknown to the owner or operator of an Internet service provider, the following obstacle cannot be overcome even if the IP address of a cybercriminal is linked to a specific location[205].

[205] EFG Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy.' *Journal of Internet and Information Systems* [2016] (6) (1) 1-12.

4.3 Challenges and Limitations of Prosecuting Cybercrime in Nigeria and the Need for a Paradigm Shift

4.3.1 Jurisdictional and Procedural Hurdles in Enforcement

Cybercrime exhibits distinct characteristics that differentiate it from traditional terrestrial crimes. Its unique nature is marked by borderless and transnational reach, defying geographical constraints. Unlike conventional crimes confined to a specific locale, cybercrimes transcend territorial boundaries, affecting victims globally[206].

The enforcement of the *Nigerian Cybercrimes Act, 2015*, is significantly impeded by jurisdictional complexities. Although *Section 50* of the Act purports to provide a solution to this issue, the reality is more nuanced, revealing inherent challenges that undermine the efficacy of the legislation.

According to *Section 50 (1) (c)* of the Act, Nigeria retains jurisdiction to conduct trials over her nationals or residents for offences committed abroad, provided that the act in issue constitutes an offence under the law of the country where the offence occurred. This is referred to as the dual criminality principle.

However, a critical quandary arises when a Nigerian citizen's or resident's conduct constitutes an offense under the *Cybercrime Act of 2015*, yet remains permissible under foreign law. Specifically, *Section 50 (i) (c)* of the Act presents a formidable obstacle to enforcement,

[206] Brenner Susan, 'Cybercrime: Investigating High-Technology Computer Crime'. *Information Science Reference* [2010] 12. doi: 10.4018/978-1-59904-887-3.

highlighting the need for clarity on jurisdictional boundaries and harmonization with international laws[207].

4.3.2 Capacity Deficits in Regulation

The widespread use of the internet is becoming more and more global. Stated differently, cybercrime is a worldwide problem. The rapid global dispersal of cybercrime's geographic areas is being driven by the expansion of broadband infrastructure and the rise in the skills needed to commit cybercrime. The expertise of cybercrime cannot be compared to Nigerian enforcement authorities, which are only government officers lacking the necessary abilities, because cybercriminals are experts in computer and cyberspace issues. They typically provide their services without adequate security and protection, are poorly compensated, and lack proper training. This is a significant disadvantage in the jet age. As a result, there is a great need for skilled individuals who are knowledgeable about the process of acquiring evidence.

The old criminal justice system[208] to which we are all accustomed in Nigeria is complicated and often unfamiliar with information and communication technology. It takes skilled professionals to handle crimes involving these gadgets throughout the investigative stage, prosecution, and legal proceedings. This is hardly something Nigeria can brag about. As a result, capacity building in this area is critically needed.

The existence of numerous national and international legal systems presents another difficulty for the Act's execution. Every level of the legal system has distinct requirements for measuring

[207] Aside this, fear of inhuman treatment is also a bar to extradition and this basically includes torture, and degrading punishment which are likely to be meted out to the defendant. See *Soering v. The United Kingdom* (1989) European Court of Human Rights; Extraterritorial responsibility under Article 3 EHRC establishes a legal barrier on deportation or extradition if there are substantial grounds for believing that there is a real risk of treatment contrary to *Article 3*; *Othman (Abu Qatada) v. United Kingdom* 81 39/09 (2012) ECHR 56.
[208] Jose Grabiel Cordova and Others, *Law Versus Cybercrime* (Global Jurist 2018) 4.

cybercrime, which might lead to legal loopholes that allow immunity based on territoriality[209]. The point here will become evident if we take a serious look at the cyber-content crimes covered by the Act. *Section 23* of the Act, for instance, undoubtedly addresses child pornography. The issue is that there are a number of ways to define pornography; some jurisdictions permit the creation and dissemination of various forms of pornography, while others forbid the use of minors in pornography, and still others forbid the creation and dissemination of pornography in any form. The same behaviour is treated differently under these several laws. Each nation's values and features determine this predicament. Effective cybercrime laws depends on international cooperation, therefore this legal discrepancy may make it more difficult for the 2015 Cybercrime Act to function as intended.

4.3.3 The Evidentiary Conundrum

Electronic evidence is used to unravel cybercrime incidents. Dealing with such evidence presents a variety of difficulties, particularly given that the process of investigating cybercrimes must be conducted within cyberspace, where data can be altered or vanish in a matter of seconds[210]. Therefore, in the majority of situations, the capacity to properly identify and punish an offender depends on the proper gathering and analysis of electronic evidence. In Nigeria, this is a significant challenge. Due to limited resources and outdated technology, law enforcement agencies in Nigeria often struggle to effectively collect and analyze electronic evidence[211]. This challenge is exacerbated by the lack of adequate resources, training, and technology for law enforcement agencies to effectively collect and analyze electronic evidence. As a result,

[209] *Ibid*, 4.
[210] S Adebayo Oluwaseun and O Olabode Sunday, 'Challenges of Electronic Evidence in Cybercrime Investigation in Nigeria'. *Journal of International Technology and Information Management* [2020] (29) (1) 1-15.
[211] *Ibid*

cybercriminals in Nigeria often operate with impunity, making it crucial for the government to invest in improving capabilities in this area.

4.4 Cybercrime Prevention: A Comparative Study of Legislative Frameworks and Enforcement Mechanisms in Selected Jurisdictions:

4.4.1 Cybercrime Prevention: The USA Paradigm

The United States' federal system necessitates a multifaceted approach to computer crime legislation, with laws enacted at both state and federal levels[212]. Notably, the *Computer Fraud and Abuse Act (CFAA) of 1986* constitutes a foundational federal statute. This law has been amended and expanded as internet technology advanced, and it continues to form the basis for federal prosecutions of computer-related criminal activities[213].

The Act makes obtaining financial or credit information through a computer a crime. Before the Act was put in place, there was not much that could be done for computer fraud in the United States of America. Not only did this Act help fight against computer fraud, but it also acted against the use of computers as a means of inflicting damage on other computing systems[214]. The *Computer Fraud and Abuse Act (CFAA)*[215] makes it illegal for anyone to distribute computer code or place it in the stream of commerce if they intend to cause either damage or economic loss. The Computer Fraud and Abuse Act prioritizes the mitigation of computer system damage and associated economic losses, imposing criminal penalties for the intentional or reckless

---

[212] SW Brenner, 'State Cybercrime Legislation in the United States of America: A Survey'. *Rich. J. L. & Tech.* [2001] (7) 28.
[213] S Eltringham, 'Prosecuting Computer Crimes', *Computer Crime and Intellectual Property section, Office of Legal Education, Executive Office for United States Attorneys*, available at: <https://www.justice.gov/criminal/file/442156/download> accessed 18 October 2024.
[214] C Doyle, 'Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.' *Congressional Research Service* [2014] 1.
[215] Computer Fraud and Abuse Act 1986, 18 U.S.C. *section 1030*.

dissemination of computer viruses within interstate commerce frameworks[216]. Specifically, violations under this Act can incur substantial sanctions, including prison sentences of up to 20 years and fines reaching $250,000[217]. Notably, the development and possession of harmful computer code do not, in themselves, constitute criminal acts; however, the utilization of such code can precipitate criminal liability. The purpose of each major subsection of the *Computer Fraud and Abuse Act* is to provide an explanation of a specific facet of cybercrime. The *Computer Fraud and Abuse Act*, explained simply, forbids: (a) unauthorised access to a computer and subsequent transmission of secret government information[218]; (b) theft of financial information[219]; (c) accessing a "protected computer"[220]; (d) Computer fraud[221]; (e) transferring code that causes damage to a computer system[222]; (f) trafficking in computer passwords with the intention of affecting interstate commerce or a government computer[223] and (g) Computer extortion[224].

The September 11, 2001 terrorist attacks constitute a pivotal moment in the history of computer crime in America. Although the attacks themselves were not directly related to computer crime, they precipitated the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) in

[216] CFAA 1986, 18 U.S.C., ss 1030(c).
[217] *Ibid*
[218] *Section 1030(a) (1).*
[219] *Ibid, Section 1030(a) (2).*
[220] *Ibid, Section 1030(a) (3).*
[221] *Ibid, Section 1030(a) (4).*
[222] Ibid, *Section 1030(a) (5).*
[223] Ibid, *Section 1030(a) (6).*
[224] *Ibid, Section 1030(a) (7).*

2001. This legislation significantly enhanced the authority of government agencies to combat computer crime, leveraging expanded powers to intercept and obstruct terrorism[225].

The *Computer Fraud and Abuse Act of 1986* was substantially modified by the National Information Infrastructure Protection Act of 1996, which was signed into law by then-President Clinton. Its definition of a "protected computer" was broadened to include any computer with an internet connection[226]. It makes using government computers to access private information, such a person's tax or medical records, illegal. The offence of using a computer to distribute private information will be prosecuted against violators[227]. Additionally, the Act stiffened the penalties for offences established by the *1986 Computer Fraud and Abuse Act*. Violators of the National Information Infrastructure Protection Act of 1996 can face hefty fines and even imprisonment for their actions. This updated legislation aimed to better protect individuals' personal information and prevent cyber crimes from occurring.

4.4.2 Cybercrime Prevention: The UK Paradigm

After a Law Commission report on computer misuse revealed that the UK was lagging behind many EU member states in terms of technological advancement, the *Computer Misuse Act 1990 (CMA) was implemented in August 1990*[228]. The Act includes provisions to protect computer materials from unauthorised access or alteration, as well as for related purposes. Three new offences were added to the criminal code of the United Kingdom. These are:

[225] USA PATRIOT Act 2001, Explanatory Memorandum.
[226] National Information Infrastructure Protection Act 1996, *Section 201*.
[227] *Ibid, Section 201.*
[228] N Macewan, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future.' *Criminal Law Review* [2008] 955.

a) Unauthorised access to computer material[229];

b) Unauthorised access with intent to commit another offense[230];

c) Unauthorised acts with the intent or recklessness to harm computer operation[231].

The core concept of hacking, in which an individual causes a computer to execute a function while intending to access a program or data stored in a computer, is covered under the offence of unauthorised access to computer material[232]. The sole element of this offence is unauthorised access to computer material and awareness of the lack of authority to access the material[233]. No intention is required for this crime to be committed; as long as there was unauthorised access with awareness that it was not authorised, the crime has occurred. *Section 17(5) of the Computer Misuse Act 1990* provides some advice on what constitutes 'not being authorised', stating that if the defendant was not entitled to the type of access in question and did not consent to it, entry is unauthorised[234]. In *Ellis v. DPP* (No. 1)[235], the legal question was whether an ex-student's use of a log-in terminal while aware he was barred might be considered "unauthorised" under section 1. Lord Woolf CJ held that the access was nonetheless unauthorised, and that the legislative prohibitions were broad enough to cover the appellant's usage of the computers. Additionally, the House of Lords ruled in *R v. Bow Street Magistrates and Allison*[236], that insider hackers would be held accountable under section 1 of the Computer Misuse Act 1990 in cases where the employer explicitly outlined the boundaries of the employee's permission to access programs or data and the employee went beyond those boundaries.

---

[229] Computer Misuse Act 1990, *Section 1*.
[230] *Ibid, Section 2.*
[231] *Ibid, Section 3.*
[232] *Ibid, Section 1.*
[233] *Ibid*
[234] *Ibid, Section 17(5).*
[235] [2001] EWHC Admin 362.
[236] [2000] 2 A.C. 216.

Unauthorised access to computer material with the aim to conduct or assist in the commission of additional offences is punishable under *Section 2* of the Act[237]. The main idea is that if someone commits an infraction under *section 1* of the Act[238] with the intent to conduct or assist in the commission of additional offences, they will face additional criminal penalties. *Section 2* defines "further offences" as those that carry a legal penalty or for which a person convicted of the offence faces a minimum sentence of five years in prison[239].

For the purposes of this section, it makes no difference whether the subsequent crime is committed on the same day as the unauthorised access offence or on a later date[240]. A person may be guilty of an offence under this section even if the facts make the conduct of a subsequent offence impossible[241]. *Section 3 of the Computer Misuse Act 1990* was changed by the *Police and Justice Act of 2006*. Its goal was to combat computer viruses and denial of service attacks, which can have disastrous consequences for the organisations attacked. Even if the denial of service is merely momentary, for instance, the crime is still committed and does not need to be directed at a specific computer, program, or data[242].

As a result, the substantial Crime Act of 2015 created a new offence of "unauthorised acts causing, or creating risk of, serious damage"[243]. A person is guilty of 'unauthorised acts causing, or creating risk of, serious damage' if:

(a) the person does any unauthorised act in relation to a computer;

(b) the person knows that the act is unauthorised at the time of doing the act;

---

[237] Computer Misuse Act 1990.
[238] *Ibid*
[239] *Ibid*
[240] *Ibid, Section 2(3).*
[241] *Ibid, Section 2(4).*
[242] The Police and Justice Act 2006, chapter 48 in force on October 1st 2008.
[243] The Computer Misuse Act 1990, s 3ZA.

(c) the act causes, or creates a significant risk of, serious material damage; and

(d) the person intends to cause serious material damage or is reckless as to whether such damage is caused[244].

For the purposes of this offence, "material kind" damage is defined as: (a) damage to human welfare in any place; (b) damage to the environment in any place; (c) damage to any country's economy; or (d) damage to any country's national security[245]. The territorial reach of computer abuse has also been expanded, which means that a UK national can still be charged with an offence if the computer misuse occurred outside of the UK, as long as it was illegal in the country where the hacking occurred[246].

Unauthorised access to computer material carries a maximum penalty of two years in prison and/or a fine under the *Computer Misuse Act 1990*. Unauthorised access with the intent to commit or facilitate the commission of additional offences carries a maximum penalty of five years in prison and/or a fine, unauthorised modification of computer material carries a maximum penalty of ten years in prison and/or a fine, and violation of *section 3ZA* carries a maximum penalty of life in prison and/or a fine. The *Computer Misuse Act of 1990* has been updated to ensure that hackers, who initiate significant assaults, such as on essential infrastructure, face life in a prison sentence[247]. The amendments to the act also include harsher penalties for those who engage in cyber attacks that cause serious harm or disruption to critical services, depicting how essential it is to have strong legislation in place to deter and punish those who seek to exploit vulnerabilities for malicious purposes.

---

[244] Serious Crime Act 2015; the Computer Misuse Act 1990, *Section 3ZA*.
[245] *Ibid*
[246] The Serious Crime Act 2015; The Computer Misuse Act 1990.
[247] O Solon, 'U.K Law Introduces Life Sentence for Cyber Criminals' (2014) available at <https://www.wired.com/story/cybercrime-bill-life-sentence/> accessed 12 October 2024.

4.4.3 Cybercrime Prevention: The South African Paradigm

Cybercrime prevention in South Africa has evolved significantly over the years, reflecting the country's commitment to combating this burgeoning threat[248]. The South African paradigm is characterized by a multifaceted approach, integrating legislative, technological, and societal measures to mitigate cybercrime risks[249]. Notably, the *Electronic Communications and Transactions Act 25 of 2002 (ECT Act)* and the *Cybercrimes Act 19 of 2020* provide the legislative framework for cybercrime prevention, aligning South Africa with international best practices[250]. Furthermore, the National Cybersecurity Policy Framework (2011) outlines the country's strategic objectives for cybersecurity, emphasizing the importance of cooperation between government, private sector, and civil society[251]. This integrated approach enables South Africa to effectively address the complexities of cybercrime.

Effective cybercrime prevention in South Africa also relies on collaborative efforts between government agencies, private sector stakeholders, and civil society organizations[252]. The South African Police Service (SAPS) has established specialized units, such as the Cybercrime Investigation Unit, to investigate and prosecute cybercrimes[253]. Furthermore, public-private partnerships, like the South African Banking Risk Information Centre (SABRIC), facilitate

---

[248] T Mothibi, 'Cybercrime in South Africa: An overview'. *Journal of Contemporary Management* [2018] (15) (2) 193-206.
[249] South Africa, ECT Act (Electronic Communications and Transactions Act No 25 of 2002. Available at <http://www.acts.co.za/ect_act/> accessed 10 October 2024.
[250] South Africa, Cybercrimes Act 19 of 2020; United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (United Nations Publications, New York 2013) 12-15.
[251] South Africa, *National Cybersecurity Policy Framework* (Department of Communications, Pretoria 2011) 5.
[252] R Naidoo, 'Public-Private Partnerships in Cybercrime Prevention: A South African Perspective'. *Journal of Financial Crime* [2019] (26) (4) 1048-1058.
[253] South African Police Service, *Cybercrime Investigation Unit* [2020]. Available at <https://www.saps.gov.za/> accessed 19 October 2024.

information sharing and coordination to combat cyber-enabled financial crimes[254]. These initiatives demonstrate South Africa's proactive stance against cybercrime, echoing the sentiments of Kruger et al.[255], who emphasize the importance of collaboration in cybersecurity. Additionally, research has shown that cybersecurity awareness programs targeting individuals and small and medium-sized enterprises (SMEs) are crucial in preventing cybercrime[256].

Research-informed strategies are crucial in enhancing South Africa's cybercrime prevention capabilities[257]. Studies have highlighted the importance of adopting advanced technologies, such as artificial intelligence and machine learning, to bolster cybercrime detection and response[258]. Moreover, the implementation of robust cybersecurity measures, including encryption and secure protocols, can significantly reduce the risk of cybercrime[259]. By integrating these evidence-based approaches, South Africa can fortify its cybercrime prevention framework, ensuring a safer digital environment for its citizens and businesses. As Mothibi[260] notes, a comprehensive cybercrime prevention strategy requires ongoing evaluation and adaptation to stay ahead of emerging threats. This proactive approach will not only mitigate the impact of cybercrime but also build resilience within the country's digital infrastructure.

---

[254] South African Banking Risk Information Centre (2020). Available at <https://www.sabric.co.za/> accessed 19 October 2024.
[255] H Kruger, WD Kearney and A Rossouw, 'Cybersecurity Awareness in South Africa: A Survey'. *Journal of Information Security* [2019] (10) (2) 143-56.
[256] M Maree and A Marnewick, 'Cybersecurity Awareness among SMEs in South Africa'. Journal of Cybersecurity [2016] (2) (1) 1-10.
[257] *Ibid*, at note 77.
[258] S Barnes, 'Artificial Intelligence and Machine Learning in Cybersecurity'. *Journal of Cybersecurity* [2020] (6) (1) 1-12.
[259] International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology - Security Techniques - Information Security Management Systems – Requirements (ISO Publications, Geneva) 10-12.
[260] T Mothibi, 'Cybercrime in South Africa: An Overview'. *Journal of Contemporary Management* [2018] (15) (2) 193-206.

4.5 The Imperative for a Paradigmatic Shift in Legal Approaches and Governance: Lessons from USA, UK, and South Africa

4.5.1 Insights from US Cyber Governance

Nigeria can draw valuable lessons from the United States' approach to cybercrime prevention. The U.S. has a multifaceted system, with laws enacted at both state and federal levels, which has been effective in combating cybercrimes[261]. The *Computer Fraud and Abuse Act (CFAA) of 1986*, amended by the *National Information Infrastructure Protection Act of 1996*, provides a comprehensive framework for prosecuting cybercrimes. This legislation has been instrumental in mitigating computer system damage, economic losses, and protecting sensitive information. Nigeria can benefit from enacting similar legislation, addressing unauthorized access, theft of financial information, computer fraud, and computer extortion. Additionally, establishing international cooperation, capacity building, and training programs for law enforcement agencies, and encouraging private sector partnerships would enhance Nigeria's cybercrime prevention efforts. Furthermore, Nigeria should consider establishing a national cybercrime reporting system[262], similar to the U.S. Internet Crime Complaint Center (IC3), to facilitate incident reporting and tracking.

4.5.2 Insights from UK Cyber Governance

Nigeria can draw valuable lessons from the UK's *Computer Misuse Act 1990*, which provides a comprehensive framework for combating cybercrime. To enhance its own cybercrime prevention efforts, Nigeria can establish clear definitions of cybercrimes, implement a tiered penalty system,

[261] Goodman Marc, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It* (Doubleday 2015).
[262] RO Akinyemi, 'Cybercrime and National Security in Nigeria'. In *Cybersecurity and Digital Forensics for Decision Makers* (Springer Nature 2019) 137-154.

and foster international cooperation to combat transnational cybercrimes. This includes adopting provisions similar to *Section 1-3 of the UK Act*, which address unauthorized access, modification, and distribution of malicious software[263]. Furthermore, Nigeria can benefit from creating specialized cybercrime units within law enforcement agencies, launching public awareness campaigns to educate citizens about online security best practices, and engaging stakeholders from government, private sector, and civil society in developing holistic strategies against cybercrime. By adopting these measures and updating its laws to address emerging threats, Nigeria can strengthen its cybercrime prevention framework, protect its digital landscape, ensure a safer online environment for citizens and businesses, and align with international standards. Effective implementation would require training law enforcement, judiciary, and stakeholders on the dynamic nature of cybercrime and fostering collaboration with international partners to stay ahead of emerging threats.

4.5.3 Insights from South African Cyber Governance

Nigeria can draw valuable lessons from South Africa's comprehensive approach to cybercrime prevention, characterized by a multifaceted strategy integrating legislative, technological, and societal measures to mitigate cybercrime risks. By adopting South Africa's legislative framework, notably the *Electronic Communications and Transactions Act 25 of 2002* and *Cybercrimes Act 19 of 2020*, Nigeria can align with international best practices, while establishing specialized units like the Cybercrime Investigation Unit to efficiently investigate and prosecute cybercrimes. Furthermore, Nigeria can benefit from South Africa's collaborative efforts between government agencies, private sector stakeholders, and civil society organizations, as seen in public-private partnerships like the South African Banking Risk

[263] David Bainbridge, *Information Technology Law: The Law and Society* (Oxford University Press 2018).

Information Centre (SABRIC), facilitating information sharing and coordination to combat cyber-enabled financial crimes. Additionally, Nigeria can implement targeted cybersecurity awareness programs for individuals and small and medium-sized enterprises (SMEs), leveraging research-informed strategies and advanced technologies like artificial intelligence, machine learning, and robust cybersecurity measures, including encryption and secure protocols, to significantly reduce cybercrime risks. Moreover, Nigeria can develop a National Cybersecurity Policy Framework, similar to South Africa's 2011 framework, outlining strategic objectives for cybersecurity and promoting cooperation between government, private sector, and civil society, while engaging in regional cooperation with neighboring countries and international organizations to enhance cybercrime prevention capabilities. By integrating these evidence-based approaches, Nigeria can fortify its cybercrime prevention framework, ensuring a safer digital environment for citizens and businesses, and driving economic growth in the digital economy.

4.5.4 Implementing Effective Cyber Governance

A comprehensive response to cybercrimes necessitates a multi-faceted approach to network security, encompassing robust network architecture and software, advanced encryption methodologies, stringent data protection legislation, adherence to established information security standards, and the deployment of cutting-edge threat protection and detection tools.[264] Cybercriminals exploit gaps in existing legislation to evade detection and prosecution; therefore, it is imperative that every legal system takes proactive measures to ensure its penal and procedural laws are sufficiently robust to address the complex challenges posed by cybercrimes. This necessitates a continuous review and refinement of legal frameworks to keep pace with the

[264] O Ukwueze Emmanuel and C Chinedu Obuka, 'Legal Framework for the Regulation of Electronic Fraud in Nigeria'. *Law and Policy Review* [2011] 75.

evolving nature of cyber threats and ensure effective prosecution and punishment of cybercriminals.[265]

The global mobility of computer data in international networks necessitates international solutions to combat cybercrime. National strategies alone would be insufficient, as they could create data havens and undermine security. A collaborative international framework is essential to address the transnational nature of cybercrime and provide robust protection.[266] To safeguard personal information and financial security in the digital realm, it is vital to authenticate the identity of online recipients and scrutinize account activity and monthly statements with precision, verifying the accuracy of all transactions to prevent potential cyber threats.

[265] N Ani Lawrence, 'Cyber Crime and National Security: The Role of the Penal and Procedural Law'. *Journal of International Law and Cybercrime* [2017] (1) (1) 34-51.
[266] T Adebiyi, 'Internet/Computer-Related Crimes'. *The Advocate, Journal of the Students Representative Council, Nigerian Law School, Lagos Campus* [2003/2004] (2) 81-96.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This study critically analyzed the Cybercrime (Prohibition, Prevention, etc.) Act 2015, Nigeria's primary legislation combating cybercrime, and benchmarked it against international best practices in the USA, UK, and South Africa.

The key findings of the study are:

1. The Act establishes a foundational framework for combating cybercrime, encompassing offenses such as hacking, cyber-stalking, and online fraud.
2. The legislative definition of cybercrime requires clarification to accommodate emerging threats.
3. Law enforcement agencies face substantial challenges in investigating and prosecuting cybercrime cases due to resource deficiencies, inadequate training, and limited awareness.
4. Variations exist between Nigeria's cybercrime definition and those employed in the USA (Computer Fraud and Abuse Act), UK (Computer Misuse Act 1990), and South Africa (Electronic Communications and Transactions Act 2002).
5. Provisions pertaining to data protection and privacy in Nigeria's Act are less comprehensive compared to the UK's Data Protection Act 2018 and the USA's Privacy Act of 1974.

6. Effective combating of transnational cybercrime necessitates robust international cooperation and collaboration, as exemplified by the USA's and UK's partnerships with international organizations.
7. Nigeria's Act lacks specific provisions addressing emerging cyber threats, such as cryptocurrency-related crimes, whereas the USA and UK have implemented targeted regulations.
8. Judicial processes are characterized by protracted delays, hindering expeditious prosecution of cybercrime cases.
9. Public awareness and education initiatives targeting cybercrime prevention are presently insufficient.
10. Regular updates and reviews are necessary to ensure the Act remains effective in addressing evolving cybercrime landscapes.

These findings highlight areas for improvement in Nigeria's cybercrime legislation and enforcement, emphasizing the need for alignment with international best practices, enhanced law enforcement capacity, and strengthened data protection and privacy provisions.

5.2 Conclusion

The worldwide nature of cybercrime necessitates international cooperation, regardless of how successful a country's domestic laws may be. National and international law enforcement must work together and independently, as well as implement strong corporate information security safeguards. This could be done to get evidence of crime or to apprehend the criminals themselves. However, conflict between competent authorities is a serious issue in worldwide efforts to combat the pandemic. Along with this, there is a lack of a standardized definition of

cybercrime, as well as challenges in acquiring and using evidence and detecting cybercrime crimes. Also, as commendable as the Act's provisions are, the near-complete dependence on punishment as the sole means of combating computer cybercrime is a fundamental flaw that the Nigerian government must address immediately. Over the years, it has been demonstrated that prevention is an essential component in an effective fight against cybercrime. Technical solutions (such as firewalls that prevent unauthorised access to a computer system and antivirus software that prevents the installation of harmful software) to the banning of access to illicit content are examples of such measures. Furthermore, investing in education and awareness campaigns to teach individuals about safe online practices and potential threats is crucial in preventing cybercrime. It is also important for the government to work closely with international partners and law enforcement agencies to track down and prosecute cybercriminals operating across borders. By implementing a more comprehensive approach that includes prevention, detection, and punishment, Nigeria can better protect its citizens and businesses from the growing threat of cybercrime.

The point being made here is expressed clearly in the Pacific Island Draft Model Policy for cybercrime[267] in the following words: “In addition to the criminalization of cybercrime and the improvement of the ability of law enforcement to combat cybercrime, crime prevention measures need to be developed within the process of developing such measures, that can range from technical solutions to increasing user awareness, it is important to identify those groups that require specific attention such as youth, technologically challenged people (such as people from isolated villages that are technologically unaware) and women.”

[267] The approved documents related to the projects are available at <www.itu/ITU-D/projects/ITUECACP/icbAPis/index.html> accessed on 20 October 2024.

However, crime prevention measures should also apply to more advanced users and technologies, encompassing affiliate players such as critical infrastructure providers (such as tourism and financial sectors). The debate about necessary measures should include the whole range of instruments, including awareness-raising initiatives, making available and promoting free-of-charge protection technologies (such as antivirus software), and the implementation of solutions to enable parents to restrict access to certain content. Ideally, these safeguards should be in place when a service or technology is introduced and should remain in place for the duration of its use. A wide range of stakeholders, including internet service providers, governments, and regional organisations, should be included in order to guarantee that such measures have a wider reach. Additionally, different funding sources should be investigated.

5.3 Contributions to Knowledge

This study contributes significantly to the body of knowledge on cybercrime legislation in Nigeria, particularly in relation to the Cybercrime (Prohibition, Prevention, etc.) Act 2015. By conducting a critical analysis of the Act, this research fills a gap in existing literature on the effectiveness of Nigeria's cybercrime laws. The findings provide useful insights into the strengths and weaknesses of the Act, throwing light on its impact on digital economy growth, e-commerce, and online freedom in Nigeria.

The study's evaluation of the Act's alignment with international best practices and standards in cybercrime legislation offers a strong understanding of Nigeria's position within the global cybercrime landscape. The identification of gaps and loopholes in the existing legal framework provides a foundation for future research and policy reforms. Furthermore, this research

contributes to the ongoing discourse on balancing cybersecurity with individual rights and freedoms, particularly in the context of data protection and surveillance.

This study also enhances scholarship on cybercrime law and digital governance in Africa, offering implications for policymakers, practitioners, and researchers. The recommendations for capacity building, public awareness, and education contribute to the development of a comprehensive framework for combating cybercrime in Nigeria. By examining emerging cybercrime threats and trends, this research informs strategies for future-proofing Nigeria's cybercrime legislation.

Ultimately, this study advances understanding of Nigeria's cybercrime legislation and its implications, addressing a critical research gap in the field. The findings and recommendations provide a valuable resource for stakeholders seeking to strengthen Nigeria's cybercrime laws and enhance digital governance.

5.4 Areas for Further Studies

Further research is warranted to explore the intricacies of Nigeria's cybercrime landscape. One potential area of investigation is a comparative analysis of cybercrime laws in African countries, shedding light on best practices and areas for regional cooperation. Additionally, evaluating Nigeria's compliance with international cybercrime conventions, such as the Budapest Convention, would provide valuable insights into the country's alignment with global standards.

The intersection of technology and cybercrime also necessitates further exploration. Studies could examine the effectiveness of digital forensic tools in investigating cybercrimes in Nigeria, as well as the challenges faced by law enforcement agencies in collecting digital evidence.

Moreover, the development of a framework for digital evidence management in Nigerian courts would contribute significantly to the enhancement of cybercrime prosecutions.

The socioeconomic and cultural factors influencing cybercrime perpetration in Nigeria merit further investigation. Research could delve into the social and cultural factors driving cybercrime, as well as the economic impact of cybercrime on Nigerian individuals and businesses. Furthermore, examining the role of public perception and awareness in preventing cybercrime would inform evidence-based strategies for cybercrime prevention.

The rapidly evolving nature of cyber threats necessitates research into emerging technologies and their implications for cybercrime. Studies could explore the impact of emerging technologies, such as artificial intelligence and blockchain, on cybercrime risks and opportunities. Moreover, investigating the implications of 5G networks on cybercrime would provide critical insights into the future of cybersecurity in Nigeria.

International cooperation and capacity building are crucial components of effective cybercrime prevention. Future research could analyze international cooperation in combating cybercrime, focusing on Nigeria's partnerships with countries and regional organizations. Assessing capacity building programs for law enforcement and judiciary would also inform strategies for enhancing Nigeria's cybercrime response.

Empirical studies would provide valuable contributions to the existing literature. Surveys of cybercrime victims' experiences and perceptions in Nigeria, analyses of cybercrime trends and patterns, and case studies of high-profile cybercrime cases would all enhance understanding of Nigeria's cybercrime landscape.

The above areas offer fertile ground for further research, policy development, and practical applications to strengthen Nigeria's cybercrime prevention and response efforts.

5.5 Recommendations

There is little doubt that cybercrime has had a significant impact on international trade and economic operations. As the usage of the internet has increased exponentially, so have the efforts of unscrupulous individuals to swindle innocent users in cyberspace. The scourge of cybercrime impacts individuals, businesses, and countries, making it a significant danger to nations' economic and financial security, which is why all countries prohibit it. Nigeria has enacted the *Cybercrimes (Prohibition, Prevention, etc) Act 2015*, as well as other legislations, in order to combat the country's growing cybercrime prevalence. This study looked at the Nigerian Cybercrimes Act and other legislations dealing with cybercrime in Nigeria. The study concluded that, in spite of the Cybercrimes Act's innovative measures, the nation's cybercrime rate has not significantly decreased. Given the poor adoption of the Act in combating cybercrime in Nigeria, the study provides the following recommendations:

a) The Nigerian people should be informed about how computer systems and data can be protected. For example, the adoption of anti-virus softwares and passwords by the general public should be encouraged. In some circumstances, a computer system intrusion is disguised so that it appears to have come from a source that is completely unaware of the breach. This is possible because the victim's network lacks complete security measures such as firewalls, passwords, and anti-virus software. The widespread adoption of anti-virus software and passwords would significantly improve computer security.

b) Although *Section 8 of the Cybercrime Act* deals with unauthorised change of computer data, which clearly includes the use of computer viruses to modify computer systems and data, it does not address the manufacture and dissemination of computer viruses. *Section 8 of the Act* should be expanded to more effectively address the manufacturing and propagation of computer viruses, thereby improving computer security and combating cybercrime.

c) Additionally, *section 15 of the Cybercrime Act*, which addresses cyber stalking, should be expanded to include email spam, which is the sending of a significant number of unwanted commercial emails.

d) In order to facilitate the efficient application of the Cybercrime Act, judges should be included in the training provided by *Section 24(3) of the Act*, which deals with the training of law enforcement authorities.

e) The Cybercrime Advisory Council, established under *Section 25* of the Cybercrime Act, requires regular training to stay updated on evolving cybercrime trends and effective prevention/prosecution strategies.

f) In the same way that *section 1030(g) of the Computer Fraud and Abuse Act* provides for compensatory damages and other forms of remedies to victims of cybercriminals in the United States, the Cybercrime Act should be reenacted to do the same.

g) Nigeria's high unemployment fuels cybercrime. To combat this, the government should create jobs and establish IT labs/forums for young people to develop and showcase their skills, fostering employment and IT growth.

BIBLIOGRAPHY

A. TEXT BOOKS

Simester A and Sullivan G, *Criminal Law: Theory and Doctrine*, (3rd edn.: Oxford University Press, 2007).

Akinyemi RO, 'Cybercrime and National Security in Nigeria'. In *Cybersecurity and Digital Forensics for Decision Makers* (Springer Nature, 2019).

Alisdair Gillespie A, *Cybercrime: Key Issues and Debates* (Routledge, 2016).

Ashaolu D, 'Combating Cybercrimes in Nigeria' in D Ashaolu (ed.) *Basic Concepts in Cyberlaw* (Velma Publishers, 2012).

Ashworth A, *Principles of Criminal Law*, (5th edn.: Oxford University Press, 2005).

Brenner Susan W, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Springer, 2012).

David Bainbridge, *Information Technology Law: The Law and Society* (Oxford University Press, 2018).

David Plunkett, 'Robust Normativity, Morality, and Legal Positivism' in David Plunkett, Scott Shapiro & Kevin Toh (eds), *Dimensions of Normativity: New Essays on Metaethics and General Jurisprudence* (Oxford University Press, 2019).

Felix EE and Mark AK, *Handbook on Nigerian Cybercrime Law* (Justice Jeco Printing and Publishing Global, 2018).

Friedmann Wolfgang, *Legal Theory* (Stevens & Son Limited 1953) L dalam Bernard Tanya dkk, Teori Hukum: Strategi Tertib Manusia dalam Lintas Ruang dan Generasi (Genta Publishing 2013).

Goodman Marc, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It* (Doubleday Publishing, 2015).

Hall HW, *Neighborhoods: Their Place in Urban Life* (Sage Publication, 1990).

Ikenga KEO and Ewulum BE, 'Assessing the Nigerian Cyber-Security Law and Policy for Protection of Critical Infrastructure for National Development' in Okeke GN et al. (eds) *Law, Security and National Development* (Amaka Dreams Ltd., 2017).

Iorliam Aamo, *Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime* (Springer International Publishing, 2019).

Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2015).

Jose Grabiel Cordova and Others, *Law Versus Cybercrime* (Global Jurist, 2018).

Kremling J and Sharp-Parker AM, *Cyberspace, Cybersecurity and Cybercrime* (Sage 2018).

M Chawki, Darwish A, Khan MA and Tyagi S, *Cybercrime, Digital Forensics and Jurisdiction* (Springer International Publishing, 2015).

Neff C and Sthepenn A, ‘Short History of International Law, in D dalam Malcolm Evan ‘, *International Law* (1st Edn.) (Oxford University Press 2003).

Oluwatomi Ajayi A, *Internet Technologies and Cybersecurity Law in Nigeria* (Malthouse Press, 2024).

Onoja E, *Fundamental Principles of Nigerian Criminal Law* (Green World Publishing Company Ltd, 2015).

Ormerod D, *Smith and Hogan Criminal Law* (11th edn.: Oxford University Press, 2005).

Protevi John, *The Edinburgh Dictionary of Continental Philosophy* (Edin-burgh University Press, 2005).

Sen A, ‘Capability and Well-being,’ in M Nussbaum and A Sen (eds.), *The Quality of Life* (Clarendon Press 1993).

Sen A, *Commodities and Capabilities* (North-Holland Publishing Company, 1985).

Sherraden M, *Assets and the Poor: A New American Welfare Policy* (ME Sharpe, 1991).

Sherraden M, Curley J and Grinstein-Weiss M, *Wealth Creation and Rural America* (National Rural Funders Collaborative, 2003).

Somit A and Peterson SA (eds.), *The Dynamics of Evolution* (Cornell University Press, 1992).

Tom Campbell, *Prescriptive Legal Positivism: Law, Rights and Democracy* (Cavendish Publishing, 2004).

Wall DS, 'Cybercrimes and the Internet', In DS Wall (Ed.), *Crime and the Internet* (Routledge, 2001).

Zedner L, *Criminal Justice* (Oxford University Press, 2004).

B. JOURNAL ARTICLES

Abayomi Sogunle B, 'Cybercrimes (Prohibition, Prevention etc) Act 2015: Challenges to Enforcement', *Journal of Law and Judicial System* [2021] (4) (1). DOI: <https://doi.org/10.22259/2637-5893.0401001> accessed on 12 September, 2024.

Adebayo OS and Olabode SO, 'Challenges of Electronic Evidence in Cybercrime Investigation in Nigeria'. *Journal of International Technology and Information Management* [2020] (29) (1).

Adebiyi T, 'Internet/Computer-Related Crimes'. *The Advocate, Journal of the Students Representative Council, Nigerian Law School, Lagos Campus* [2003/2004] (2).

Ajayi EFG, 'Challenges to Enforcement of Cyber-crimes Laws and Policy.' *Journal of Internet and Information Systems* [2016] (6) (1).

Akintola KG, Akinyede RO and Agbonifo CO, Appraising Nigeria Readiness for Electronic Commerce Towards Achieving Vision 20:2020, *International Journal of Research and Review in Soft and Intelligent Computing* [2020] (9) (2).

Ani Lawrence N, ‘Cyber Crime and National Security: The Role of the Penal and Procedural Law’. *Journal of International Law and Cybercrime* [2017] (1) (1).

Aransiola JO and Asindemade SO, ‘Understanding Cybercrime Perpetrators and the Strategic they Employed in Nigeria,’ *Cyberpsychology, Behaviour and Social Networking* [2011] (14) (12).

Ashworth A, ‘Is the Criminal Law a Lost Cause?’ *LLQR* [2000] (116).

Awhefeada UV and Bernice OO, ‘Appraising the Laws Governing the Control of Cybercrime in Nigeria’. *Journal of Law and Criminal Justice* [2020] (8) (1).

Barnes S, ‘Artificial Intelligence and Machine Learning in Cybersecurity’. *Journal of Cybersecurity* [2020] (6) (1).

Brenner Susan, ‘Cybercrime: Investigating High-Technology Computer Crime’. *Information Science Reference* [2010]. doi: 10.4018/978-1-59904-887-3.

Brenner SW, ‘State Cybercrime Legislation in the United States of America: A Survey’. *Rich. J. L. & Tech.* [2001] (7).

Chawki M, ‘Nigeria Tackles Advanced Fee Fraud’. *Journal of Information, Law and Technology* [2009] (1) 8.

Doyle C, ‘Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.’ *Congressional Research Service* [2014] 1.

Eboibi FE, ‘A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015’. *Computer Law and Security Review* [2017] (33) (5).

Eboibi FE, ‘Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence’. *Nigerian Law and Practice Journal* [2011] (10).

Eboibi FE, ‘Money Laundering in Nigeria: Implications for National Development’. *Umaru Musa Yar’Adua University Law Journal* [2014] (1) (1).

Ehimen O and Bola A, ‘Cybercrime in Nigeria.’ *Business Intelligence Journal* [2010] (3) (1).

Grant C and Osanloo A, ‘Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for ‘House’’, *Administrative Issues Journal: Connecting Education, Practice and Research* [2014]. DOI: 10.5929/2014.4.2.9

Hassan AB, Lass FD and Makinde J, ‘Cybercrime in Nigeria: Causes, Effects and the Way Out,’ *ARPN Journal of Science and Technology* [2012] (2) (7).

Henry Osborn Quarshie, ‘Cyber Crime in a World without Borders’, *Texila International Journal of Academic Research* [2017] (4) (2). DOI: 10.21522/TIJAR.2014.04.02.Art007

Hirschi T and Gottfredson M, ‘Age and the Explanation of Crime,’ *American Journal of Sociology* [1983] (89).

Hu Y, Chen X and Bose I, ‘Cybercrime Enforcement Around the Globe,’ *Journal of Information Privacy and Security* [2013] (9) (3). Available at: <https://doi.org/10.1080/15536548.2013.10845684> accessed on 2 October 2024.

Ibrahim Abubakar, ‘Cybercrime Regulation in Nigeria: An Analysis of the Cybercrimes Act 2015’. *Journal of International Commercial Law and Technology* [2017] (12) (2).

Ikenga KE Oraegbunam, ‘Admissibility of Electronic Evidence under Section 84 of Evidence Act 2011: Examining the Unresolved Authentication Problem’. *UNIZIK Law Journal* [2015] (11).

Ikenga KE Oraegbunam, ‘Admitting Computer-Based Evidence in Nigeria: Resonances from South Africa, India and United Kingdom’. *The Nigerian Law Journal* [2017] (20) (1).

Izevbuwa OG and Abhavan RN, ‘Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations’, *Journal of Law, Policy and Globalization* [2022] (119). DOI: 10.7176/JLPG/119-01.

Izuakor CF, ‘Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context’. *ISSA Journal* [2021].

Kesiena URHIBO, ‘Combating and Addressing the Menace of Cybercrime In Nigeria: An Overview of Applicable Laws’, *African Journal of Criminal Law and Jurisprudence (AFJCLJ)* [2021] (6) (1).

Kruger H, Kearney WD and Rossouw A, 'Cybersecurity Awareness in South Africa: A Survey'. *Journal of Information Security* [2019] (10) (2).

Kshetri N, 'Pattern of Global Cyber War and Crime: A Conceptual Framework'. *Journal of International Management* [2005] (11) (4).

Macewan N, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future.' *Criminal Law Review* [2008].

Maree M and Marnewick A, 'Cybersecurity Awareness among SMEs in South Africa'. *Journal of Cybersecurity* [2016] (2) (1).

McGuire M and Dowling S, Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications,' *Home Office Research Report* [2013].

Moga E, Salihu AG and Abdulkarim R, 'A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development,' *Journal of Research in Humanities and Social Science* [2021] (9) (9).

Mothibi T, 'Cybercrime in South Africa: An Overview'. *Journal of Contemporary Management* [2018] (15) (2).

Naidoo R, 'Public-Private Partnerships in Cybercrime Prevention: A South African Perspective'. *Journal of Financial Crime* [2019] (26) (4).

Okeshola F and Adeta A, 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria Kaduna State, Nigeria'. *American Journal of Contemporary Research* [2013] (3) (9).

Olayemi O, 'A Socio-Technological Analysis of Cybercrime and Cybersecurity in Nigeria'. *Academic Journal* [2014] (6) (3).

Olayemi OJ, 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria,' *International Journal of Sociology and Anthropology* [2014] (6) (3).

Olujobi OJ and Olujobi OM, 'Re-Thinking and Optimizing Nigeria's Anti-Corruption Legal Framework: Upstream Petroleum Sector Corruption Evaluation'. *Journal of International and Comparative Law* [2020] (8).

Olusola M, 'Cyber Crimes and Cyber Laws'. *The International Journal of Engineering and Science* [2013] 2(4).

Opebiyi FM, 'Protecting the Interest of Buyers in Online Contracts of Sale in Nigeria: Making a Case for Legislative Intervention'. *Elizade University Law Journal* [2018] (1).

Oraegbunam KE, 'Combating Crimes in Cyberspace: Examining the (In) Adequacy of the Criminal Code Act and the Criminal Procedure Act'. *Ebonyi State University Law Journal* [2015] (6) (1).

Oriole T, ‘Advanced Fee Fraud on the Internet’. *Computer Law and Security Report* [2005] (21).

Pradeep MD, ‘Legal Research- Descriptive Analysis on Doctrinal Methodology.’ *International Journal of Management, Technology, and Social Sciences (IJMTS)* [2019] (4) (2). DOI: http://doi.org/10.5281/zenodo.3564954.

Renu P, ‘Impact of cybercrime: Issues and challenges,’ *International Journal of Trending Scientific Research and Development* [2019] (3) (3).

Salim IA, Zuryati MY, and Zainal AA, ‘Legal Research of Doctrinal and Non-Doctrinal,’ *International Journal of Trend in Research and Development* [2017] (4) (1).

Sampson RJ and Byron GW, ‘Community Structure and Crime: Testing Social-Disorganization Theory,’ *American Journal of Sociology* [1989] (94).

Samuele C and DW, ‘On the (in) significance of Hume’s Law’, *Philosophical Studies* [2021].

Sarre R, Lau LYC and Chang LYC, ‘Responding to Cybercrime: Current Trends. Police Practice and Research,’ *An International Journal* [2018] (19) (6).

Sherraden M, ‘Rethinking Social Welfare: Toward Assets,’ *Social Policy* [1988] (18) (3).

Ukwueze EO and Obuka CC, 'Legal Framework for the Regulation of Electronic Fraud in Nigeria'. *Law and Policy Review* [2011].

Williams G, 'The Definition of Crime'. *Current Legal Problems* [1955] (107).

C. CONFERENCE PAPER(S)

Olanrewaju AO and Abraham FA, 'A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria' *A Paper Presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL)* at Halifax, Nova Scotia, Canada [2016] p. 1-11.

D. NEWSPAPER(S)

Premium Times News Report (2023) 'Nigeria losing huge resources to cybercrime – Akpabio'. Available at <https://www.premiumtimesng.com/news/more-news/645665-nigeria-losing-huge-resources-to-cybercrime-akpabio.html?tztc=1> accessed on 17 April 2024.

SaharaReporters (2024) 'Nigeria Lost $500Million to Cybercrime in 2022, Global Loss May Hit $10.5 Trillion By 2025 – EFCC Boss'. Available at <https://bit.ly/4eSrX7e> accessed 20 April 2024.

E MAGAZINES/BULLETINS/REPORTS

Becker G, *Human Capital*, Bureau of Economic Research (1964) p. 47.

Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime (UNDO), February 2013.

Explanatory Report of the Committee of Ministers of the Convention on Cybercrime 109th Session, Adopted on 8 November 2001.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology - Security Techniques - Information Security Management Systems – Requirements (ISO Publications, Geneva) 10-12.

Jonathan Clough, 'Cybercrime', *Commonwealth Law Bulletin* [2011] (37) (4) 671-680, at 675.

South Africa, *National Cybersecurity Policy Framework* (Department of Communications, Pretoria 2011) 5.

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (United Nations Publications, New York 2013) 12-15.

F. INTERNET/WEBSITE CONTENTS

African Union, *African Union Convention on Cyber Security and Personal Data Protection,* Available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 20 April 2024.

Article 3 of the European Convention on Cybercrime, 2000, (CETS No. 185) available at: <http://conventions.co.int> accessed on 15 October, 2024.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 2007, available at <http://conventions.coe.int> accessed on 16 October 2024.

DataReportal, 'Digital 2022: Global Overview Report', available at <https://datareportal.com/reports/digital-2022-global-overview-report> accessed 14 May 2024.

Eltringham S, 'Prosecuting Computer Crimes', *Computer Crime and Intellectual Property Section, Office of Legal Education, Executive Office for United States Attorneys*, available at: <https://www.justice.gov/criminal/file/442156/download> accessed 18 October 2024.

Enhancing Competitiveness in the Caribbean Through ICT Policies, Legislation and Regulatory Procedure 1980, available at <www.itu.int/ITU-D/projects/ITU EC ACP/icb4pis/index.html> accessed on 17 October 2024.

European Union Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography 2003; available at <http://eur-;ex.europe.en/Lexuriserv/site/en/oj/2004/1013/101320040120en004400e8.pdf> accessed on 16 October 2024.

Gbenga Olowu, Cybercrime in Nigeria: Evolution and Forms. Available at <https://www.researchgate.net/publication/368757425_Cybercrime_in_Nigeria_Evolution_and_Forms> accessed 7 Jul 2024.

International Telecommunication Union (ITU), 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (2012) September Report, available at <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> accessed 14 May 2024

Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012) available at: <www.itu.int/ITUD/Cyb/cybersecurity/legislation.htmlatpage21> accessed on 15 October 2024.

Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Available online at <www.itu.int/ITU-D/Cyb/Cybersecurity/legislation.html> accessed on 17 October 2024.

Pacific Island Draft Model Policy for cybercrime available at <www.itu/ITU-D/projects/ITUECACP/icbAPis/index.html> accessed on 20 October 2024.

Prof. Dr. Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, (September 2012), 179. Available at <www.itu.int/ITUD/Cybersecurity/legislation/html.page> accessed on October 17 2024.

Solon O, 'U.K Law Introduces Life Sentence for Cyber Criminals' (2014) available at <https://www.wired.com/story/cybercrime-bill-life-sentence/> accessed 12 October 2024.

South African Banking Risk Information Centre (2020). Available at <https://www.sabric.co.za/> accessed 19 October 2024.

South African Police Service, *Cybercrime Investigation Unit* [2020]. Available at <https://www.saps.gov.za/> accessed 19 October 2024.

Stanford Draft International Convention 1999. Available at <http://media,hoover.org/documents/0871999825 249.pdf> accessed on 15 October 2024.

Statista, 'Number of Internet Users in Nigeria from 2017 to 2026', available at: <https://www.statista.com/statistics/183849/internet-usersnigeria/> accessed 14 April 2024.

Tania U, *Criminology Theories: The Varied Reasons Why People Commit Crime*. Available at: <www.blog. udemy.com> accessed August 12, 2024.

The European Convention on Cybercrime, 2000 and section 7 of the 2002 Commonwealth Model Law, available at <www.thecommonwealth.org/sharedaspfiles/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77=86970A639805%7Computer%20Crime.pdf> (Annex1).

The United Nations, 'The United Nations Convention on the Use of Electronic Communications in International Contracts Enters into Force on 1 March 2013,' *Information Service Vienna.* Available at <https://unis.unvienna.org/unis/pressrels/2013/unisl181.html> accessed on 26 July 2024.

United Nations Conventions on the Rights of the Child (1989), available at <www.g8.gc.ca/genoa/july-22-01-1-e.asp> accessed on 16 October 2024.

United Nations General Assembly, Resolution 56/183: World Summit on the Information Society (2001) available at <https://www.itu.int/net/wsis/documents/background.asp?lang=en&c_type=res> accessed 29 May 2024.

Vuk Mujovic, 'Evolution of Cybercrime: Where Does Cybercrime Come from? The Origin & Evolution of Cybercrime,' (2018). Available at < https://www.le-vpn.com/history-cyber-crime-origin-evolution/> accessed on 28 July 2024.