



NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF INTERNATIONAL LAW

**A COMPARATIVE APPROACH: LEGAL FRAMEWORK OF CYBERCRIME IN
NIGERIA**

LLM. THESIS

YILJWAN BITRET PAN'AN

Nicosia

MAY, 2023

NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF INTERNATIONAL LAW

**A COMPARATIVE APPROACH: LEGAL FRAMEWORK OF CYBERCRIME IN
NIGERIA**

LL.M. THESIS

YILJWAN BITRET PAN'AN

SUPERVISOR


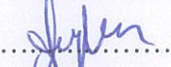

Assist. Prof. Dr. Nabi Berkut

Nicosia

May, 2023

APPROVAL

We certify that we have read the thesis submitted by Yiljwan Bitret Pan'an, titled "A Comparative Approach: Legal Framework of Cybercrime in Nigeria" and that in our combined opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Educational Sciences.

Examining Committee	Name-Surname	Signature
Head of the Committee:	Assist. Prof. Dr. Nabi Berkut	
Committee Member*:-	Dr. Ayten F. O. ben. Fren	
Supervisor:	Assist. Prof. Dr. Nabi Berkut	

Approved by the Head of the Department

...../...../2023




Assist. Prof. Dr. Nabi Berkut

Head of Department

Approved by the Institute of Graduate Studies

...../...../2023



Prof. Dr. Kemal Hüsnü Can Başer
Head of the Institute

DECLARATION

I hereby declare that all information, documents, analysis and results in this thesis have been collected and presented according to the academic rules and ethical guidelines of Institute of Graduate Studies, Near East University. I also declare that as required by these rules and conduct, I have fully cited and referenced information and data that are not original to this study.

Yiljwan Bitret Pan'an

...../...../.....

Day/May/2023

DEDICATION

Dedicated to my extraordinary Parents, Hon. Pan'an Yiljwan and Mrs. Christiana Yiljwan, my outstanding siblings Blessing, Donata and Prosper, my amazing closest friends, and all the victims of cybercrime around the world.

ACKNOWLEDGEMENTS

I want to express my appreciation to the Almighty God for his consistency and reliability during the course of this program. To my parents, Hon. Pan'an Yiljwan and Mrs. Christiana Yiljwan, I am eternally grateful for all their help, guidance, and immeasurable contributions to this work and to my life. My sincere appreciation for you beyond the capacity of any words, but please accept my heartfelt thanks all the same. Thanks especially to Assist. Prof. Dr. Nabi Berkut (my supervisor), whose commitment and thoroughness in the field of teaching in international law and for his supervision not only made this project a better research paper, but also made me a better person. Jude Bamidele Alabi deserves particular thanks for serving as a consistent guide and mentor to me while I worked through my coursework and for serving as the drive and inspiration that ultimately led to the successful completion of this project. To Jacob Luka, Hannaih Samuel, Daspan Luther, and Kinsley Opara, I appreciate your undying support. To Banje Faith, Mary Tagwi, Maryam Yemi, Aisha Alfa and Esther Jatau, thank you for your friendship and advice always. Pastor James Swanson and Rachael Swanson of Lefkosa Protestant Church (LPC) thank you for being my spiritual guides and Parents far away from home. God has given me three wonderful siblings, and I am eternally grateful to each of them, Blessing, Donata, and Prosper. I would also want to express my appreciation to everyone who works at Near east University's International Law Department. In addition to fellow students and anybody else who helped make this research project a success I love you all. Last but not least, I want to give myself a huge round of applause for working so diligently and persistently on my thesis.

Yiljwan Bitret Pan'an

ABSTRACT**A Comparative Approach: Legal Framework of Cybercrime in Nigeria****Yiljwan Bitret Pan'an****MA/PhD, Department of International law****May, 2023, 80 (number) pages**

To perpetrate a cybercrime, one needs access to a computer and the internet. Now that ICT (Information and Communication Technology) has arrived, we live in a digital world. The development of such a system has facilitated both verbal and monetary exchanges. Even though there are benefits, the increase in internet usage and the availability of device technology have rendered not only new business opportunities possible, but also new ways for people to do illegal things. Concerns about online safety have grown as there are more and more ties between organized crime and the internet. Legislators have had trouble trying to change the laws they already have to include cybercrimes. Based on what this study found, it is clear that Nigeria's present legal structure is not enough to control cybercrime effectively. The findings of this study further demonstrate that law enforcement authorities are helpless when faced with cybercrime on their own. This study also highlights several weaknesses in the Cybercrime Act that should be addressed by lawmakers. The study's author suggests, among other things, that IT experts serve as advisers to police departments during criminal investigations.

***Key Words:* Cybercrime, Legislations, Lawmakers and Computer.**

TABLE OF CONTENTS

Approval.....	iii
Declaration.....	iv
Dedication.....	v
Acknowledgements.....	vi
Abstract.....	vii
Table of Contents	viii
Table of Casas.....	ix
Table of Statutes.....	x
List of Abbreviations.....	xi
Introduction.....	1
Statement of the Problem	5
Purpose of the Study	5
Research Questions.....	5
Methodology.....	5
Significance of the Study	6
Limitations.....	6
Definition of Terms	7
CHAPTER I	
1.1. Literature Review	8
Cybercrime.....	8
1.2. The Formation of Cybercrime legal framework.....	10
1.3. Types of cybercrime.....	14
1.3.1.	
Hacking.....	14
1.3.2.	
fraud.....	15
	Identity

1.3.3. Terrorism.....	16	Cyber
1.3.4. Phishing.....	17	
1.3.5. Spamming.....	18	
1.3.6. Cyberbullying.....	19	

CHAPTER II

Analyses of Cybercrime legal framework in international law (European Union).....	20
2.1. Legal framework decisions on cybercrime by the European Union.....	21
2.2. Council of Europe convention on Cybercrime	22
2.3. Council of Europe accepted definition of cybercrime.....	24
2.4. Cybercrime provided by the convention.....	25
2.3. Procedures of investigation.....	26
2.6. Cybercrime And Jurisdiction.....	27
2.7. The Locus Commissi Delicti Issue.....	28
2.8. International Cooperation Under the Convention.....	28
2.9. Cybercrime And Criminal Justice Systems.....	29

CHAPTER III

Cybercrime Legal Framework in Nigeria, US and UK.....	33
3.1.1. Nigeria Evidence Act 2011.....	34
3.1.2. The National Identity Management Council (2007 Edition).....	34
3.1.3. The Communications Act of 2003 in Nigeria.....	34
3.1.4. Economic And Financial Crimes Commission (EFCC).....	35
3.1.5. Nigerian Financial Intelligence Unit (NFIU).....	36
3.1.6. Challenges	37
Cybercrime Legal Framework in The U.S.	38
3.2.2. The Computer Fraud and Abuse Act 2020.....	42
3.2.3. Wire fraud Act 1994.....	43
3.2.4. The Computer Misuse Act (CMA) of 1990.....	43
3.2.5. Criminal Justice Act of 1988 and the Protection of Children Act of 1978.....	44
3.2.6. The Racial and Religious Hatred Act of 2006.....	44
Cybercrime Legal Framework in UK.....	44

3.3.2. R v. Gold and Schifreen.....	46
3.3.3. Computer Misuse Act of 1990.....	46
3.3.4. Investigatory Powers Act of 2016.....	47
3.3.5. Cyber Essentials.....	48
3.3.6. The National Cyber Security Centre (NCSC).....	48
3.3.6. The United Kingdom's Data Protection Act of 2018.....	49

CHAPTER IV

Canada Legal Framework on Cyber Crime and Universal View Of Cybercrime.....	51
4.1. Canada Legal Framework on Cyber Crime.....	51
4.2. Impact of Cyber Crimes	52
4.3. Universal View of Cybercrime.....	55
4.4. An Evaluation Of The United States' Cybercrime Legal Framework In Context Of Other Countries.....	56

CHAPTER V

Summary, Conclusion and Recommendations.....	59
5.1. Summary.....	59
5.2. Recommendations According to Findings.....	60
5.3. Recommendations for Further Research	60
REFERENCES	62
PLAGIARISM REPORT.....	69

LIST OF STATUTES

1. Data Protection Act 1998
2. European Patent Convention 1973
3. Communications Decency Act's 1997
4. Cybersecurity Act of 2021
5. European Convention on Cybercrime 2001
6. Computer Misuse Act 2015
7. Data Protection Act (DPA) of 2018
8. Nigeria Evidence Act 2011
9. Nigerian Cybercrime Act of 2015
10. Cybercrime Act 2015
11. Advanced Fee Fraud Act 2006
12. Money Laundering (Prohibition) Act of 2011
13. Constitution of the Federal Republic of Nigeria 1999
14. Malicious Communications Act 1988
15. Telecommunications Act of 1984
16. Copy rights designs and patents Act of 1998
17. Canadian Criminal Code 2005
18. Racial And Religious Hatred Act 2006
19. Council Of Europe Convention on Cybercrime
20. Hague convention
21. Economic And Financial Crimes Commission (Establishment) Act 2010
22. Obscene Publications Act 1964
23. Police And Justice Act 2006
24. Identity Theft and Assumption Deterrence Act 1998

LIST OF ABBREVIATIONS

CAN-SPAM Act: Controlling the Assault of Non-Solicited Pornography and Marketing Act

CCIRC: Canadian Cyber Incident Response Centre

CDPA: Copyrights, Designs and Patents Act

CFAA: Computer Fraud and Abuse Act

CMA: Computer Misuse Act

COE: Council of Europe

ECOWAS: Economic Community of West African States

ED: Edition

EFCC: Economic and Financial Crimes Commission

GSM: Global System for Mobile Communications

ICT: Information and Communication Technology

IOSCO: International Organization of Securities Commissions

ITU: International Telecommunications Union

NCWG: Nigerian Cybercrime Working Group

NFIU: Nigerian Financial Intelligence Unit

LFN: Laws of the Federation of Nigeria

OCIPEP: Office of Critical Infrastructure Protection and Emergency Preparedness

UNODC: United Nation on Drugs and Crime

INTRODUCTION

Background of the study

The development of new technologies has aided in human advancement but has also given birth to new challenges, such as cybercrime which is punishable offence.¹ As 21st-century technology has progressed; the globe has become increasingly digitized.² As a result of technological advances, the globe has shrunk to the size of a global village. The internet facilitates access to the economies of most countries throughout the world. Because of the widespread use of ICT, the current notion of “information society” has emerged. There are currently over 5 billion mobile phone connections and approximately 2 billion internet operators. The “International Telecommunications Union” (ITU) reported in 2011 that 26.5% of the population of Nigeria used the internet. This equates to more than 45 million people.³ Our biggest economic assets are not iron ore or coal mines, but rather, ideas and the means to put them into practice, as the Information Age continues in which we live.

Cybersecurity is critical to the nation’s economy and national defense. Cyberspace has made global communication and financial transactions easier.⁴ Industries including journalism, tourism, and banking have seen radical shifts as an effect of the widespread practice of electronic commerce and delivery of goods and services.⁵

Despite these benefits, it is via cyberspace that the security of the economy, personal information, and social relationships has been compromised and lead to the escalation of the

¹ Bossler Adam M., Berenblum Tamar. “Introduction: New directions in cybercrime research.” *Journal of crime and justice* 42(5) (2019):495-499.

² Holt Thomas J., Bossler Adam M.: “The Palgrave Handbook of International Cybercrime and Cyber deviance” (1st ed, Palgrave Macmillan Cham 2020).

³ Herhalt, J., “Cyber Crime- A Growing Challenge for Governments” (2018) US Department of Justice <<https://www.ojp.gov/ncjrs/virtual-library/abstracts/issues-monitor-cyber-crime-growing-challenge-governments>> accessed 5 March 2023

⁴ “United States Attorney, Central District of California; Chair, Attorney General’s Subcommittee on Cyber and Intellectual Property Crimes”, 2005-Present

⁵ Osman Goni “Introduction to Cyber Crime” *International Journal of Engineering and Artificial Intelligence* 3(1) (2022) 9–23

“cybercrimes”.⁶ A price must be paid for the expanding ease of internet, though. It's no secret that the rise of the internet and widespread use of computers has unlocked up new horizons for business, but it's also facilitated new ways for criminals to conduct their operations.⁷ The growth of organized crime's online presence has raised concerns about the safety of online interactions which contribute to the formation of legal regulations against “cybercrime”.⁸ Several complex crimes that had not been previously covered by our criminal legislation, such as the online credit card scam, have been linked to the advent of the internet as the remote cause. Intriguingly, some academics have stated that “in cyberspace, nobody knows you're a dog.” Criminals may target and victimize people engaged in online activity just as easily as they can target and victimize those engaged in traditional, offline activity.⁹

Because of this change, so-called “cyber-crimes” (crimes committed via the internet to cause damage to a computer) are on the increase. Online fraud and hacker assaults remain only two examples of the many types of cybercrime that are performed on a daily basis. As a result of the widespread availability of the internet, scams, fraud, and other forms of deception-based crime have flourished.¹⁰ The issue of cybercrime continues to be difficult to tackle because of the rapid leap of high-tech advancement and the diversity in the methods used to conduct crimes online. One of the fastest expanding types of crime is cybercrime.¹¹ Crimes against the confidentiality, security, and disposal of information technology resources are also considered cybercrimes, along with those connected to content, copyright, and trademark violations, and computer misuse.¹²

Many internet-facilitated crimes, such as identity theft, “desktop counterfeiting, cyber harassment, fraudulent electronic communications, ATM spoofing, pornography, piracy,

⁶ Phillips Kirsty, Davidson Julia C., Farr Ruby R., Burkhardt Christine, Caneppele Stefano, Aiken Mary P. “Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies” *Forensic science Journal* 2(2)2022

⁷ Robert W. Taylor, Eric J. Fritsch, Liederbach John, Saylor Michael R., William L. Tafoya: “Cyber Crime and Cyber Terrorism” (4th ed, Pearson 2017).

⁸ Sri Sundari, Muhammad Haikal Kautsar “Cyber Crime Triangle Approach to Encounter Cybercrime” *“Budapest International Research and Critics Institute-Journal”* 4(2)(2021)1815-1821

⁹ Ashaolu, D., “Combating Cybercrimes in Nigeria” *Basic Concepts in Cyberlaw*, (Velma Publishers, 2012)

¹⁰ Igwe K.N., Ibegwam Ahiaoma “Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria” *“International Journal of ICT and Management”* 2(2)(2014)1-14

¹¹ Azernikov A., Norkina A., Myseva E., Chicheroy K. “Innovative Technologies in Combating Cyber Crime” *1(2)(2021)248-252*

¹² Samuel Oni, Segun Joshua, “E-Government and the Challenge of Cybercrime in Nigeria”(6)(2019)

hacking, phishing, and spamming”, are done every day in Nigeria. Some crooks in Nigeria, who go by the name “yahoo guys” online, are using the internet's e-commerce infrastructure to rip off unsuspecting users. It's worth noting that Nigeria is the third jurisdiction in the world with the biggest sum of cybercrimes, behind China and the United States.¹³

Increases in cybercrime pose a serious risk to the expansion of every country e-commerce sector and to the country's safety as a whole.¹⁴ It is for this reason that Nigeria, US, UK and Canada need an effective legal framework on cybercrimes. When computers were first introduced, they were mostly used for looking up information. Now, however, individuals from all over the world can instantly connect, do business, and exchange and store massive amounts of data online.¹⁵ The 20th century saw widespread utilization of technological innovation. Increase connection across related industries to facilitate commercial and other transactions. Cyberspace is overloaded with cyber activities powered by the internet, IoT, and WAN. This has attracted hackers and other unauthorized invaders who wait for vulnerable targets. “Cybercrime” uses electronic equipment (computers), the internet, and data to extort assets from victims when a vulnerability is exploited.¹⁶ Because of the computer, it is now easier than ever to get in touch with anybody, anytime, anywhere in the universe by storing, searching, retrieving, and communicating vast amounts of information and data. With no clear jurisdiction or defining features, cyberspace presents a difficult challenge for national security services. Every person who accesses the internet is considered a resident of the state from where their connection originated. Although while cybercrime is a worldwide issue, each nation has evolved its own set of laws and regulations to attempt to curb it inside its borders.¹⁷ Most people associate Nigerians with cybercrime because of the widespread prevalence of “419” cyber fraud. While often associated with internet fraud, 419 really refers to a much broader category of cybercrime. Cyberstalking, cyberhate speech, cyberespionage, cyberterrorism, cyber colonialism, revenge porn, and

¹³ Andrew Goldsmith, Wall S. David “The seductions of cybercrime: Adolescence and the thrills of digital transgression”19(1) (2019)

¹⁴ Marcum D. Catherine, Higgins E. George: Cybercrime (1st ed, HSSR 2019)459-475

¹⁵ Carin M., Reep-van den Bergh, Marianne Junger “Victims of cybercrime in Europe: a review of victim surveys” Palgrave Macmillan 7(5) (2018)

¹⁶ Akhilesh Chandra, Melissa J. Snowe “A taxonomy of cybercrime: Theory and design” International Journals of accounting information systems 38(1) (2020)

¹⁷ George Christou “The challenges of cybercrime governance in the European Union” European Union cyber security 19(3) (2018)355-375

cyberbullying are all forms of illegal activity that may be committed in the digital realm. Fraud committed online originates primarily in Nigeria. In addition to data theft, cyber stalking, and revenge porn, other forms of cybercrime common in Western nations are rare there. The term “digital crime” is confusing, which is why it is fair to cast doubt on Nigeria's credibility. Nigeria is ranked third in the world by the Internet Crime Complaint Centre of the “US Federal Bureau of Investigation (FBI)”, which ranks only the US and UK higher. Yet, the claims made by the FBI's Washington field office are questionable given that all fraud in Nigeria takes place digitally. The concept of "cybercrime" in Nigeria is distinct from that in the West. Different online and offline jurisdictions have different norms, which might lead to discrepancies.¹⁸

The traditional approach to criminal law holds that wrongdoing is characterized by its inherent moral reprehensibility. The purpose of punishment was to make the offender make amends for the harm he caused and to atone for his moral transgressions by requiring him to pay reparation. Criminal law has its roots in both common law, which develops out of judicial decisions and opinions, and statute law, which is established by the federal government or individual states. As the United States is the origin of international norms forbidding crimes, international law has an impact on the United States.¹⁹ Examples of International Crimes are, “war crimes, genocide and crimes against humanity”.

The first Hague Conventions, which established standards for military behavior during combat and were signed at the end of the 19th century, are only one example of the many international treaties and accords that define international crimes. Everyone (i.e., the command and the commander) who plotted or permitted the crimes to occur is held accountable under these pacts.²⁰ Why is there an increase of “cybercrime” in Nigeria: Without a question, the threat of “cybercrime” in Nigeria has risen owing to a number of major causes, the most serious of which is a lack of statutory provisions meant to tackle the issue. Because of the sophisticated and detailed nature of the investigation, as well as the quick growth of new technologies, most law enforcement authorities, including the police, are unprepared to cope with online crime. Our society is becoming increasingly entangled in crime, and the public

¹⁸ Tade Oludayo “COVID ‘419’: Social Context of Cybercrime in the Age of COVID-19 in Nigeria” 14(4) (2021)460-483

¹⁹ Sources of Criminal Law (Statutes, Case Law, Ordinances, Regulations), 22 January 2014, <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118517383.wbeccj427>,

²⁰ Open society foundation; Fact sheet: International Crimes.

assumes our law enforcement organizations to keep up with up-to-date technology as it impacts the investigation and hearing process, and therefore addressing crime in general. Cybercrime remains to be a major source of concern for many government security departments in Nigeria, and combating cyber threats is becoming more difficult due to the complex ways in which fraudsters operate, as well as law enforcement agencies' poor crime investigation approaches.

Statement of the Problem

The problem this research is going to pursue is; counter the act of cybercrime despite the measures and ratified conventions. This issue has affected a lot of businesses, government documents, individual life, NGOs, Cybercrimes have caused so many losses of properties and breach of intellectual rights for organizations, hence this issue needs to be brought to light. This behavior is still causing serious havoc around the world. People have a right to a happy life unobstructed by cybercrime, which is why this issue must be addressed. However, the common slang term for a kind of cybercrime in Nigeria is 419, which refers to a technique of defrauding individuals, governments, and businesses by falsely assuming the identities of others. So, a careful examination of the cybercrime legal framework is required before tackling this subject.

Purpose Of the Study

The goals of this study are to evaluate Nigeria's, US, UK and Canada current legal framework on cybercrime; (ii) to compare and contrast Nigeria with the other jurisdictions that have a more established legal regime on cybercrime like the US, UK and the CANADA. and (iii) to provide remedies to any issues that are found.

Research Questions

- Why is there an increase of “cybercrime” in Nigeria?
- Is there a solid plan in place to stop cybercrime in Nigeria, the United States, Great Britain, and Canada?
- How successful is legal regulations on cybercrime in these countries?

Methodology

This research will employ the qualitative research technique, which is multimethod in nature and involves an interpretative, naturalistic approach to its subject matter. This study will employ a variety of methods to gain a thorough understanding of the legal framework of cybercrime in international law and international criminal law and how such cases interact with social realities, as well as how legal authorities and international law deal with the case as it emerges on a daily basis. This will be accomplished by gathering data from appropriate sources such as legislation, Journal articles and Textbooks and combining that data around the study question and problem in an attempt to address the question at hand. Data from the Council of Europe Convention on Cybercrime 2001, National Cybersecurity Protection Act (NCPA), Cybersecurity Enhancement Act 2014, Cybercrime Prevention Act of 2012 and more will be evaluated. This study also intends to contribute by analyzing an existing metric, namely the reporting mechanism. The study would also make usage of comparative review by comparing the Nigerian jurisdiction with the authority of US, UK and Canada.

Significance Of the Study

This dissertation will contribute to our understanding of Cybercrime by analyzing its legal context in an effort to slow its rise. It will serve as a foundation for further research, analysis, and scrutiny of measures to enable Nigeria, the United States, the United Kingdom, and Canada stay safe and secure. Lastly, it tries to draw our attention to some of the errors/problems related with the activity of protecting our data online and suggests plausible remedies on how to better the use of our legal instruments to safeguard persons from internet crimes.

Limitations

The research analyzed the lawful frameworks for cybercrime in Nigeria, Canada, the United States, and the United Kingdom, with special devotion paid to Nigeria. It didn't make an effort to explain Cybercrime in detail. All it did was analyze the legal framework on cybercrimes and their impacts on the economy and breach of individual rights were highlighted, and legislative measures for Nigeria's, US, UK and Canada were examined. Several difficulties were experienced throughout the study process. Despite the fact that many students have written about this topic and considered it from a global perspective, the country still lags behind in Cybercrimes legislations. Although many other affluent nations place a focus on cybercrime impact and has strong rules against this act, Nigeria is still

trapped in a culture of apathy. It was simple to evaluate foreign writers and publications in terms of the steps they took to slow the degradation of their Cybercrime regulations. Yet, despite some progress, this is not the case in Nigeria. Last but not least, the study ran into the difficulties of time as well as finances.

Term Definitions

Cyber: referring to or utilizing computer technology, most notably the World Wide Web.

A criminal offense is an act that is punished by law, or the violation of a lawful obligation that is the issue of a criminal prosecution.

“Cybercrime” means any illicit activity that takes place on the cyberspace, such as hacking or stealing information that has been saved digitally.

Cyberspace is a generic network that links many pieces of technology to one another and, if compulsory to the cyberspace.

A computer is an electrical device used for a variety of tenacities, including but not restricted to doing computations, controlling other devices, storing and retrieving text, numbers, and images.

Digital: Everything that is captured or sent utilizing computer technology is considered digital.

Being a global network of interconnected computers, the Internet facilitates global communication and the exchange of information.

The term “network” meaning a “large system composed of numerous similar components that are connected to one another to allow for movement or communication along the parts, or between the parts and a central control point”.

CHAPTER I

1.1. Literature Review

Acts that violate the law and carry legal penalties are crimes.²¹ It focuses on the steps used to bringing criminals to justice, from the first police inquiry through the final sentencing. In all likelihood, crime is the most urgent cultural issue in the universe.²² Nigeria has a substantial unemployment rate, a dysfunctional government, an improper education system, and a lot of poor people. As a result, many young people now use “cybercrime”, also called “advance fee fraud,” as a major way to make money.²³ This has given most people outside of Nigeria a bad impression of Nigerians. “According to the Federal Bureau of Investigation (FBI) and its Internet Crime Complaint Centre (IC3), Nigeria is third in the world for data breaches, after the United States and the United Kingdom. But the history doesn't take into justification the circumstance that only a small number of cybercrime losses report it”.²⁴ To do these things, you need to be smart and know how to use smart technology. Your education isn't as important. Some of the situations that will be looked at in this study are: Obinna Okeke, the owner of the Invictus group of companies, was arrested and brought before a US Attorney office. There, he pleaded guilty to a computer-based infiltration fraud

²¹ Freund Ernst., “Classification and Definition of Crimes” *Journal of Criminal Law & Criminology*, 5(6) (1915):1-21

²² < <https://www.writework.com/essay/hillside-stranglers-darcy-o-brien-crime-biggest-problem-fa>> accessed 21st March,2023

²³ Pasculli L., “The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory” *Journal of Ethics and Legal Technologies*,2(1) (2020): 48-74

²⁴ < <https://theconversation.com/the-view-that-419-makes-nigeria-a-global-cybercrime-player-is-misplaced-73791>> accessed 21st March, 2023

scheme that cost his victim \$11 million (eleven million dollars).²⁵ Second, a celebrity called Hushpuppi, Ramon Olorunwa Abbas, was arrested in Dubai along with a few Nigerians. They are being investigated and tried for their roles in money laundering, hacking into computers, and the BEC scam.²⁶ Dton (also known as "Bill Henry") is a 25-year-old Nigerian who uses Aspire Logger, Origin Logger, and Nanocore to buy and sell stolen credit card information.²⁷

The “Nigerian Economic and Financial Offenses Commission” (EFCC) and the “Federal Bureau of Investigation” (FBI) detained 281 people for different crimes, including 167 Nigerian minors. In 2017, 37% of all internet transactions in African countries were done by Nigerians, and 7% of these were frauds. Cyberattacks on businesses, banks, and government infrastructure in Nigeria caused an estimated N250 billion and N288 billion in financial damage in 2017 and 2018, respectively. With the general lockdown in 2020, this has gotten a lot worse. Nigeria loses \$500 million each year to cybercrime, which is less than the country's GDP. Banks are among the people who lose money because of cyberattacks.²⁸ The common goal of all criminal justice systems is to vindicate the innocent and punish the evil. Their dedication gives them a common goal that revolves on the concept of punishment. There is no concept of criminal law without the concept of punishment and the institutions created to quantify and carry out punishment. Punishment, it seems fair to argue, is what sets criminal law apart from other systems. The two most common definitions of criminal intent are (1) an intentional act or omission (actus reus) and (2) a certain mental condition A person's “men's rea,” which may be translated roughly as “guilty mentality,” is an essential factor in determining their criminal responsibility.²⁹

When courts comprehended that an act alone could not produce unlawful responsibility, the impression of men’s rea was devised to account for the need of a guilty state of mind on the part of the defendant. “Every intentional human behavior is considered

²⁵ <<https://www.bbc.com/news/world-africa-56085217>> accessed 15 march, 2023

²⁶ <<https://www.theafricareport.com/79818/hushpuppi-419-and-the-perceived-glorification-of-fraud-in-nigeria/>> accessed 18th March, 2023

²⁷ <<https://www.vanguardngr.com/2020/03/expose-how-nigerian-internet-scammer-pursues-his-million-dollar-dream/>> accessed 18th March, 2023

²⁸ Idris Abubakar., “FBI announces arrest of 167 alleged fraudsters in Nigeria in anti-fraud operation,” *Techcable*, 2020

²⁹ Freund Ernst., “Classification and Definition of Crimes” *Journal of Criminal Law & Criminology*, 5(6) (1915):1-21

an act. Even if they cause someone else's death, a sleepwalker's motions or those done during an epileptic seizure do not qualify as actions. For the accused to be criminally responsible for the result, the victim must have experienced genuine, verifiable suffering. There is causation between the conduct and its result if the event could not have happened in the same way absent the offender's participation."³⁰ As we saw in the definition of criminal law, the rules of a certain jurisdiction or state determine what kinds of actions are considered illegal. In the United States, for instance, there are six states that have outright bans on openly carrying handguns, twenty-four states that need a permit or license to openly carry handguns, and six more that restrict openly carrying handguns in public environments. Criminal law, a subset of public law, addresses actions that the state views as unacceptable and strives to limit or eliminate.³¹ Internet activities were not recognized or sanctioned by any existing legislation. The vast majority of Internet users, for instance, access their inboxes through the web. We still don't have email ids in our nation as of right now. Nowadays, email is neither recognized or protected by the law. In the absence of a specifically established ruling by the Parliament, the legality of electronic mail has been met with reluctance by our courts and judges. Hence, Cyber law has become necessary. When it comes to criminal law, the State, in its capacity as the collective conscience's active representation, actively enforces certain types of behavior.³²

1.2. The Formation of Cybercrime legal framework

The open, free, decentralized, and uncontrolled nature of the Internet is what gives rise to the misconception that anything goes up on it. We've demonstrated that the platform encourages user-driven innovation, which in turn boosts user-to-user contact, increases the usage of web-based services, and generates significant interest from users as well as practical benefits and financial gains. The "Information Revolution," as described by the "Council of Europe's Committee on Cybercrimes," has supposedly fundamentally changed the way our society functions. This is so because information technology has seeped into every part of human existence. They also made references to the immense amount of data that is transmitted and

³⁰ Freund Ernst (n9) p2

³¹ Cryer Robert, Robinson Darryl, Sergey Vasiliev, "An Introduction to International Criminal Law and Procedure" (4th ed, Cambridge University press, 2019).

³² Ye Hong, William Neilson, "Cybercrime and Punishment" *University of Chicago Press*, 49(2) (2020)

the freedom this provides to everyone, as well as the Internet's seemingly infinite accessibility and searchability of information and knowledge.³³

Even the bad guys are enjoying this new form of entertainment. Given that it “is a stupid network” that doesn't care what's on it, the Internet is just as happy to assist criminals as it is to assist genuine entrepreneurs in developing novel and valuable products and services. In the online world, we see the rise of new crimes and the reinvention of old ones.³⁴

In 2009, authors Ashaolu and Oduwole voiced alarm about criminals' pervasive use of online platforms. According to data collected in the years leading up to the turn of the century, "640 complaints of cybercrime were made, or about 1.7 per day in 1993." In 1994, there were 971, but by 1996, there were 1,494 (four per day), 47,009 in 1998, and over 100,000 in 1999. It was estimated that by 2100, at a daily rate of 775 complaints, there will be more than 280,000. The IC3 claims that in 2010, they received a record number of complaints about cybercrime. In a typical month, IC3 is expected to receive and resolve around 25,000 complaints.³⁵ Damages from cybercrime also reached record highs in 2018, costing an unprecedented amount of money. The administration took similar, but more gradual, steps. The US Congress revised the Cyber Facilitation Act (CFAA) and the Cybersecurity Act of 2021 to cover cyber operations. Several countries have enacted cyber laws designed specifically to handle online issues, while others have amended existing laws to do the same.³⁶ The growing prevalence of cybercrime has eroded consumers' confidence in conducting financial transactions online. Due to concerns about identity theft and credit card fraud, many individuals avoid internet shopping. Online shopping has a lot to offer customers, but only a minority of them really use it.³⁷

At the present, it seems that hackers are driven by the dual goals of proving their own cleverness and making a quick money. Yet, there is increasing evidence of infiltration being carried out for motives like espionage, extortion, and fraud as more and more sensitive

³³ Filippo Spiezia., “International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime” *Era Forum*, 23, (2022)101–108

³⁴ <https://www.annales.org/site/enjeux-numeriques/DG/2020/DG-2020-09/EnjNum20c_7Freyssinet.pdf> accessed 18th March 2023

³⁵ Ashaolu, D., “Combating Cybercrimes in Nigeria” *Basic Concepts in Cyberlaw*, (Velma Publishers, 2012).

³⁶ Jurjen Jansen, Rutger Leukfeldt., “Coping With Cybercrime Victimization: An Exploratory Study into Impact And Change” 6(2)(2018) 1-22

³⁷ Marcum Catherine D, George Higgins., “Cybercrime and deviances” (2nd ed,HSSR,2019).

company information is exchanged through the Internet. There have been no limits placed on the development of the Internet.³⁸

There has been a worldwide call to action to reduce this horrible crime, but different nations have responded with diverse degrees of fervor. The United States and the United Kingdom, for instance, both have laws on the books that criminalize internet misconduct. Despite being a frequent target of cybercrime, the European Union is currently a leader in the fight against it. Member nations and other interested governments may establish a more optimistic treaty to combat cybercrime. Governments throughout the world are working together to make the internet a safer place because cybercrime affects people everywhere.

In light of the growing threat posed by computers' growing capacity to collect, store, and transmit vast amounts of data, the first wave of legislation in the United States and much of Europe in response to computer crimes prioritized privacy protection, as noted by Ulrich Seiber, who has written a history of cyber regulations.³⁹

According to Mohamed Chawki, administrative, civil, and criminal standards are included in the created and often changed data protection legislations to defend the public's right to privacy. Beginning in the 1980s, it became clear that conventional criminal legislation was unable to adequately punish or discourage cybercrime. Things that people may look at or touch were given extra security to prevent common burglaries.⁴⁰ For example, the Court of Lords concluded in the case of "Gold and Schifreen" that in England, using a stolen or fake password to gain access to data stored on a computer does not constitute a distinct criminal offence. This resulted in the development of a new body of cyberlaws that seek to punish cyber-enabled financial crimes. Intangible assets like computer software are being protected by new regulations that make "unauthorized access" and "excessive access" unlawful as a means of combating cybercrime's ability to break into conventional commodities through new media.⁴¹

³⁸ Sari Andika, Setiawan Ananda, "The Development of Internet-based Economic Learning Media using Moodle Approach" *International Journal for active learning*,3(2) (2018)50-57

³⁹ Ulrich Seiber, "Legal aspect of computer related crimes in the information society" (1998)

⁴⁰ Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, "Cybercrime, Digital forensic and Jurisdiction" (1st ed, Springer Cham, 2015).

⁴¹ R v. Gold and Schifreen, [1988] 2 WLR 984

As a result, several nations now have laws that punish those who conduct economic crimes online. Similar wording may be found in Section 21 of the Swedish “Data Protection Act” from 1973, the first of these laws, which emerged in 1978 in numerous state legislatures in the United States.⁴² In other nations with comparable regulations, the current criminal code is updated or new laws are enacted to account with the unique characteristics of ICT. Mohamed Chawki claims that many European nations, including Denmark, Germany, and Finland, have passed laws to safeguard trade secrets. He goes on to argue that some nations are still using laws from the 1980s, while others are updating such legislation to reflect the new issues in criminal law brought about by the rapid growth of computer technology.⁴³

This is what the U. Third generation cyber legislation, known as Seiber, were created to safeguard ICT-related intellectual property. Strict copyright laws and geographic data protection were incorporated in the new legislation, making software piracy difficult in the future. The European Patent Office, however, does not protect abstract concepts such as ideas. This implies that computer programmed cannot be copyrighted under European Patent Convention article 52 section (2) and (3). In most European nations, such restrictions on patentability are written into law.⁴⁴

Because of the Internet's widespread availability and ease of use, it has become a new venue for the spreading of hate speech and other illicit information since its inception in the 1990s. The courts have been reluctant to give online companies the same protections as traditional businesses. Judge Fletcher ruled in *Yahoo vs. France* that Yahoo! does not have a right under the First Amendment to violate French criminal law or facilitate the violation of French criminal law by others, despite the fact that Yahoo is headquartered in the United States and any violation would be caused by Yahoo activities on the internet from the United States.⁴⁵ Importantly, the court ruled in *Fair Housing Council v. Roommates.com* that a real estate agent who only operates online is subject to the same regulations as a traditional agent.⁴⁶

⁴² Data Protection Act 1998

⁴³ Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, “Cybercrime, Digital forensic and Jurisdiction” (1st ed, Springer Cham, 2015).

⁴⁴ European Patent Convention 1973

⁴⁵ *Yahoo vs. France*

⁴⁶ *Fair Housing Council v. Roommates.com*

According to Chawki, in the 1980s, a handful of countries passed the first cyber reform legislation to control the spread of hate speech and other harmful content online. The most common reaction, however, has been for local governments to adjust their own legislation in light of the new reality.⁴⁷ For instance, between 1994 and 1997, the UK and Germany passed comparable legislation modifications that adapted pre-existing regulations against the spread of pornography, hate speech, and defamation to material kept in digital form and, by extension, the internet. The Communications Decency Act's Section 208, as well as similar legislation passed in Germany in 1997, were enacted in part to clarify the scope and nature of intermediary responsibility. One last set of worries emerged in the '90s, in response to the growing sophistication of cybercrime and other forms of online malice. Concerns about online security measures were central to these issues. Limits on encryption and other forms of security are among them, as are laws meant to assure the prosecution of offenders and the protection of citizens' personal information.

1.3. Types of cybercrime

1.3.1. Hacking, the illegal accessing of a computer system is known as hacking. "Hackers" are often very proficient computer programmers, and the word "hacking" refers to the unauthorized use of a computer system. They focus on one particular piece of software or programming language and know it through and out.⁴⁸ A fundamental human need for anything like "money, fame, or power" may be at the root of many of the aforementioned reasons. Some hackers do it only to show off their expertise; this may range from harmless tweaks to software or hardware to blatant assaults designed to cause harm. One or all of these desires might drive a hacker to get into a system and steal confidential data like bank records.⁴⁹ They also want to tweak the systems to allow for arbitrary functioning. "Crackers" is a term used to define these criminal hackers and their harmful actions. The term "black-hat hackers" may also be used to describe this subset.⁵⁰ Nonetheless, there are many who develop an interest in computer hacking out of pure intellectual curiosity. In order to help find security flaws and execute patches, some businesses may hire computer experts. To

⁴⁷ Chawki(n 1) p6

⁴⁸ Ames Morgan G., "Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning" 2(18) (2018)1-19

⁴⁹ Boireau Olivier, "Securing the blockchain against hackers" *Network security journal*,2018(1) (2021) 6-8

⁵⁰ Seemna P.S., Nandhini S., Sowmiya M., "Overview of Cyber Security" *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11) (2018) 2-5

stop others from abusing systems, white-hat hackers take preventative measures. They actively look for vulnerabilities in networks to exploit in order to raise awareness of such vulnerabilities. Some hackers do it for no other reason than to get notoriety or to show off their knowledge of the subject. “Grey hat hackers” engage in activities that neither strictly adhere to the black hat nor the white hat traditions. It's common knowledge that many famous people in technology started out as hackers, but that they've subsequently made beneficial contributions to their respective fields.⁵¹ Dennis Ritchie and Ken Thompson, creators of the UNIX operating system upon which Linux is based, remained two among them. Mark Zuckerberg, founder of Facebook, and Shawn Fanning, inventor of Napster, are two more. The first step in protecting your systems against infiltration is gaining an understanding of the hacking process. In this Fast Track, we will not go through some of the most popular methods that hackers use to get access to your machine via the internet.

1.3.2. Identity Fraud: The growing digitalization of government documents makes personal information about individuals of a specific nation or region more susceptible to identity fraud than it has ever been. U.S. citizens and certain permanent residents who are part of the country's central registry are each given a unique nine-digit number known as a Social Security number. This kind of identification is used by a variety of private companies to keep track of its employees for purposes like payroll, benefits, and taxes. Because of the wealth of data that can be gleaned from a individual's Social Security number, identity theft is a very serious concern. And it's not only those whose Social Security numbers have been stolen; victims of this kind of cybercrime also lose access to their digitally stored credit card details.⁵²

The loss of sensitive information, such as a credit card number or Social Security number, might open the door to theft or fraud. One of the most frequent types of cybercrime, identity theft, has global repercussions.

Yet, there aren't many trustworthy worldwide data available on this subject. While around 1.1 million Americans fall prey to identity theft every year (Department of Justice, 2015), another 15 million have had their bank account information taken, leading to unauthorized access of their cash (Department of Justice, 2020). More than \$15 billion is lost each year in the United States due to identity theft. The aftermath of this tragedy has sparked

⁵¹ “Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?” *American Journal of Criminal Justice*, 44(2019),63–82

⁵² Marcum Catherine D, George Higgins, (n 15) p4

research into strategies for preventing identity theft. When successful, identity theft often involves or sets off further forms of cybercrime. Some common forms of cybercrime include hacking, ATM fraud, wire fraud, file sharing, and piracy. Identity theft on computer or digital networks is indicated when a user receives a request for personal information such as a Social Security number, credit card details, username, password, and PIN for a mobile financial application, or details about a savings account via email or social media platforms. An employer, medical provider, school, bank, or tax agency are examples of organisations that have a legitimate need for this information but almost never resort to asking for it in this way. Tracking bills to see if and when a billing address change has occurred; routinely checking bills and bank accounts for unauthorized charges; perusing credit reports for evidence of accounts opened in a foreign name; and investing in sophisticated software for robust password protection and the detection of unauthorized network intrusion are all additional methods for spotting fraud.⁵³

1.3.3. Cyber Terrorism

When terrorist acts are carried out through the internet, this is known as cyber-terrorism. It's the use of computers, networks, or the data contained inside them to attack or threaten a government or its citizens for political or social ends. A cyber assault is considered terroristic if it results in real physical injury to people or property, or if it causes sufficient disruption to inspire widespread fear. Cybercrime differs from other types of cyber-based malice, such as cyber-terrorism, because of the motivation of the offender. Hacking, cyberstalking, and online child pornography are all unlawful activities, but the reasons cybercriminals engage in them might vary widely. So, without knowing the illegal intent or motivation, it may be hard to evaluate whether or not a certain action constitutes cybercrime. It has been noted that, because to the rapidity and secrecy of cyberattacks, it is often only after the event that the identities of the attackers whether terrorists, fraudsters, or country states can be determined. Cyber terrorism, like more traditional forms of terrorism, is not only pervasive but also potentially disastrous. Disseminating carefully crafted propaganda via internet technologies and social media platforms can have devastating effects, including undermining trust in information, enabling political sabotage, shifting public opinion in an unpleasant direction,

⁵³ Raj Singh Deora, Dhaval Chudasama, "Brief Study of Cybercrime on an Internet" *Journal of Communication Engineering & Systems*, 11(1) (2021) 1-6

disrupting law and order, causing property damage, and even causing loss of life.⁵⁴ Cyber terrorism is difficult to detect since its aims are typically achieved before any warning is sent. In actuality, many victims of cyber terrorism never even understand what was happening to them. Specialists, normally employed by the government, who possess the psychological and analytical talents appropriate for the detection of fake content making the rounds on the internet, are thus frequently tasked with classifying this kind of cybercrime. Identifying online content that has been taken out of context by the author or that unjustly incites the audience to undertake severe measures may seem like a good way to prepare yourself to detect and avoid the repercussions of cyber terrorism.

Ability to identify online content that has been taken out of context by the author or that unjustly incites the audience to undertake severe measures may seem like a good way to prepare yourself to detect and avoid the repercussions of cyber terrorism. Slavery of Children and Child pornography is a kind of cybercrime that involves the distribution of digital recordings (films, photos, and audio files) of minors and youth acting sexually provocative or improperly clothed. Regardless of cultural context, the dissemination of child pornography is a serious crime on a worldwide scale. Exposure to child porn may have serious consequences on a person's mental and emotional health, as well as cause interpersonal problems and delay sexual development. Recognizing digital information including people who seem young in sexual positions may not be a fool proof method, making the detection of child pornography a challenging task. This occurs because the legal age of majority is so low in many nations (18 in certain places), allowing individuals to pass themselves off as much younger than they really are.⁵⁵ Yet, it is still the best way to spot digital child pornography. Producers of adult digital content face more legal scrutiny if they cannot verify the age of all actors and crew members.

1.3.4. Phishing This is a method of phishing, in which an attacker poses as a trustworthy business in order to get sensitive information such as financial details and login credentials. Email spoofing is commonly used in phishing scams. It's likely that you've received emails with suspicious links that go to sites that look to be real. Perhaps, you were wary about it and

⁵⁴ Goni Osman "Introduction to Cyber Crime" *International Journal of Engineering and Artificial Intelligence* 3(1) (2022) 9–23.

⁵⁵ Akhilesh Chandra, Melissa J. Snowe "A taxonomy of cybercrime: Theory and design" *International Journals of accounting information systems* 38(1) (2020)40-46

decided against clicking the link. It was a clever move, Malware would have secretly infiltrated your system and taken sensitive data. Social engineering is a tactic used by cybercriminals to coerce you into performing malicious actions, such as installing malware or providing sensitive information. There are ways to avoid falling victim to a phishing scam that disguises itself as an email. Phishing attacks are not always carried out through electronic means.⁵⁶ To commit “vishing” (voice phishing), criminals pose as legitimate businesses while calling potential victims. Someone pretending to be from the bank may instruct you to call a certain number (given by the VoIP provider and owned by the attacker) and enter your account information. Account security is breached once you do that. Be wary of anyone who contacts you out of the blue and never give out any sensitive information over the phone. Numerous financial institutions have issued precautionary warnings to their customers about phishing scams and what they should and should not do with their account information. “If you’re a long time reader of Digit, you may remember that we successfully phished hundreds of readers years ago in an article on, yep, you got it, phishing, by disclosing a technique to hack other people's Gmail accounts by sending an email to a made-up account with your own login and password”.

1.3.5. Spamming, in an email bombing assault, the attacker bombards a single email address with so many messages that the recipient's inbox or mail server crashes. A message that is excessive in length and sent for no other reason than to eat up network capacity. A denial of service might occur if many user accounts on the mail server were to be simultaneously attacked. Spam filters are programmed to detect unwanted emails as soon as they arrive in your inbox and delete them immediately. Email bombing is a kind of DDoS assault that is often executed by a network of compromised private computers (a botnet) that are connected to the Internet and further down the invader’s control. As several email accounts are used, and the bots are trained to send varied messages to trick spam filters, this kind of attack is more challenging to defend against. Spam is a kind of email bombing in which several recipients receive unwanted communications. Unwanted emails sometimes include links to malicious or fraudulent websites. It's not only spam that may include malicious attachments. When the receiver of an email attack replies, the attacker now has access to the whole thread.⁵⁷ In order to generate revenue, spammers buy customer lists, online forums, message boards, websites, and malware that harvest email addresses. Many spam messages are sent to

⁵⁶ Raj Singh Deora, Dhaval Chudasama (n 3) p9

⁵⁷ Raj Singh Deora, Dhaval Chudasama (n 3) p9

addresses that do not exist. Virtually every Internet service provider will cut off your connection if you transmit spam. If your mail server suddenly stops working, you may have a large number of messages waiting to be sent or received. There is presently no fool proof technique to halt email bombs and spam emails since the origin of the next attack cannot be foreseen. Nevertheless, if you find out the sender's IP address, you may tell your router to reject all data packets coming from that address.

1.3.6. Cyberbullying, Cyberbullying is the use of electronic means, such as the web or social networking sites, to harass, intimidate, or otherwise exert power and influence over another person. With an ever-increasing user base that spans all demographics, social media has become a fertile environment for the growth of cyberbullying and other negative societal trends. Women and young people are disproportionately represented among cyberbullying's victims. The word "cyberbullying" is used to define a wide range of online harassment and intimidation tactics, such as cyber abuse (repeated verbal assaults on social media) and "morphing" (unlawful collecting and online distribution of a victim's digital information for pornographic reasons). Cyberslandering (the distribution of false or implausible information) (the spreading of false or implausible information).⁵⁸ This chapter has focused on a literature study of cybercrime as an umbrella term. And the term "cybercrime," which is synonymous with "computer crime," refers to any illegal activity conducted via a computer, network, or other electronic device. The international legal framework governing cybercrime would be discussed in the next chapter.

⁵⁸ Raj Singh Deora, Dhaval Chudasama (n 3) p9

CHAPTER II

Cybercrime Legal Framework in International Law (European Union).

Cybercrime is a big deal around the world because it has some features that make it hard to stop.⁵⁹ This chapter presents an overview of European law and a legal analysis of UK law as they pertain to the prevention and detection of cybercrime. The United Nations, the Group of Eight, the Organization for Economic Cooperation and Development (OECD), the Commonwealth, the Council of Europe, and the European Union are just some of the international bodies that have taken an interest in this matter (EU). Two international agreements of particular importance from a European perspective are the 2001 Council of Europe Convention on Cybercrime (henceforth the CoE Convention) and the 2005 European Union Framework Decision on attacks against information systems. Both of these agreements focus primarily on Europe and carry legal weight.⁶⁰ Cybercrime, is a global threat that requires international cooperation to effectively combat. Several international legal instruments have been developed to provide a framework for addressing cybercrime at the international level.⁶¹

The Budapest Convention on Cybercrime is one of the most important international legal agreements in this field. Almost sixty nations have already accepted the agreement after it was established by the Council of Europe in 2001. International collaboration in the investigation and prosecution of cybercrime, such as fraud, forgery, and hacking, is facilitated by the treaty. Concerns like keeping electronic evidence intact and securing vital infrastructure are also covered. In addition to unlawful access to computer systems, data tampering, and computer-related fraud, the Convention on Cybercrime criminalizes a wide variety of other cyber acts. It sets up mechanisms for international collaboration in investigations and prosecutions, as well as for the cross-border acquisition of electronic evidence.

In addition to the Budapest Convention, other international legal instruments address specific aspects of cybercrime. For example, the United Nations General Assembly has

⁵⁹ Brenner S., B.J. Koops, "Approaches to Cybercrime Jurisdiction" *Journal of HighTechnology Law*, 4 (1) (2004) 1-46.

⁶⁰ The Council of Europe's Convention on Cybercrime (CETS No. 185)

⁶¹ Koops B.J., "Cybercrime Legislation in the Netherlands", country report for the 18th International Congress on Comparative Law.

implemented several tenacities related to cybercrime, including the 2010 resolution on “Combating the criminal misuse of information technologies.” The resolution calls on member states to establish appropriate legal frameworks to prevent and combat cybercrime, to cooperate with each other in investigating and prosecuting cybercrime, and to promote public awareness of cybercrime risks.⁶² Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security were established by the Organization for Economic Cooperation and Development (OECD) to help prevent cybercrime. The guidelines provide suggestions for governments, corporations, and people to better protect themselves from cyber threats and fight online crime.⁶³ Cybercriminals are able to operate internationally because, as professor James Boyle put it, “Cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries.” This means that, for example, “if the Kings writ reaches only as far as the King of sword,” much content on the internet might be presumed to be free from the regulation of any particular sovereign. The program was distributed through a hidden website run by a Canadian university. The absence of criminal legislation, the lack of procedural authorities, and the lack of enforceable mutual aid clauses with other nations all contribute to the jurisdictional challenge of cybercrime. The emphasis of this chapter is on the laws of the United Kingdom, but we will also look at the convention on cybercrime and the legislation of other nations.⁶⁴

2.1. Legal framework decisions on cybercrime by the European Union

Cybercrime is one kind of crime that the European Union's Framework Decisions want to standardize how it is dealt with. The Council of the European Union (composed of the justice ministers of the member states of the European Union) has the discretionary power to “adopt framework decisions for the purpose of approximation of the laws and regulations of the member states” per Article 34(2)(b) of the Treaty on European Union (before the Lisbon Treaty). Police and judicial cooperation in criminal situations are outlined in Title VI of the Treaty on European Union. Framework decisions about the intended goal must be

⁶² Convention on Cybercrime 2001

⁶³ <https://www.researchgate.net/profile/Stein-Schjolberg/publication/267946947_The_History_of_Global_Harmonization_on_Cybercrime_Legislation_-_The_Road_to_Geneva/links/556f05b008aefcb861dd4adb/The-History-of-Global-Harmonization-on-Cybercrime-Legislation-The-Road-to-Geneva.pdf> Accessed 8th April 2023

⁶⁴ Weber A., “The Council of Europe's Convention on Cybercrime” *Berkeley Technology Law Journal*, 18(1) (2003) 425-446

adhered to by all member states, but the details of how this is to be achieved are left up to each country's responsible authorities. No immediate repercussions will result from this.⁶⁵

To “improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services of the member states, by approximating rules on criminal law in the area of attacks against information systems,” the EU Council adopted Framework Decision 2005/222/JHA on attacks against information systems on February 24, 2005. (Recital 1 of the preamble). According to the preamble of the framework decision, “criminal law in the area of attacks against information systems should be approximated to ensure the greatest possible police and judicial cooperation in the area of criminal offenses related to attacks against information systems, and to contribute to the fight against organized crime and terrorism” (recital 8). Due to the internet's worldwide reach, most attacks on modern information systems are of a transnational character, underscoring the pressing need for a more comprehensive approach to criminal legislation in this area. The Framework Decision went into force on March 16, 2005.

On June 2, 2001, the EU Council passed Framework Decision 2001/413/JHA to combat fraud and counterfeiting of non-cash means of payment, which includes computer-related offenses (article 3) and offenses involving specially adapted devices (article 4). On June 2, 2004, the EU Council passed Framework Decision 2004/68/JHA to combat the sexual exploitation of children and child pornography.

Article 69B of the Lisbon Treaty states that “the European Parliament and the Council may, by means of directives adopted pursuant to the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offenses or from a special need to combat them on a common basis.” Concerns include terrorism, human trafficking (including sexual exploitation of children and women), drug trafficking (including the trafficking in illicit firearms), arms trafficking (including the trafficking in illicit money), corruption (including the counterfeiting of currency), cybercrime, and organized crime.

2.2. The Council of Europe Convention

⁶⁵ Cybercrime Act, Section 28

The Council of Europe's 41 member nations produced the "Convention on Cybercrime" in Strasbourg, France. Hungarian negotiators first met in 2001 to draft the agreement, and it finally went into effect in 2004. It was made because of rising dissatisfaction with the current legal framework for punishing illegal behavior on the internet. Like a treaty, this piece of international law binds signatory nations to its terms. According to Article 26 of the Vienna Convention on the Law of Treaties, all treaties in effect are binding on their parties and must be carried out in good faith, which provides for the "pacta sunt servanda" concept. "Pacta sunt servanda" is a Latin phrase that means "agreements must be kept" or "promises must be kept." It is a principle of contract law that emphasizes the importance of upholding the terms of a legally binding agreement.⁶⁶ The phrase is often used to remind people of their obligations and responsibilities to follow through on their commitments, whether they are personal or professional in nature. The main mechanism for updating and reinforcing the authority of a rule of law between nations is the treaty system, which has not kept up with the rapid pace of change in international affairs. The convention is the first international treaty that addresses cybercrime and provides a legal framework for countries to cooperate in the fight against cybercrime. The convention has three main objectives:

1. To harmonize national laws relating to cybercrime.
2. To improve international cooperation in the investigation and prosecution of cybercrime.
3. To promote the protection of computer networks and data from cybercrime.⁶⁷

According to the convention, cybercrime is any act that compromises the privacy, security, or availability of digital information or computer systems. Criminal offenses relating to computers and the internet are outlined, such as hacking, data theft, computer fraud, and even child pornography.

The convention requires countries to establish laws that criminalize these offences and to take measures to investigate and prosecute cybercrime. It also establishes procedures for international cooperation in the inquiry and trial of cybercrime, including the preservation of electronic evidence, the identification and location of suspects, and the extradition of suspects.

⁶⁶ Article 26 of the Vienna convention 1961

⁶⁷ European Convention on Cybercrime 2001

The United States, Canada, and the vast majority of European nations have all accepted the Budapest Convention on Cybercrime as of 2021. Many other nations have also signed it, showing their desire to ratify it in the future. Second Convention Article Offenses Made a Crime: Cybercrimes like as hacking, computer fraud, and child pornography are all addressed in this article, which mandates that member nations create criminal penalties for them. Article 3 is about jurisdiction, establishes the principle of territoriality in the investigation and prosecution of cybercrime, meaning that a member state has jurisdiction over an offense committed within its territory or by one of its nationals.⁶⁸ Article 4 comes up with the idea of search and Seizure of Stored Computer Data: This article requires member states to have the necessary legal powers and procedures to enable law enforcement authorities to search or seize computer data, either in real-time or stored.⁶⁹ In order to combat cybercrime, member nations must share information and provide mutual legal help to one another in accordance with Article 10, which is titled “Assistance to Other States.”⁷⁰ Sanctions and actions are discussed in Article 23. Article 17 of the Convention mandates that member states impose suitable penalties for violations of its provisions, taking into consideration the seriousness of the conduct and the damage done to victims.⁷¹

The Budapest Convention on Cybercrime has been widely recognized as a significant international legal instrument for the prevention and suppression of cybercrime and the promotion of international cooperation in this field.

2.3. The Convention Accepted Dictionary Definition of a Computer System

Article 1 of the Convention defines four terms fundamental to the Treaty. The treaty defines “computer data” as “information in such a manner that it may be immediately processed by the computer system.” A computer system is a combination of computer hardware and computer software that can automatically handle digital data. The data must be provided in a readily usable format, such as an electronic file or paper copy.

The third concept, service provider, covers a wide range of organizations with specialized functions in the realm of data transmission and processing inside digital infrastructures.⁷²

⁶⁸ Article 3 European convention on Cybercrime.

⁶⁹ Article 4 European convention on Cybercrime.

⁷⁰ Article 10 European convention on Cybercrime

⁷¹ Article 23 European convention on Cybercrime

⁷² Article 1 European convention on Cybercrime

Any organization, public or private, and any organization that stores or processes data on behalf of public or private organizations fall under this description.

2.4. Cybercrimes Provided by the Convention

The domestic law of the party, that is, the state that ratified the convention, shall make it a criminal offense to aid or abet the commission of any offenses against the confidentiality, integrity, and availability of computer data and systems, and offenses related to infringements of copyright and related rights. Article 11 of the treaty stipulates that domestic implementation of the treaty's substantive offenses is mandatory for ratifying countries.⁷³ A few examples of convention-provided offenses include; Hacking is the unauthorized use of a computer system for the purpose of collecting data or engaging in other dishonest activity, or gaining access to one computer system through its connection to another. Based on domestic legal explanations, defenses, or similar ideas, “without right” indicates an action taken without authority from any branch of government (legislative, executive, administrative, judicial, contractual, or consensual) or in a manner not protected by law. Thus, this provision will not apply when such data or access to the computer system is permitted. Keeping tabs on electromagnetic emissions from a computer system that are carrying private data in transit to, from, or inside the system is an example of eavesdropping, which is the unlawful use of technology to spy on private data transfers to, from, or within the system. Unauthorized impairment to, deletion of, degradation of, or suppression of digital information, with the caveat that a convention signatory may retain the right to insist on the occurrence of “severe harm”, this clause might be utilized to prosecute crimes involving the deployment of harmful malwares and viruses to destroy computer data.

Unauthorized access to, use of, storage of, or modification of information that disrupts or destroys the functionality of a computer system. The use of malicious software like viruses or malware to damage or destroy computer systems is a crime that may be punished under this clause. Cybercrime is a global problem, and this convention offers a legal framework for governments to collaborate in the fight against cybercrime by criminalizing a range of online transgressions.

⁷³ Article 11 European convention on Cybercrime

Countries that ratify the Convention are obligated to implement safeguards to prevent cybercrime against computer networks and digital information. Preserving electronic evidence, safeguarding essential infrastructure, and securing computer systems and data are all part of this. The Convention's overarching goal is to encourage international collaboration in the fight against cybercrime by providing a thorough legal framework for doing so.

2.5. Procedures Of Investigation

In the second major section of the Convention, parties are obligated to adopt specific procedural methods and processes to aid in the investigation of cybercrime and other offences where digital evidence may be found. For the sake of conducting the investigations into the convention's specified crimes, ratifying nations must enact whatever domestic laws and other measures are required to effectively deal with these transgressions.

The Council of Europe Convention on Cybercrime, offers a legal framework for investigating cybercrime and cooperating across borders. The convention sets out procedures that are intended to facilitate effective and efficient investigations into cybercrime. Here are some of the key procedures:

1. **Electronic evidence preservation:** Countries that ratify the convention are obligated to take certain steps to preserve the integrity and trustworthiness of electronic evidence, such as establishing protocols for its preservation.
2. **Search and seizure of electronic evidence:** Subject to specific criteria and safeguards, including the need for a warrant or similar court permission, the agreement permits the search and seizure of electronic evidence.
3. **Data interception and real-time collection:** Under certain circumstances and protections, such as the need for a warrant or comparable court authorization, the agreement permits real-time data interception for the purpose of investigating cybercrime.
4. **International cooperation:** The convention facilitates international cooperation in cybercrime inquiry and prosecution. It permits member nations to exchange information and evidence, with specific protections and limitations.

5. Extradition: The convention provides for the extradition of suspects in cybercrime cases, subject to certain conditions and safeguards, including the requirement that both the asking and responding nations have criminal penalties in place for the alleged offense.
6. Mutual legal assistance: The convention requires signatory countries to provide mutual legal assistance to each other in the investigation and prosecution of cybercrime, subject to certain conditions and safeguards.

Overall, the procedures set out in the Budapest Convention on Cybercrime are intended to promote effective and efficient investigations into cybercrime, while also protecting the rights of individuals and safeguarding the integrity of electronic evidence.

2.6. Cybercrime And Jurisdiction

Cybercrime poses unique challenges for determining jurisdiction because the Internet has no physical boundaries and cybercriminals can operate from anywhere in the world. Determining jurisdiction is critical because it determines which laws and legal authorities apply to a particular case. In situations involving cybercrime, jurisdiction is established according to the concept of territoriality. This principle holds that a state has jurisdiction over crimes that occur within its territory. Yet, pinpointing the precise location of a cybercrime may be tricky since the offender may be situated in a different jurisdiction than the victim or the target system. In cases where the victim and the perpetrator are located in different jurisdictions, there are several ways to determine jurisdiction. One approach is to use the principle of the “effects doctrine”, which holds that a state has jurisdiction over a crime if the effects of the crime occur within its territory. For example, if a cybercriminal in one country hacks into a computer system in another country, causing damage or stealing data, the country where the victim is located may have jurisdiction over the crime.

Another approach is to use the principle of the “active personality doctrine,” which holds that a state has jurisdiction over a crime if the perpetrator is a citizen of that state. For example, if a citizen of one country commits a cybercrime against a victim in another country, the victim's country may have jurisdiction over the crime.⁷⁴ In some cases, multiple jurisdictions may have overlapping claims of jurisdiction. In these cases, international

⁷⁴ Boyle J., “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors” *University of Cincinnati Law Review*, 66 (1997) 177-178

cooperation and coordination are necessary to ensure that the appropriate authorities are involved and that the case is handled properly. Overall, determining jurisdiction in cybercrime cases is complex and requires careful consideration of the relevant legal principles and the specific circumstances of each case. Effective international cooperation and coordination are essential for combating cybercrime and ensuring that perpetrators are brought to justice.

2.7. The Locus Commissi Delicti Issue

The locus commissi delicti issue refers to the question of where a crime was committed in cases of cross-border cybercrime. Locus commissi delicti is a Latin term that means “the place where the crime was committed.” In traditional crimes, it is usually straightforward to determine where the crime was committed because it occurs in a specific physical location. However, in cases of cybercrime, the physical location of the perpetrator and victim may be different, and the crime itself may not occur in a physical location.⁷⁵ The issue of locus commissi delicti can be challenging in cases of cross-border cybercrime because it determines which country has jurisdiction over the case. The concept of “jurisdiction” in criminal law is based on the notion of territoriality. It holds that a state has jurisdiction over crimes that occur within its territory. However, in cases of cybercrime, it may be difficult to determine where the crime occurred because the perpetrator may be located in a different jurisdiction from the victim or the target system. To address this issue, international legal frameworks, such as the Budapest Convention on Cybercrime, provide guidance on determining jurisdiction in cross-border cybercrime cases. The Convention recognizes that jurisdiction can be based on several factors, such as the location of the victim, the location of the perpetrator, and the location of the computer system used to commit the crime. Overall, the locus commissi delicti issue highlights the complexities involved in determining jurisdiction in cases of cross-border cybercrime. International cooperation and coordination are essential for ensuring that cybercriminals are brought to justice and that victims receive appropriate compensation and support.

2.8. International Cooperation Under the Convention

⁷⁵ European Convention on Cybercrime 2001

The Agreement acknowledges that cybercrime is a global issue requiring a concerted international response. The Agreement includes a number of provisions intended to improve international collaboration:

1. Mutual legal assistance - According to the Agreement, nations should work together to effectively investigate and prosecute cases of cybercrime. Provide evidence, carry out search and seizure orders, and extradite wanted individuals.
2. Joint investigations - the Convention allows for the creation of joint investigation teams (JITs) between different countries to investigate cross-border cybercrime cases. JITs facilitate the sharing of information and resources between countries to ensure effective and efficient investigations.
3. International cooperation networks - the Convention promotes the establishment of international networks of experts and law enforcement agencies to exchange information and expertise on cybercrime-related issues.
4. Capacity building -The Agreement urges signatory nations to strengthen their capabilities in cybercrime investigation and prosecution. Training of law enforcement personnel, drafting of national laws, and providing technical support to foreign nations all fall under this category.

The Cybercrime Convention Committee (T-CY) is established under the Convention to monitor the Convention's implementation and to promote international collaboration. T-CY is in charge of keeping tabs on how the parties to the Convention are adhering to its terms, helping governments implement the Convention, and encouraging international collaboration in the fight against cybercrime. Cybercrime is a worldwide problem, and the European Convention on Cybercrime establishes a cooperative framework for governments to work together to tackle it.

2.9. Cybercrime And Criminal Justice Systems

The challenges that cybercrime presents to traditional criminal law and the criminal justice system are many. The difficulty starts with trying to pin down what it really is. The trendy term "cybercrime" really encompasses a wide range of online crimes. Various Offenses. The categories used here are those defined by the Agreement on English Usage. The policies of

the European Union (EU) and other countries have been heavily impacted by this conceptual framework for cybercrime. As such, it contributes to our understanding of Europe's cybercrime laws.

In addition, it helps differentiate between forms of cybercrime in which information systems are either the intended victims or the actual perpetrators. Hence, crimes committed against the privacy, security, and availability of digital information and computing resources (CIA crimes) make up the first category of cybercrime. An example of this kind of crime is the theft or destruction of data by illegal access to a victim's computer. The second category comprises computer-related crimes when a computer is used as a tool, but is not necessary, in the conduct of the crime. One kind of online scam involves the use of a fraudulently created website to steal credit card information. Third, when conducted through computer system, offenses linked to content, such as kid pornography and acts of racism and xenophobia, come under the category of cybercrime. Fourth, there's the issue of copyright infringement, which includes things like selling pirated software.

The second difficulty is that the conventional criminal justice environment sometimes lacks experience with and understanding of Information and Communication Technologies (ICT). Crimes employing these gadgets need competent investigators, prosecutors, and judges to resolve. States should invest in training and education for professionals in the criminal justice system who need to be familiar with technological and computer skills. In order to keep up with the ever-evolving nature of the information and communications technology (ICT) industry, workers in the field must undergo continuous retraining this dynamic and consistent strategy is likely foreign to many in the criminal justice industry. A significant portion of cybercrime takes place in non-physical locations, such as through mobile phone networks or online. This often runs counter to the two primary tenets of criminal justice operation sovereignty and the territoriality concept. Countries need to set clear guidelines on a judicial system's jurisdiction over cybercrimes because of the mostly virtual character of many cybercrimes. In addition, these crimes typically take place in several locations, each of which may be focus to the laws of a separate nation state. Thus, there is a pressing need for well-defined standards outlining the responsibilities of each participating nation.

The fourth difficulty is that the speed at which the digital and physical worlds evolve is quite different. Very rapid crime dissemination is possible and crimes themselves happen

in a fraction of a second. Evidence of cybercrime often takes the form of digital information, which is transitory and subject to modification or erasure. So, law enforcement authorities need to be able to respond quickly and gather and reserve digital evidence for usage in court. Effectively addressing the issues surrounding the suppression of cybercrime would need updating laws and law administration mechanisms somewhere they are inadequate to handle the enquiry and prosecution of the phenomena. The CoE Convention and the FD are two international accords that aim to address these concerns. Together, they provide a triangulated strategy for enhancing international collaboration, lowering barriers between different national criminal codes, and gaining additional investigative resources. The following sections provide a concise summary of the key steps along each of these routes, as well as a short discussion of some of the critiques and other difficulties that have arisen as a result.

In conclusion, the present state of cybercrime legislation implementation in Europe reveals a number of discrepancies in the legal framework. More than the legality of international measures, these concerns pertain to the security, politics, economy, and reputational elements involved in their implementation. There is currently no evidence that the EU's intervention is beneficial. The difficulties of implementing the FD prove this to be true. Certain adjustments will be made as a result of the Treaty of Lisbon and the Stockholm Program CRIM, but they are not expected to be dramatic in the near future. Nonetheless, they may eventually lead to more effective enforcement of the existing cybercrime laws. Considering the rapid evolution of cybercrime, one may reasonably question the continued viability of the existing European legal framework by the time the new norms take effect.

The European criminal justice system is confronting significant difficulties from cybercrime. The aforementioned effort to strengthen cybercrime suppression in Europe (and beyond) is best shown by the three-pronged strategy outlined above. Secondly, it provides novel methods for exploring these crimes. Furthermore, it standardizes the definitions of computer-related offenses among countries. Finally, it sets the groundwork for international criminal cooperation. The CoE, the CoE Convention, and the FD, which together comprise the European and international legal framework, have all been criticized, despite their role in bolstering the global response against cybercrime. A possible misunderstanding of the role of human rights and freedoms in international criminal cooperation may have contributed to some of these concerns. However, the effectiveness and implementation of these multilateral mechanisms are the most urgent challenges. The difficulties of implementing them legally are

quite serious. It seems, nonetheless, that indirect use of these is optimal. This supports the idea that national security, politics, the economics, and public opinion are more important to the effective application of these international tools than their legal enforcement. The European Union's (EU) efforts in this area have so far been disappointing. The CoE and the FD are major bodies of international law with the aim of improving European and international cooperation in the fight against cybercrime, and it is conceivable that they will be of assistance, but you shouldn't bank on it occurring any time soon. Despite the setbacks, they still seem to be significant advances. However, given the complexity and other potential obstacles to their implementation, their enforcement is just the beginning.

In conclusion, the Budapest Convention on Cybercrime is a crucial tool for international collaboration and criminalization of cyber activities, notwithstanding the complexity and evolution of the legal framework for addressing cybercrime under international law. When it comes to dealing with certain areas of cybercrime, other international legal instruments and standards also give crucial advice.

CHAPTER III

Cybercrime Legal Framework in Nigeria, U.S. and U.K.

Since no previous Nigerian Federal Law specifically addressed cybercriminals, the Nigerian Cybercrime Act of 2015 stands as the country's most important piece of legislation.

The primary goal of this law is to establish procedures for dealing with cybercrimes in Nigeria, including their abolition, detection, reaction, investigation, and prosecution.⁷⁶ Hackers in Nigeria who gain unauthorized access to a computer system or network may face up to a N10 million fine and 5 years in jail, according to the country's Cybercrime Act of 2015. In addition, a conviction for identity theft may lead to a jail sentence of about three years, a fine of at least N7 million, or both. The Cybercrime Act of 2015 mandates stringent measures to secure user data, including the storage, processing, and retrieval of all traffic data and subscriber information. Constitutional protections for personal privacy must be upheld. The statute provides the following guidance for distinguishing one thing from another: The Act establishes a uniform and comprehensive legal, regulatory, and institutional framework for the suppression, identification, prosecution, and punishment of cybercrimes in Nigeria. Cybersecurity, the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights, all fall within the purview of this legislation. Nigeria is third on the list of the world's top ten sources of cybercrime, showing that the trend persists even if the act is very creative. The statute also specifies the process through which a judge may obtain electronic data for use in a lawsuit. All cybercafés are required to register with the Computer Professional Registration Council (CPRC) under the Cybercrime Act of 2015. “Revisions to the Economic and Financial Crimes Commission Act Of 2004” The EFCC Act allows for the investigation and prosecution of many forms of cybercrime, such as advance fee fraud, money laundering, computer credit card fraud, contract scams, etc. “Advanced Fee Fraud Act 2006” this Act establishes definitions, prohibitions, and penalties for offenses involving advance fee fraud. Section 2 of the Act makes it illegal to engage in any kind of fraud, cybercrime, or unjust property acquisition.⁷⁷

⁷⁶ Cybercrime Act 2015

⁷⁷ Advanced Fee Fraud Act 2006

3.1.1. Nigeria Evidence Act 2011

The use of digital functionality was officially acknowledged as an important factor in the court system for the first time by the Evidence Act of 2011. A good example of this is Section 84 of the Evidence Act (2011), which allows for the admission of evidence created by a computer. By its very definition, Cybercrime ensures that both the prosecution and the defence will rely on electronic evidence throughout the prosecution of offenders, necessitating the use of Section 84 to set conditions for admission of electronic evidence. When appropriate, electronic signatures can be used in place of handwritten ones thanks to Section 93 (2) and (3). Both the Criminal Code and the Penal Code Act are referred to as “the Code.” Whereby Southern Nigeria’s penal law and the Penal Code, which is in effect in the north, both make theft a crime; in this context, “theft” can also refer to theft committed through the Internet. Both laws prohibit what amounts to a form of cyber fraud known as “obtaining” anything by means of deception.⁷⁸

3.1.2. The National Identity Management Council (2007 Edition)

The Nigerian Identity and Biometrics Management Commission (NIMC) was established by the NIMC Act to create a national database of Nigerians and to provide national identification cards to those individuals. The Commission is the sole agency authorized to assign Nigerians with National Identity Numbers, which will function as a form of digital identification.

The Money Laundering (Prohibition) Act of 2011 outlaw’s offenses involving unlawful financial transactions, which aids in the prevention of fraud and the transfer of illegal funds, especially when conducted via the internet.⁷⁹

3.1.3. The Communications Act of 2003 in Nigeria

Over time, the Nigerian Communication Commission, the supreme agency charged with regulating telecommunications in Nigeria, has implemented the NCA to guarantee the safety of telecommunications for all Nigerians. All Network providers and ISPs are required by the Act to guarantee compliance with all of its provisions or risk penalties. The Cybercrimes Act mandates that all ISPs provide subscriber data and information to law enforcement authorities if there is suspicion that a phone number is being used for unlawful activity, and the Commission is tasked with ensuring that this legislation is fully implemented.

⁷⁸ Nigeria Evidence Act 2011

⁷⁹ Money Laundering (Prohibition) Act of 2011

3.1.4. Economic And Financial Crimes Commission (EFCC)

In Nigeria, incidents of advance fee fraud and monetary laundering are investigated by the Economic and Financial Crimes Commission (EFCC). Specifically, the commission can investigate, prevent, and prosecute “money laundering, embezzlement, bribery, looting, and any form of corrupt practices; illegal arms deal, smuggling, human trafficking, and child labor; illegal oil bunkering; illegal mining; tax evasion; foreign exchange malpractices including counterfeiting of currency; theft of intellectual property and piracy; open market abuse; dumping of toxic wastes; and prohibited goods.” Section 5 of the Act states that the Commission is in charge of enforcing and administering the Act, as well as investigating and prosecuting economic and financial crimes like advance fee fraud, money laundering, counterfeiting, and illegal charge transfers. This is done in consultation with the Attorney-General of the Federation. The “Yahoo lads” are committing economic sabotage, hence their criminal actions would fall under this category of economic crime. Many EFCC prosecutions, notably the one against Emmanuel Nwude (the accused) in “Federal Republic of Nigeria v. Chief Emmanuel & Ors”⁸⁰, have relied on Section 5. It was said that the defendant in this case was responsible for the third largest single swindle in the history of the planet. The defendants in this case have been brought before the High Court of Lagos State. All 57 defendants were found guilty and given appropriate sentences for their roles in a \$181.6 million dollar fraud scheme. In addition to this sentencing, the Federal Government of Nigeria also recovered and restored the large quantities of money that had been forfeited to it. The Act's jurisdictional offenses are outlined in Sections 14-18. All types of fraud, theft, terrorism, supplying false information, and other economic and financial crimes are covered. In Section 46 of the Act, “any nonviolent criminal and illicit activity committed with the objectives of earning wealth illegally, either-individually or in a group or organized manner,” by violating existing legislation governing the economic activities of government and its administration, is defined as an economic crime. All forms of fraud, narcotics trafficking, money laundering, embezzlement, bribery, looting, corrupt practices, and armed robbery are included in this description.

The commission is also accountable for tracking down and seizing any money made through terrorist acts, as well as freezing or confiscating any funds found. The EFCC, for instance, seized about \$100,000,000 from spammers and other defendants in 2005 alone. Conviction

⁸⁰ Federal Republic of Nigeria v. Chief Emmanuel & Ors

for terrorist funding or operations carries a mandatory minimum sentence of life in prison, in addition to the fine and loss of assets outlined in the EFCC Establishment Act.⁸¹ EFCC's good working connection with key Law Enforcement Agencies worldwide must be emphasized. A few examples of these organizations include the UN Office on Drugs and Crime (UNODC), the Council of Europe (CoE), and the Economic Community of West African States (ECOWAS).

3.1.5. Nigerian Financial Intelligence Unit (NFIU)

Established in accordance with the EFCC Act of 2004 and the Money Laundering (Prohibition) Act of 2004, as amended, this section serves as an operational unit within the EFCC's office. The section plays a crucial role in the EFCC as a whole. It works in tandem with the EFCC's Directorate of Investigations rather than independently. Currency Transaction Report and Suspicious Activity Report financial disclosure is received and analyzed as a unified goal of the unit. Financial institutions and certain non-financial organizations are required by law to report financial transactions to the National Financial Intelligence Unit (NFIU). Numerous other financial intelligence centres and the NFIU have signed memorandums of understanding (MOUs) on information sharing, allowing the NFIU access to all government and financial organization documents and databases.

Both the legislative and the judiciary have a role in shaping the legal framework within which a situation operates. The institutional framework, the agency responsible for carrying out the policies established by different authorities, may be regarded of as a third arm of the institution. It's sufficient to note at this moment that Nigeria does not yet have an ICT Law that would make illegal activities using InfoTech, computers, or computer networks a criminal offense. A straight law forbidding cybercrime in its original cyber form would be *nullus secundus* in this fight since cybercrime can only be conducted in cyberspace. It would be ridiculous to believe we are making significant progress in the battle against cybercrime given the trickle of charges and convictions that appear almost daily. If we look at what other nations have (even an African country like Ghana, which has an ICT Law), we can see that we are far behind where we should be. Some of the obstacles to cybercrime prosecution in Nigeria are discussed below.

⁸¹ Economic And Financial Crimes Commission (Establishment) Act 2002

3.1.6. Challenges

(1). Administrative Predicament Section 36(12), 1999 Constitution of the Federal Republic of Nigeria provides hence:

“a person shall not be convicted of a criminal offence unless that offence is defined and the penalty thereof prescribed in a written law; and a written law refers to an Act of the National Assembly or a law of a State”⁸²

Consequently, the components of criminal prosecution in Nigeria stem mostly from the law itself. Crimes that are not codified do not have any legal consequences.⁸³ The courts have consistently shown strong backing for this view. The wrongdoing at issue in *Udokwu v. Onugha* occurred six months before it was made illegal by law.⁸⁴ Based on Article 22(10) of the Constitution of 1963, the court found the accused not guilty.⁸⁵ The conduct that are being prosecuted as cybercrimes must be considered illegal and punished under local law. It would be a violation of the accused's right to a fair trial to prosecute them for conduct that are morally repugnant but not explicitly criminalized by local statutes. We are certain that the current democratic dispensation of the Rule of Law and due process in Nigeria would not enable such a situation to exist.

The absence of specific laws against cybercrimes is the biggest obstacle to their prosecution. In the current day, they are regarded as societal vices and are considered bad from a moral perspective. The first step toward an ICT future devoid of crime is an ICT Law.

The Nigerian Cybercrime Working Group (NCWG) was founded sometime in 2004. The NCWG's mandate included drafting a Cybercrime Bill as part of Nigeria's Information and Communications Technology Act. The group was concerned more with “resource management” than “crime control” nevertheless. They wasted time arguing over who had greater authority rather than getting to work with the urgency and dedication called for by their Terms of Reference. The NITDA argued that the Cybercrime agency should report to it, but the EFCC preferred that it be part of the EFCC's Commission. The Nigerian Computer

⁸² Section 36(12), 1999 Constitution of the Federal Republic of Nigeria.

⁸³ Article 1, Council of Europe, Convention on Cybercrime

⁸⁴ *Udokwu v. Onugha*

⁸⁵ Article 22(10) of the Constitution of 1963

Society has long called for a dedicated agency to combat cybercrime. This is how we wasted seven years of our lives making no real progress.

So, law enforcement is limited in its ability to prosecute cybercrimes due to the availability of conventional criminal laws. Cybercrime, for instance, may be punished as an offense of gaining by false pretences under the Criminal Code or the Advanced Fee Fraud and other Related Offences Act, 1995.⁸⁶

A Data Protection Act would have been ideal for prosecuting cases of online privacy invasion, plagiarism, piracy, and other intellectual property violations.⁸⁷ While data saved on a computer system and some forms of software that only exist in the ICT world are protected by the Nigerian Copyright Act, they are not included in the definition of property.⁸⁸

Due to the cyber nature of crimes, which is characterized by cyber-anonymity and pseudo-identity, standard regulations are insufficient in adequately catering to all types of cybercrime.

(2). Procedural Predicament

Nonetheless, there are situations in which the conventional laws are enough to address the alleged wrongdoing, such as the cases of cybercrime outlined above. When this occurs, law enforcement agencies have a powerful accusatory weapon at their disposal for bringing online offenders to justice. Also, on the lower instances, they have obtained quite costly convictions. Because of the sluggish development of our Criminal Justice System in Nigeria, convictions are not being issued at the same rate as trials are being carried out. The Criminal Process Act and the Evidence Act are the primary sources of law in this area as discussed above.

3.2.1. Cybercrime Legal Framework in The U.S.

Cybercrime started from the USA, the first act established in the USA is the computer fraud and abuse Act, 1986.⁸⁹ This act reduced hacking of computer systems. It was amended in

⁸⁶ Advanced Fee Fraud 1995

⁸⁷ Data Protection Act (DPA) of 2018

⁸⁸ Copyright Act 2019.

⁸⁹ Computer fraud and abuse Act, 1986

1994 and 2001 by the Patriot Act which reduced the misuse of technology devices. The USA federal crime code describe cybercrime as Fraud and related activities in linking with access device, in connection with computers and communication lines or systems. In 1980 the USA established the US privacy protection act 1980 which saw to protecting people's right to privacy saved on a computer or electric database or storage. The electronic communication privacy act secures the privacy rights of customers and subscribers of network providers. Criminals are progressively moving online as the global population becomes relying on Digitalization.⁹⁰ The FBI predicted that in 2020 alone, cybercrime cost the US economy over \$4 billion. As the epidemic progressed, cyberattacks increasingly knocked essential services down, including those that were offered by medical professionals. Malicious hackers are able to take advantage of loopholes in technological advances and consumer carelessness about security for easy money because of lax regulation and enforcement by nation-states. Stealing of intellectual property hampers American innovation and costs businesses billions of dollars in damages, while ransomware has the potential to affect crucial industries, harm national and economic security, and disrupt American life. Cybercriminals attack the basic principles of our contemporary information society by taking advantage of the anonymity, confidentiality, and interconnection given by the Internet. Botnets, computer viruses, cyberbullying, cyberstalking, cyberterrorism, cyberpornography, distributed denial of service attacks, hacktivism, identity theft, spyware, spam, and a wide variety of other online crimes all fall under the umbrella of cybercrime. Cybercriminals are a serious threat to the global economy, and law enforcement agencies have had a hard time keeping up with them. The police are making an effort to utilize the same tools that cybercriminals use in an effort to stop cybercrime and apprehend those responsible for it. The economic and societal effects of cybercrime are discussed once a definition of the term is provided. Cyberbullying and cyberpornography, two notably emblematic forms of cybercrime, are then explored at length, and finally, strategies for limiting the spread of cybercrime are discussed. USA established the paperwork reduction act, 1995 which was to recognize the transmission of information through computer and the internet the act was amended to become the information technology management reform act 1996 which laid down guidelines for security agencies to start using electronic devices to store or keep information. In 2014 the USA passed 5 laws to

⁹⁰ Jarret M., Bailie M., "Prosecuting Computer Crimes" (Published by Office of Legal Education Executive Office for United States Attorneys) <<http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>> Accessed 9th April 2023

protect businesses, individuals and the government in the cyberspace, National Cybersecurity Protection Act (NCPA), Cybersecurity Enhancement Act of 2014 (CEA), Federal Information System Modernization Act of 2014 (FISMA 2014), Cybersecurity Workforce Assessment Act (CWWA), and the Border Patrol Agent Pay Reform Act (BPAPRA).⁹¹

The US government has made strict laws to help organizations secure their data and information from cyber criminals.⁹² Although based on English common law, American criminal law has been modified to reflect local realities. Most states in the United States no longer use the common law of crimes due to legislative action. The result of these measures is that no one may be prosecuted for a crime that isn't explicitly included in the state's statutes. However, even in these jurisdictions, common law concepts remain influential due to the fact that criminal legislation are often just codifications of the common law and their contents are read in light of the common law. In the remaining states, it is possible to face criminal charges for a common-law violation that is not explicitly prohibited by state legislation. Some state criminal codes and the federal criminal code are nothing more than collections of laws, with little attempt to link them to one another or to develop or execute any philosophy of control through punitive measures. As with other types of crimes, the United States has its own set of federal laws pertaining to cybercrime. Although there were provisions in the federal criminal code relating to the wire and mail fraud, they were unable to combat the new computer crimes as they emerged in the early 1980s, when law enforcement agencies first began grappling with the dawn of the computer age and the emergence of computer-related criminal activity.

This resulted in the creation of legislation to punish cybercriminals. Therefore, rather than amending pre-existing statutes to include new computer-related elements, Congress passed a new legislation to cover all federal computer-related crimes. The attempts to pass new legislation resulted in 1986's fraud and Abuse Act (CFAA). This regulation pertains to the safety of computer networks. Federal networks and Internet-connected PCs are safe. They are safe against intruders, vandalism, espionage, and being used dishonestly in frauds thanks to this. It's not a sweeping legislation; rather, it patches up the protections offered by existing federal criminal statutes. The Act covers a wide range of acts relating to computers, including malicious communication with knowledge, reckless access, negligent access resulting in

⁹¹ Cyber Crime - United states department of justice, http://www.usdoj.gov/criminal/cybercrime/1030_anal.html

⁹² A glance at the United States cyber security laws, <https://www.appknox.com/blog/united-states-cyber-security-laws>

harm and loss, trading in passwords, and computer-related extortion.⁹³ The Act provides for civil proceedings to be brought against offenders for compensatory damages and injunctive or other equitable reliefs on behalf of victims who have suffered certain forms of loss or harm as a result of violations of the Act. Damage to a government computer system used in the administration of justice, national defence, or national security; loss to one or more persons in any 5-year period 1; and loss similar to or identical to the only loss for purposes of an investigation, prosecution, or other proceeding brought by the only. All electronic communications, including those transmitted over computer networks, are protected under the Electronic Communication Privacy Act, a law that was enacted as an amendment to the Wiretap Act. The law prohibits any entity, including the police, from engaging in unlawful interception or disclosing or using information received via illegal interception, and it does so on both a substantive and procedural level. Intercepting or attempting to intercept a wire, oral, or electronic communication is a crime under Section 2511(1)(a) of the Wiretap Act. However, intent must be proved before a breach of this rule may be proven.⁹⁴ In a case involving the civil wiretap act, the Fourth Circuit upheld the use of the following standard jury instruction defining “intentional”.

*“An act is done intentionally if it is done knowingly or purposely, that is an act is intentional if it is the conscious objective of the person to do the act or cause the result. An act is not intentional if it is the product of inadvertence or mistake. However the defendant’s motive is not relevant and the defendant needs not to have intended the precise results if its conduct or have known its conduct violated the law” (Abraham v County of Greenville).*⁹⁵ It follows that in cases of interceptions committed by careless third parties., Section 2511(1)(a) will not apply.

Section 2511 (1) (c) of the act also provides that *“Except as otherwise specifically provided in this chapter any person who intentionally discloses, or endeavour’s to disclose, to any other person the contents of any wire, oral, or electronic communication in knowing or having reason to know that the information was obtained through the interception of a wire,*

⁹³ 1986's fraud and Abuse Act

⁹⁴ Section 2511(1)(a) of the Wiretap Act

⁹⁵ Abraham v County of Greenville

*oral or electronic communication in violation of this shall be punished as provided in subsection (4).*⁹⁶ This section provides for two mental state requirements.

The act of disclosing a communication must be done ‘intentionally’ and it must also be proved that the disclosing individual knew. Although the act’s major enforcement tools are its civil and regulatory provisions, the CAN-SPAM ACT of 2003 (commonly known as the “spam legislation”) also creates many new criminal charges to prosecute individuals responsible for sending significant quantities of unsolicited commercial email. Any of the following applies if you send multiple commercial emails : (i) without authorization access a protected computer to send them; (ii) send them through a protected computer to hide their origin; (iii) materially falsify header information; (iv) materially falsify registration information for five or more email accounts; (v) falsely represent yourself as the registrant of two or more domain names; (vi) falsely represent yourself as the registrant of five or more intellectually distinct names. The severity of the consequences for breaking Section 1037 depends on the specifics of the violation and any prior convictions that are relevant. It might be anything from one year to five years.⁹⁷ In England, the law holds the offender accountable regardless of the medium in which the crime was committed.

3.2.2. The Computer Fraud and Abuse Act 2020

The original intent of the law was to safeguard federal government computers together with those of financial and medical organizations. The Act forbids unauthorized use of a publicly accessible computer for the purpose of obtaining information that ought to be kept private, such as credit records, etc. Password trading for government or military networks is likewise illegal. Yet, as seen by a slew of changes made recently, Computers “used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects the interstate or foreign commerce or communication of the United States,” are considered “protected computers,” and any unauthorized or unlawful access to these computers is a crime.⁹⁸ This technically makes all Internet-connected computers across the globe subject to the provisions of the Computer Fraud and Abuse Act. A police detective was found guilty of illegally accessing the NCIC database of the FBI and the SSA and of encouraging others to do the same in *U.S. v.*

⁹⁶ Wire tape Act Section 2511 (1) (c)

⁹⁷ Can-Spam Act Of 2003

⁹⁸ The Computer Fraud and Abuse Act 2020

Pederson, the transfer of "a program, information, code, or instruction to a computer or computer system" with the goal to destroy or cause damages to, or to withhold or refuse the use of a computer, computer services or networks, information, data, or program is also prohibited under the Act's provisions. Several forms of the actus reus of cybercrime fall under this stipulation.⁹⁹ Hacking, the spread of viruses and other dangerous programs, and unauthorized access are all explicitly forbidden by this Act. Another example included a first-year graduate of Cornell University's Computer Science Ph.D. program who created and deployed a worm that crippled computer networks in many states. He was found guilty, fined \$10,500 plus the cost of supervision, placed on probation for three years, and ordered to do 400 hours of community service.

3.2.3. Wire fraud Act 1994

The Supreme Court's decision in *U.S. v. Cassiere* established the elements necessary to establish wire fraud: "a plot to defraud by means of false pretences," "the defendant's knowing and deliberate involvement in the scheme with the purpose to defraud," and "the use of interstate wire communications in furtherance of the scheme."¹⁰⁰ Scammers' Use of Wires in Their Scheme computer systems are now included in legislation. *U.S. v. Riggs* alleges that the defendant accessed a computer belonging to Bell South Telephone Company from his house, then downloaded a text file outlining the company's improved 911 system. The plan was to utilize it to defraud unsuspecting victims by hiding the theft and publishing the information on a computer bulletin board in Illinois with the aid of a partner. He was found guilty.¹⁰¹

3.2.4. The Computer Misuse Act (CMA) of 1990, The Computer Fraud and Abuse Act, as revised by the Police and Justice Act of 2006, is the only law that specifically addresses computer crimes. illegal access to computer material, illegal access to a computer system with the aim to conduct or enable future crimes, and unlawful alteration of computer material are the three primary offenses created by the legislation. For such violations, the maximum punishments are imprisonment for six months and/or a fine of 500 Euros, or imprisonment for ten years and/or an infinite fine. There have been recent amendments to the CMA, such as those included in "Miscellaneous part 5 computer Misuse modifications" of the Police and

⁹⁹ *U.S. v. Pederson*

¹⁰⁰ *U.S. v. Cassiere*

¹⁰¹ *U.S. v. Riggs*

Justice Act. The original punishment for hacking into a computer system was 5 years in prison, however this has been doubled to 10 years under Clause 39.¹⁰² The Obscene Publication Act of 1964 is the key piece of law that makes it illegal to print information that encourages depravity and corruption. According to the law, it is against the law to own or distribute child pornographic material because of how offensive it is.¹⁰³

3.2.5. Criminal Justice Act of 1988 and the Protection of Children Act of 1978.

Having any obscene photographs of children in your possession is illegal.¹⁰⁴

There are laws against inciting hatred based on race and religion as well.¹⁰⁵

3.2.6. The Racial and Religious Hatred Act of 2006 received royal assent on February 16, 2006. Section 21 of this law makes it illegal to publish or distribute material that is threatening, abusive, or insulting if doing so is intended to stir up racial hatred or, taking into account all the circumstances, racial hatred is likely to be stirred thereby. A violation of this law would result in criminal penalties for the offender. Threatening someone because of their religion or inciting hate against someone because of their religion is prohibited. Sending a letter, electronic communication, or other article that could be construed as indecent, offensive, or threatening to another person is illegal in England under Section 1 of the Malicious Communications Act 1988¹⁰⁶, and under Section 1 of the Communications Act 2003, it is illegal to send a letter, electronic communication, or other article that sending an indecent, offensive, or threatening telephone message is also a crime under Section 43 of the Telecommunications Act of 1984; similarly, the England copyright law also provides for criminal sanction in certain situations.¹⁰⁷ However, most copyright criminal offenses in England are covered by the Copyright Designs and Patents Act of 1998, which allows for civil remedies to compensate wronged intellectual property right holders (CDPA), care about business and commerce.¹⁰⁸

¹⁰² The Computer Misuse Act (CMA) of 1990

¹⁰³ Obscene Publication Act of 1964

¹⁰⁴ Criminal Justice Act of 1988

¹⁰⁵ Protection of Children Act of 1978.

¹⁰⁶ Malicious Communications Act 1988

¹⁰⁷ Telecommunications Act of 1984

¹⁰⁸ Copyright Designs and Patents Act of 1998

3.3.1. Cybercrime Legal Framework in UK

When a legislation was finally passed in England in 1990, it was the first of its kind in Europe. There are now three additional crimes thanks to the Computer Misuse Act: breaking into a system without permission; breaking into a system with the intent to conduct or facilitate the commission of another crime; and altering digital data (ss. 1, 2, and 3). The Serious Crime Act of 2007 and the Police and Justice Act of 2006 (both of which took effect in October of 2008) are two recent pieces of legislation that have updated this law. The scope of the changes will be addressed in more detail below. In the United Kingdom, crimes committed on a computer are also punishable under the Criminal Damage Act of 1971. The child pornographic material offenses are defined under the Protection of Children Act of 1978, as revised by the Criminal Justice and Public Order Act of 1994, Part 4. Forgery and counterfeiting are covered under the Forgery and Counterfeiting Act of 1981 and the Fraud Act of 2006, respectively; the Copyright and Rights Related Statutes are also applicable. The United Kingdom, like many other governments throughout the globe, is becoming more concerned about cybercrime. The government of the United Kingdom has established the National Cyber Security Centre in response to the problem's severity (NCSC). The National Cyber Security Centre (NCSC) is tasked with reacting to and investigating cyber intrusions, as well as offering advice and assistance to the public and commercial sectors. Organizational goals also include spreading education about cybercrime and encouraging safe internet habits. The number of reported cases of computer abuse in the United Kingdom rose by 16 percent in 2020, according to data compiled by the country's Office for National Statistics (ONS). All sorts of cybercrime are included here, from hacking to viral assaults. The survey also identified an alarming rise in phishing schemes, in which the perpetrator poses as a reputable organization in order to trick its targets into divulging important information.

The government of the United Kingdom has launched many efforts to reduce cybercrime, including CyberFirst, which promotes employment in cybersecurity among young people. Law enforcement has also received more resources to help them track down and punish cybercriminals. Cybercrime is still a major problem in the United Kingdom, but the administration and other groups are working to combat the issue and safeguard citizens and companies. Protecting oneself online requires constant vigilance and the adoption of best practices, such as the use of complex passwords, the avoidance of questionable emails and links, and the regular updating of software and security systems. The United Kingdom is another country that takes the fight against cybercrime seriously. This is likely because it has

been the target of cybercriminals, who have exploited gaps in conventional crime laws to launch innovative attacks.

3.3.2. In R v. Gold and Schifreen, In England, for example, the Court of Lords found that stealing or otherwise misusing a legitimate user's password in order to access data stored on a computer was not a crime. It was not possible to establish any of the conventional property offenses under the Theft Act of 1968 or 1978 since there was no general crime of impersonation under English law. The Forgery and Counterfeiting Act of 1981 was considered for possible use in this scenario; however, a previous prosecution under this law, although first successful, was reversed on appeal. As it would be difficult to show dishonest or malevolent intent at the moment of access or that a crime subsequent upon access had been committed, the likelihood of successfully prosecuting a hacker or other computer misuser was significantly reduced. To address the gap, lawmakers established the Reform Committee in 1988 to examine the pre-existing canonical laws and propose replacements. As a result, in 1990, lawmakers passed the Computer Misuse Act. The United Kingdom has a amount of cybercrime laws and principles in force. Cybercrime-related laws and activities in the UK include:

3.3.3. Computer Misuse Act of 1990, Intrusion into a computer system without permission, as well as the modification, damage, or destruction of data stored on such systems, is unlawful under the Computer Misuse Act of 1990. The act also criminalizes the creation and dissemination of computer viruses. The Computer Misuse Act (CMA) of 1990 is a British statute that defines certain computer-related crimes. The law was created in response to the growing utilization of computers and networks, together with the attendant requirement to safeguard against them being breached, tampered with, or destroyed.

The CMA defines three main criminal offenses related to computer misuse:

1. **Unauthorized access to computer material:** This offense refers to the act of accessing a computer system or data without permission. This can include hacking into a system, stealing passwords or other credentials, or using someone else's account without their permission.
2. **Unauthorized access with intent to commit or facilitate a crime:** This offense is similar to the first, but with the added element of criminal intent. In other words, the

individual must have accessed the system with the intention of committing a further crime, such as theft or fraud.

3. Unauthorized modification of computer material: This offense refers to the act of altering or deleting computer data without authorization. This can include deleting important files, changing or manipulating data, or planting viruses or other malware.

The CMA carries significant penalties for those found guilty of these offenses, including fines and imprisonment. The law has been updated several times over the years to keep pace with changes in technology and the evolving nature of cybercrime.

3.3.4. Investigatory Powers Act of 2016, Law enforcement agencies in the United Kingdom now have the right to access and monitor electronic communications including emails and social media postings under the terms of the Investigatory Powers Act of 2016. The Investigatory Powers Act (IPA) of 2016 is a piece of legislation in the United Kingdom that establishes rules for the monitoring and interception of communications by government agencies. The law has been described as one of the most controversial and far-reaching surveillance laws in the world. The IPA gives police and intelligence agencies the power to collect and retain communications data, such as phone records, internet browsing histories, and email records, as well as intercept and monitor communications. It also allows the government to require telecommunications companies to store records of their customers' communications for up to 12 months. The law requires a warrant from a senior judge before law enforcement or intelligence agencies can carry out surveillance, but critics have raised concerns that the safeguards are insufficient to protect individual privacy. The IPA also allows the government to issue “bulk warrants” to intercept large amounts of data, which some argue could be used to collect information on innocent individuals.

In addition to the controversial surveillance powers, the IPA also includes provisions to strengthen the oversight of intelligence agencies and increase transparency around their activities. It establishes a new Investigatory Powers Commissioner to monitor the surveillance powers and mandates yearly reporting on their usage.

The IPA has been the subject of ongoing legal challenges by civil liberties groups, who argue that it infringes on the right to privacy and freedom of expression. In 2020, the European Court of Justice ruled that parts of the IPA were incompatible with EU law, but the UK government has argued that the ruling does not affect the operation of the law.

3.3.5. Cyber Essentials is a government-backed program that recommends a baseline set of cybersecurity best practices for enterprises to use in order to ward off the most frequent forms of cyberattack. The United Kingdom government introduced the Cyber Essentials certification program in 2014. The program's goal is to assist firms of all sizes in implementing best practices in cybersecurity and protecting themselves from prevalent cyber threats. Organizations seeking Cyber Essentials certification must first perform a self-assessment questionnaire and an external vulnerability scan to identify areas of IT security that might need improvement. The assessment covers five key areas of cybersecurity:

1. Internet gateways and perimeter firewalls
2. safe setup
3. Managed access for users
4. Security against Malware
5. Patch administration

Organizations that meet the Cyber Essentials standards are awarded certification, which they can use to show their customers, suppliers, and other stakeholders that they've taken basic cybersecurity precautions to keep themselves safe. The Cyber Essentials Plus certification is an upgrade from the basic Cyber Essentials certification, which requires a more rigorous external vulnerability scan and an on-site assessment by a qualified assessor. The Cyber Essentials scheme is seen as an important step in improving cybersecurity for businesses and organizations in the UK, and it is often used as a baseline for cybersecurity requirements in government contracts and tenders.

3.3.6. The National Cyber Security Centre (NCSC) is a department of the United Kingdom government responsible for advising private companies and people on cyber security. It also helps in the case of a cyberattack and in the aftermath. The NCSC's CyberFirst initiative is designed to train and educate the next generation of cybersecurity experts in the United Kingdom. In 2016, the government of the United Kingdom created the National Cyber Security Centre (NCSC) to serve as a hub for coordinating the country's cybersecurity initiatives. The National Cyber Security Centre is part of GCHQ, the UK's intelligence and

security organization. The NCSC has a range of responsibilities related to cybersecurity, including:

1. Providing guidance and advice on cybersecurity to businesses, organizations, and individuals.
2. Leading the UK's national response to cyber incidents, working with other government agencies and law enforcement.
3. Conducting research and development to improve cybersecurity capabilities and understanding.
4. Providing support and assistance to government departments and critical national infrastructure providers to improve their cybersecurity.
5. Promoting cybersecurity awareness and education across the UK.

The WannaCry ransomware assault on the NHS in 2017 and the hack on the UK's energy industry in 2018 are just two examples of high-profile cyber disasters in which the NCSC played a pivotal part in the response. To better coordinate cybersecurity activities and to encourage a collaborative approach to confronting cyber threats, the NCSC works closely with other government agencies, law enforcement, and the commercial sector. Additionally, the organization is in charge of putting the United Kingdom's National Cyber Security Strategy into action, which details the government's plan to strengthen cybersecurity across the nation.

3.3.6. The United Kingdom's Data Protection Act of 2018 establishes rules for the handling of private information and mandates that businesses use safeguards to prevent data breaches, loss, or theft. Together, these measures show the United Kingdom's dedication to combating cybercrime and safeguarding its citizens and companies from its negative impacts. Yet, these rules and regulations must be evaluated and revised on a regular basis to keep up with the constantly shifting danger environment posed by cybercrime. Personal information in the United Kingdom is protected under the Data Protection Act (DPA) of 2018. The new legislation supersedes the 1998 Data Protection Act and was enacted to make UK law consistent with the General Data Protection Regulation (GDPR) of the European Union. The

DPA sets out a number of requirements for organizations that collect, use, and store personal data, including:

1. Data protection principles: Organizations must adhere to six principles of data protection, which include requirements for data to be processed lawfully, fairly and transparently, and for data to be kept accurate and up-to-date.
2. Legitimate business interests or the data subject's permission are two examples of valid bases for processing that businesses need to comply with data privacy laws.
3. Data subjects have rights under the DPA to access their data, have erroneous data rectified, and have their data destroyed under certain conditions, among other rights.
4. Data breaches: Companies must notify the Information Commissioner's Office (ICO) within 72 hours of discovering a data breach of a specified sort.
5. Data transfers beyond the UK and the EEA: The DPA establishes standards for such transfers, including the need of organizations to put in place necessary measures to secure the data during transmission.

The DPA vests enforcement of data privacy rules and the authority to levy penalties in the hands of the ICO. Organizations may be fined up to the greater of £17.5 million or 4% of their worldwide revenue. The DPA is a useful instrument for safeguarding private information and making businesses answerable for their data security policies and procedures.

In conclusion, in this chapter, we looked at the numerous Nigerian and U.S. regulations and agencies that deal with cybercrime. Apart from the Cybercrime Act, these other acts and organizations would go a great way toward addressing especially internet-related fraud, while they are not ideal. The next chapter would evaluate the legal framework in Canada, universal view of Cybercrime and a comparative analysis of cybercrime in these countries.

CHAPTER IV

Canada Legal Framework on Cyber Crime and Universal View of Cybercrime

4.1. Canada Legal Framework on Cyber Crime

When it comes to criminalizing cybercrime, Canada was an early adopter of criminal law. When it comes to implementing rules to combat cybercrimes, a United Nations-sponsored network of internet policy professionals found that Canada was in the top five. Canada has joined other countries in signing the Convention on Cybercrime.¹⁰⁹ Each signatory state is responsible for prosecuting cases of domestic cybercrime. The difficulty of applying current regulations to illegal actions employing new technology is a significant obstacle for law enforcement. Therefore, even if the attacker is located in another nation, the victim's computer system might be considered to be within the jurisdiction of the claiming country. Legislation in this area must balance the need to safeguard internet users with the need to avoid undue limits on the transborder movement of data.¹¹⁰ To address illicit use of IT, existing law has been utilized and updated. The prevailing view is that criminal activity is criminal activity regardless of whether or not a computer was involved. Crimes using computers and networks are addressed in the most recent version of Canada's "Criminal Code," which was revised in 2005.¹¹¹ Any criminal activity using a computer or data in Canada is considered a violation of Section 430 or 342.1 of the Canadian Criminal Code.¹¹²

¹⁰⁹ Kowalski M., "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics" *Canadian Centre for Justice Statistics* <<http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf>>Accessed 6th April 2023

¹¹⁰ Article 22 Canadian Criminal Code

¹¹¹ Canadian Criminal Code 2005

¹¹² Section 430 or 342.1 of the Canadian Criminal Code.

The law allows for a variety of data-related mischief, including hardware damage, data deletion or modification, and the use of “logic bombs.” Any person who knowingly destroys or alters computer data; makes computer data meaningless, useless, or ineffective; obstructs, interrupts, or interferes with the lawful use of computer data; or denies access to computer data to a person who is entitled to access it is guilty of mischief and subject to life in prison if the mischief caused actual danger. In this way, the distribution of a virus may constitute a crime even if the virus has not yet been activated, as per Section 5.1 of the criminal code. However, there is no law expressly prohibiting the creation or dissemination of computer viruses.¹¹³ If an action or inaction is likely to constitute harm in respect to life, property, or computer data, then it is an offense under this provision. Computer fraud and other forms of economic crime are likewise codified under the penal code. Credit card and bank account fraud, forgeries, and other similar crimes fall under this category. The Canadian judicial system has determined that any item that might be regarded property can be the target of theft or fraud. The Ontario Court of Appeal ruled in *Regina v. Stewart 1988* that stealing a computer printout of a hotel union's employees' names and contact information was theft.¹¹⁴ In *Turner and the Queen 2019*, the most recent Canadian case concerning computer-5 connected criminality, the Ontario High Court harmonized the absence of government action with judicial enlargement of the definition of property.

The defendants in *Turner* “accessed computer tapes and tampered with the program stored on the tapes, rendering the program inaccessible to other users without first getting the new program code.” As a result of their acts, the court determined that the defendants prevented other parties from successfully retrieving material from the tape.¹¹⁵ Officials from the international organizations Federal government Canadian Organizations and Businesses are able to better communicate and network with one another because to OCIEP’s dissemination of information, advice, and training opportunities.

4.2. Impact of Cyber Crimes

The implications of cybercrime on individuals, corporations, and governments are significant. Since the privacy and security of users are taken into account when designing and developing

¹¹³ Section 5.1 of the criminal code

¹¹⁴ *Regina v. Stewart 1988*

¹¹⁵ *Turner and the Queen 2019*

websites, applications, and communication platforms, it is difficult to detect or identify cybercrimes. It is the user's decision as to how to put the technology to good or bad use, hence the technology itself is considered neutral. Focusing on cryptography, it is used to safeguard money transfers, data storage, and communication, but it may also be used in unlawful operations if the trail of evidence is difficult to follow. The victim of a computer crime may not even be directly involved in the attack. No signs of fight or violence during the crime, both of which are commonplace in conventional crime scenes.¹¹⁶ Everyone is at risk from cybercrime since it just takes a few clicks of a mouse to commit. It is fairly uncommon for victims of cybercrime to be completely unaware of the fact that they have been victimized.

While banks are a prime target for sophisticated hackers, even the most secure corporations have become victims of cybercrime. Financial institutions incur substantial expenses due to cybercrime as they work to prevent and detect fraudulent transactions and theft.¹¹⁷ According to a survey by Kaspersky Lab, financial institutions invest much more money on cybersecurity.¹¹⁸ The majority of funds taken by hackers are untraceable, and this is a major concern for bank authorities all over the globe. Hiring a cyber-security specialist is a costly investment for any business that wants to defend itself from online criminals, as it requires the identification of risks, the development of a new and more secure operating technique, and the acquisition of more secure software and hardware. The prices of products and services are sometimes increased to cover these expenditures. Criminals are taking advantage of the digitization of government services by making false claims and stealing money. Cybercriminals are always developing new methods of attacking governments, hacking agencies, and organizations in order to spy on officials, steal sensitive data, and open backdoors into networks. Criminals and aggressive states, including China, Russia, Iran, and North Korea, pose a threat.¹¹⁹ Cyberterrorism may be defined as an act of criminality against a state. Most of the time, terrorist groups or hostile foreign governments are behind

¹¹⁶Hemraj Saini, Yerra Shankar Rao, Panda T.C., "Cyber-Crimes and their Impacts: A Review" *International Journal of Engineering Research and Applications*, 2(2) (2012) 202-209.

¹¹⁷ Sumanjit Das, Tapaswini Nayak, "Impact Of Cyber Crime: Issues And Challenges" *International Journal of Engineering Sciences & Emerging Technologies*, 6(2) (2013) 142-153

¹¹⁸ "Things to do before the next big thing: How the financial industry reacts to cyber threats," <https://www.kaspersky.com/blog/how-the-financial-industry-reacts-to-cyberthreats/6610/#mktoForm_10582>Kaspersky, 23 March, 2023

¹¹⁹ Wall David, "Cybercrime: The Transformation of Crime in the Information Age" (1st, Polity press, 2007)

cyberattacking. Crime prevention organizations were not successful in halting the spread of "cybercrime," and its effects are still having a devastating effect on economies throughout the world. Cybercrime presents a global systemic risk, but it has also spawned a large number of "419" criminals, who constitute a direct danger to our economy. Incredibly large amounts of money may be stolen from people locally and internationally via economic crime committed through the internet.¹²⁰ Online banking theft is on the increase as dishonest bank employees work with third parties to steal customers' money.

Many Nigerians, especially young ones, are involved in international financial fraud over the Internet. These scams target both individuals and businesses in other countries. Cybercriminal activity has resulted in the creation of instant millionaires and even billionaires in our economy, which is bad for growth since much of the money isn't being used productively. The police would have a hard time tracking down such a large sum of money. The damage that cybercrime does to economies is immeasurable. The effects of the rise in cybercrime, which strikes equally at Nigeria's well-to-do and poor, can hardly be exaggerated.¹²¹ Since most people were forced to move their businesses and other operations online due to the COVID-19 infection and worldwide lockdowns, cybercriminals were able to take advantage of the surge in online transactions that resulted from the new normal. Cybercrime in Nigeria increased by 54% between 2017 and 2018, with an estimated annual loss of N250 billion in 2017 and N288 billion in 2018. This is an increase of 28,227 cybercrimes each month. The banking sector was another hardest hit industry in Nigeria, losing N15 billion (\$39 million) to e-fraud and cybercrime in 2018 an increase of 537% from the N2.37 billion loss recorded in 2017. These numbers suggest that the Cybercrime Act 2015 failed to reduce banks' vulnerability to cybercrime. Phishing and identity theft accounted for the vast majority of these crimes.¹²²

Common types of cybercrime include stealing customers' Bank Verification Numbers (BVNs), making unsolicited phone calls or sending fraudulent texts to ask for sensitive information (such as account numbers), and breaking into bank networks in order to commit fraud. A gang going by the name "anonymous" was recently accused of hacking into the

¹²⁰ Munanga Albert, "Cybercrime: A New and growing problem of older adults" *Journal of Gerontological Nursing*, 45(2) (2019)3-5

¹²¹ Samuel Onyekanmi, Nigerian National Bureau of Statistics 2021. Accessed 21st March 2023

¹²² Akinyetun Tope Shola, "Poverty, Cybercrime and National Security in Nigeria" *Journal of Contemporary Sociological*, 1(2) (2021) 1-21

websites of major financial institutions and sharing the information to Nigerians during a demonstration against police brutality. This demonstrates Nigeria's financial institutions' vulnerability to cybercrime. Furthermore, cybercrime has had a significant detrimental influence on E-commerce in Nigeria. This has grown more common as a result of the proliferation of many internet platforms for purchasing and doing other transactions. There has been an increase in cybercrime because the e-commerce market is less strictly regulated than the banking sector, which is required to report cybercrime to the Central Bank of Nigeria (CBN) or face penalties in accordance with the Banking and other financial institution Act (BOFIA).

Hackers have also affected cyberspace's intellectual property. To the average Nigerian, “copyright” means very nothing. When intellectual property is copied and distributed without permission, this is known as piracy. In Nigeria, the proliferation of the internet and other technical breakthroughs have provided a means for the untraceable, cost-free, and illegal distribution of pirated works. Sales fraud, also known as sales forgery, occurs when counterfeit versions of legitimate items are sold to consumers.¹²³ This is more evidence that hackers in Nigeria are always adapting and developing novel techniques to carry out their malicious goals. Cybercrime has had a devastating effect on Nigeria, both economically and in terms of the country's international standing.

4.3. Universal View of Cybercrime

Cybercrime, due to its transnational nature, necessitates international enforcement since it may harm anybody, regardless of whether they are close to or distant from the location where the crime was committed. Cybercrime Convention in Europe.¹²⁴ Was an admirable effort that established standards for member states to follow in their fight against and response to cybercrime. Incorporating national laws, enhancing investigative tactics, and expanding international collaboration, it was the first international pact of its kind to deal with Internet and computer crime. The most widespread kind of cybercrime is acts of cyberterrorism. Digitization made possible by Internet networks enables almost rapid information transfer,

¹²³ Ames Morgan G., “Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning” 2(18) (2018)1-19

¹²⁴European Patent Convention 1973

yet cybercrime knowledge is low. The convergence of the Internet with other digital infrastructure enables global, mobile access (as the need for massive data centres is replaced by smaller devices like laptops and smartphones). The 'instantaneity' of viruses and malware has increased with the mobility of information transmission due to globalization of space and time. If the metaphor of “virus” is extended beyond its original public health context, then viruses in the present day are very contagious and spread rapidly.

Since the worldwide revolution and innovation in the ICTs business, cybercrime has become a more prominent and dangerous international crime. Common fraud schemes include the thieves obtaining personal information via phishing or spoofing. To perpetrate fraud or theft, the impostor poses as the victim and steals their identity. Identity theft and hacking are also used in crimes involving health care and insurance. Recent research has revealed that cybercrimes vary from traditional crimes in many key respects, including their low barrier to entry (learn how to do one in a weekend) and low resource requirements (a mobile phone can do a lot of harm) Successful cybercrime, such as the Lizard Squad's breach of Malaysia Airlines' website, does not need the offender to be physically present in the country in which the crime is committed. Teenagers from the United States, Finland, and the Netherlands called “lizard squad” perpetrated the hack in Malaysia.¹²⁵

4.4. An Evaluation of The United States' Cybercrime Legal Framework in Context of Other Countries

The Cybercrime Act, in contrast to US law, does not address spam emails at all. Section 15 of the Act covers the only offense of sending excessively insulting, vulgar, obscene, or inaccurate communications with the intent to annoy or harm any person, property, reputation, or extort. The term “cyberstalking” refers to the practice of stalking or harassing an individual, group of individuals, or organization over the Internet or other electronic means for the purposes of this law. This interpretation provision (Section 42) has the aforementioned definition. I sending multiple emails, often in a systematic fashion, with the intent to annoy, embarrass, intimidate, or threaten another person or to cause that person to fear for her or her

¹²⁵ “Krebs on security article on Lizard Squad" < <https://krebsonsecurity.com/2014/12/lizard-kids-a-long-trail-of-fail/>> Accessed 15 March,2023

family's safety; making false accusations, threats, monitoring, identity theft, data or equipment damage, solicitation of minors for sex, or gathering information with the intent to harass.

Spam emails are not included here. Although the sender of "email spam" may have no ill intent toward the receiver of the message, the practice of sending massive amounts of unsolicited commercial email is nevertheless known by this pejorative word.¹²⁶ In today's world, viruses lurking in spam may even be hidden from the sender. In light of the fact that email spam is explicitly legalized under the CAN SPAM Act's Section 1037 in the American legal system, it is sufficient to argue that the Cybercrime Act is insufficiently wide with regard to cyberstalking. The Act allows for a jail sentence of one to five years, depending on the nature of the offense and the offender's prior record. In addition, the victims of certain types of loss or damage caused by violations of the American Computer Fraud and Abuse Act (CFAA) may bring civil actions against the violators for compensatory damages and injunctive or other equitable reliefs under the CFAA, while the victims of cybercrime may not do so under the Cybercrime Act. According to Section 31 of Nigeria's Cybercrime Act, the assets are now the government's property.¹²⁷ In a civil action launched under Section 1030(g) of the CFAA, the plaintiff may seek any appropriate equitable relief. Unfortunately, the Cybercrime Act does not do enough to help victims of cybercrime. Judges are not required to participate in training programs, despite Section 24(3) of the Cybercrime Act mandating such training for law enforcement, security, and intelligence agencies. This is likely to impede the effective implementation of the Cybercrime Act. For instance, Section 27(3)(d) of the Cybercrime Act specifies that a court must be convinced that there are reasonable reasons for suspecting that the person named in the warrant is preparing to commit an offence under this Act before issuing a warrant under paragraph 2 of that section.¹²⁸ The judge hearing the request may not be well-versed in cybercrime and data security, and therefore could not know whether or not there is "reasonable basis" to infer that the person named in the warrant is intended to commit an offense under this Act. Therefore, judges with proper knowledge of computer crimes and cyber security are essential to the effective implementation of the Act. However, as mentioned in Sections 8 and 9, the Cybercrime Act does not outlaw the creation and distribution of computer viruses, only the modification of

¹²⁶ CAN SPAM Act under Section 1037

¹²⁷ Section 31 of the Cybercrime Act

¹²⁸ Cybercrime Act's Section 27(3)(d)

computer data and computer systems by destructive programs like viruses. In this case, I use the Cybercrime Act of 2015 in Nigeria as an example. Since the Cybercrime Act encompasses almost all other cybercrime legislation in Nigeria.¹²⁹ The Cybercrime Act of Nigeria addresses the problem of preventing and punishing cybercrime, and it does so quite well. However, the legislation is not without its problems. A synopsis of the project and some recommendations for moving forward will follow.

In conclusion, the international legal framework of cybercrime in Canada has been examined in this chapter, the comparative analysis of the four countries and the universal view of cybercrime. While the cybercrime agreement would significantly contribute to reducing cybercrime on a global scale, it's worth may be questioned for one key reason. The ever-evolving nature of cybercrime means that the lengthy modification procedure necessitated by treaties poses a danger of prematurely fixing the law. The United States, the United Kingdom, and Canada all have legislative frameworks in place to fight cybercrime, but it is evident from this chapter that the United States' structure is the most robust and successful. The last portion of this research project will focus on suggestions and a summary of the findings.

¹²⁹ Nigerian Cybercrime Act of 2015

CHAPTER V

Summary, Conclusion, Recommendation According to Findings and Recommendation for Further Research

5.1. Summary

The research examined the international legal structure on cybercrime, focusing on the “convention on cybercrime,” and the domestic legal frameworks of the United States of America, the United Kingdom of Great Britain and Canada. The study endeavour also compared the major international jurisdictions, with special emphasis on the US jurisdiction, with the Nigerian legislation and organizations controlling cybercrime. Over the study's course, certain flaws and openings in Nigeria’s legislative framework controlling cybercrime became apparent. The ineffectiveness of the Cybercrime Act on combating virus production and dissemination, email spam, etc., are only two examples of the gaps that have been identified. Recommendations have been made to remedy these gaps in coverage in an effort to improve the situation.

5.2. Conclusion

By comparing and contrasting the many academic definitions of “cybercrime,” this study has provided a useful conceptual overview of the topic. Cybercrime was further distinguished from what are often referred to as “conventional crimes” by elaborating on its distinctive

features. Cybercrime was compared and contrasted with similar terms like “cyber-attack” and “cyber-warfare” in this study. In addition, the many forms of cybercrime were identified and defined, including but not limited to virus distribution, phishing, computer-related fraud, cyberstalking, and hacking. Focusing on the ‘convention on cybercrime,’ the Canadian, American, and British legal systems for dealing with cybercrime were explored. The study also compared the different foreign jurisdictions, with special emphasis on the United States’ jurisdiction, to the numerous Nigerian legislation and organizations controlling cybercrime.

Over the study’s course, certain flaws and openings in Nigeria’s legislative framework controlling cybercrime became apparent. The ineffectiveness of the Cybercrime Act non dealing with virus generation and dissemination, the ineffectiveness of the Cybercrime Act in dealing with email spam, etc., were among the noted gaps. Regarding these gaps, many suggestions have been made to aid in addressing the problem.

5.3. Recommendation According to Findings.

One last point: cybercrime poses a serious risk to worlds economy and national security. The results of the research reveal that the misuse of computers poses a threat to national security, endangers public safety, and may have devastating personal consequences. Nigeria, like many other African nations, struggles to successfully address cybercrime due to a lackluster legislative structure and enforcement. Based on the findings of this study, it is clear that Nigeria’s legislative framework governing cybercrime is far less extensive than that of other developed countries, especially the United States. Notwithstanding its relative superiority, the Nigerian legal system in this area has several gaps that have been highlighted in this paper.

To that end, it is argued that improving computer and cyber security in Nigeria, America, UK and Canada will be greatly aided by adopting the suggestions made in this chapter.

5.4. Recommendation for Further Research

Cyberspace legislation must be established with great accuracy to adequately address the actions of cybercriminals. Experts in the field of information technology should be present throughout the legislative process to ensure that legislation are drafted to reflect the state of the art. The general populace needs to be properly educated on the subject of safeguarding computer infrastructure and information. Anti-virus software and strong passwords, for instance, should be promoted to the general population. Sometimes, an intruder can make it

look as if they were the unaware victim by installing a virus on their computer or by gaining easy access to their computer due to inadequate security measures (such as a lack of a comprehensive firewall, passwords, and anti-viruses). The broad use of anti-virus software and password protection would significantly contribute to the improvement of computer security.

Section 8 of the Cybercrime Act covers the illegal modification of computer data, which would surely include the use of computer viruses to modify computer systems and data, but it does not include the creation and distribution of computer viruses. Expanding the scope of Section 8 of the Act will help combat cybercrime and improve computer security by addressing the creation and distribution of viruses. In addition, Section 15 of the Cybercrime Act, which deals with cyberstalking, should include sending a large number of unsolicited commercial emails (often known as “email spam”). It is suggested that training for judges be included to the Cybercrime Act's Section 24(3), which now provides for the training of law enforcement officials.

In addition, the members of the Cybercrime Advisory Council (Cybercafé) appointed under Section 25 of the Cybercrime Act should be required to participate in regular cybercrime training sessions so that they can stay abreast of the latest developments in the field and effectively apply them to their work. This is very relevant since both the form of cybercrime and the strategies for successfully preventing and prosecuting it are always evolving.

Section VI of the Act allows for law enforcement to conduct searches, arrest suspects, and file criminal charges against them; yet, this author believes that these provisions are insufficient to effectively prosecute cybercriminals. IT experts should be able to collaborate with law enforcement authorities during investigations, hence measures should be taken to facilitate this. Compensatory damages and other forms of remedy for victims of cybercrime should be included in the Cybercrime Act, just as they are in the United States under Section 1030(g) of the Computer Fraud and Abuse Act.

BIBLIOGRAPHY

- A. Fair Housing Council v. Roommates.com [2007]
- B. Federal Republic of Nigeria v. Chief Emmanuel & Ors
- C. R v. Gold and Schifreen, [1988] 2 WLR 984
- D. Regina v. Stewart 1988
- E. Turner and the Queen 2019
- F. Udokwu v. Onugha
- G. Yahoo vs. France [2006] 433 F. 3d 1199
- H. Cryer Robert, Robinson Darryl, Sergey Vasiliev, “An Introduction to International Criminal Law and Procedure” (4th ed, Cambridge University press, 2019).
- I. Marcum D. Catherine, Higgins E. George: Cybercrime (1st ed, HSSR 2019).
- J. Marcum Catherine D, George Higgins., “Cybercrime and deviances” (2nd ed, HSSR,2019).
- K. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, “Cybercrime, Digital forensic and Jurisdiction” (1st ed, Springer Cham, 2015).
- L. Robert W. Taylor, Eric J. Fritsch, John Liederbach, Michael R. Saylor, William L. Tafoya: Cyber Crime and Cyber Terrorism (4th ed, Pearson 2017).
- M. Thomas J. Holt, Adam M. Bossler: The Palgrave Handbook of International Cybercrime and Cyber deviance (1st ed, Palgrave Macmillan Cham 2020).

- N. Adam M. Bossler, Berenblum Tamar. "Introduction: New directions in cybercrime research." *Journal of crime and justice*, 42(5) (2019):495-499.
- O. Ames Morgan G., "Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning" 2(18) (2018)1-19
- P. Ames Morgan G., "Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning" 2(18) (2018)1-19.
- Q. Ashaolu, D., "Combating Cybercrimes in Nigeria" Basic Concepts in Cyberlaw, (Velma Publishers, 2012)
- R. Akhilesh Chandra, Melissa J. Snowe "A taxonomy of cybercrime: Theory and design" *International Journals of accounting information systems*, 38(1) (2020)40-46.
- S. Akinyetun Tope Shola, "Poverty, Cybercrime and National Security in Nigeria" *Journal of Contemporary Sociological*, 1(2) (2021) 1-21
- T. Azernikov A., Norkina A., Myseva E., Chicheroy K. "Innovative Technologies in Combating Cyber Crime" 1(2) (2021) 248-252
- U. Boireau Olivier, "Securing the blockchain against hackers" *Network security journal*, 2018(1) (2021) 6-8
- V. Boyle J., "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors" *University of Cincinnati Law Review*, 66 (1997) 177-178
- W. Brenner S., B.J. Koops, "Approaches to Cybercrime Jurisdiction" *Journal of High Technology Law*, 4 (1) (2004) 1-46.
- X. Chukwuedozie Ajearo k., "The effects of rural-urban migration on rural communities of southeast Nigeria" 2013
- Y. Carin M., Reep-van den Bergh, Marianne Junger "Victims of cybercrime in Europe: a review of victim surveys" Palgrave Macmillan 7(5) (2018)
- Z. Filippo Spiezia., "International cooperation and protection of victims in cyberspace: *welcoming Protocol II to the Budapest Convention on Cybercrime*" Era Forum, 23, (2022)101–108
- AA. Freund Ernest., "Classification and Definition of Crimes" *Journal of Criminal Law & Criminology*, 5(6) (1915):1-21
- BB. Gordon, S., & Ford, R., "On the definition and classification of cybercrime" *Journal of Computer Virology*, 2(1), (2006) 13-20.
- CC. George Christou "The challenges of cybercrime governance in the European Union" *European Union cyber security* 19(3) (2018)355-375

- DD. Goldsmith Andrew, Wall S. David “The seductions of cybercrime: Adolescence and the thrills of digital transgression” 19(1) (2019)
- EE.Goni Osman “Introduction to Cyber Crime” *International Journal of Engineering and Artificial Intelligence*, 3(1) (2022) 9–23.
- FF.Hemraj Saini, Yerra Shankar Rao, Panda T.C., “Cyber-Crimes and their Impacts: A Review” *International Journal of Engineering Research and Applications*, 2(2) (2012) 202-209.
- GG. Idris Abubakar., “FBI announces arrest of 167 alleged fraudsters in Nigeria in anti-fraud operation,” *Teachable*, 2020
- HH. Jurjen Jansen, Rutger Leukfeldt., “Coping with Cybercrime Victimization: An Exploratory Study into Impact and Change” 6(2) (2018) 1-22
- İİ. Jan Kleijssen, Pierluigi Perri, “Cybercrime, Evidence and Territoriality: Issues and Options” 47(1) (2017) 147-174.
- JJ. Kamini Dashora, “Cyber Crime in the Society: Problems and Preventions” *Journal of Alternative Perspectives in the Social Sciences*, 3(1) (2018) 240-257
- KK. K.N. Igwe, Ibegwam Ahiaoma “Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria” *International Journal of ICT and Management*, 2(2) (2014)1-14
- LL.Koops B.J., “Cybercrime Legislation in the Netherlands”, *country report for the 18th International Congress on Comparative Law*.
- MM. Munanga Albert, “Cybercrime: A New and growing problem of older adults” *Journal of Gerontological Nursing*, 45(2) (2019)3-5
- NN. Olakunle Mercy Risikat, “How Cybercrime in Nigeria” *International Journal Law and Legal Ethics*, 2(1) (2021) 1-9.
- OO. Oni Samuel, Segun Joshua, “E-Government and the Challenge of Cybercrime in Nigeria” (6) (2019)6-8
- PP.“Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?” *American Journal of Criminal Justice*, 44(2019),63–82
- QQ. Omodunbi B.A., Odiase P.O., Olaniyan O.M., Esan A.O., “Cybercrimes in Nigeria: Analysis, Detection and Prevention” *Journal of Engineering and Technology*, 1(1) (2016)2-6

- RR. Olatunji Toyin Emmanuel, Aruwaji Akinola Michael, “Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria” *Journal of Auditing, Financing and Forensic Accounting*, 8(2) (2020) 6-7.
- SS. Paul Bocij, “*Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*” (1st ed, Praeger, 2004). pp. 9–10.
- TT. Phillips Kirsty, Davidson Julia C., Farr Ruby R., Burkhardt Christine, Caneppele Stefano, Aiken Mary P. “Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies” *Forensic science Journal*, 2(2) (2022)5-17
- UU. Pasculli L., “The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory” *Journal of Ethics and Legal Technologies*, 2(1) (2020): 48-74
- VV. Raj Singh Deora, Dhaval Chudasama, “Brief Study of Cybercrime on an Internet” *Journal of Communication Engineering & Systems*, 11(1) (2021) 1-6
- WW. Seemna P.S., Nandhini S., Sowmiya M., “Overview of Cyber Security” *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11) (2018) 2-5
- XX. Sumanjit Das, Tapaswini Nayak, “Impact of Cyber Crime: Issues and Challenges” *International Journal of Engineering Sciences & Emerging Technologies*, 6(2) (2013) 142-153.
- YY. Sari Andika, Setiawan Ananda, “The Development of Internet-based Economic Learning Media using Moodle Approach” *International Journal for active learning*, 3(2) (2018)50-57
- ZZ. Sri Sundari, Muhammad Haikal Kautsar “Cyber Crime Triangle Approach to Encounter Cybercrime” *Budapest International Research and Critics Institute-Journal*, 4(2) (2021)1815-1821
- AAA. Tade Oludayo “COVID - ‘419’: Social Context of Cybercrime in the Age of COVID-19 in Nigeria” 14(4) (2021)460-483.
- BBB. Ulrich Seiber, “Legal aspect of computer related crimes in the information society” (1998)
- CCC. Weber A., “The Council of Europe’s Convention on Cybercrime” *Berkeley Technology Law Journal*, 18(1) (2003) 425-446

- DDD. Wall David, “Cybercrime: The Transformation of Crime in the Information Age” (1st ed, Polity press, 2007).
- EEE. Ye Hong, William Neilson, “Cybercrime and Punishment” *University of Chicago Press*, 49(2) (2020)
- FFF. Ayeni Tofe., “Nigeria: Hushpuppi, ‘419’ and the perceived glorification of fraud” (2021) <<https://www.theafricareport.com/79818/hushpuppi-419-and-the-perceived-glorification-of-fraud-in-nigeria/>> accessed 18th March, 2023
- GGG. Cybercrime, <https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en> Accessed 30 March 2023.
- HHH. Cyber Security law, Cybercrime lawyers, <<https://www.penningtonslaw.com/expertise/data-protection-and-privacy/cyber-security-and-cybercrime>> Accessed 26 March 2023.
- III. “Cyber Terrorism, how real is the threat” <<https://www.usip.org/sites/default/files/sr119.pdf>> Accessed 19 March, 2023.
- JJJ. Éric Freyssinet., “Cyberthreats in the 21st century: From playing on borders to forming cybercriminal autonomous territories” <https://www.anales.org/site/enjeux-numeriques/DG/2020/DG-202009/EnjNum20c_7Freyssinet.pdf> accessed 18th March 2023
- KKK. FBI – Violent Crimes: Uniform Crime Reporting 2018 crime in the United States, <<https://www.fbi.gov/news/stories/2018-preliminary-semiannual-uniform-crime-report-released-022519>> Accessed March 31, 2023.
- LLL.
- MMM. Herhalt, J., ‘Cyber Crime- A Growing Challenge for Governments’ (2018) US Department of Justice <<https://www.ojp.gov/ncjrs/virtual-library/abstracts/issues-monitor-cyber-crime-growing-challenge-governments>> access 5 March 2023.
- NNN. Ibrahim Suleiman., “The view that ‘419’ makes Nigeria a global cybercrime player is misplaced” (2017) <<https://theconversation.com/the-view-that-419-makes-nigeria-a-global-cybercrime-player-is-misplaced-73791>> accessed 21st March, 2023

- OOO. “Identity Theft and the Value of Your Personal Data” <
<https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>> Accessed 18 March 2023
- PPP. Jarret M., Bailie M., “Prosecuting Computer Crimes” (Published by Office of Legal Education Executive Office for United States Attorneys) <
<http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>> Accessed 9th April 2023
- QQQ. Kowalski M., “Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics” *Canadian Centre for Justice Statistics* <
<http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf>> Accessed 6th April 2023.
- RRR. “Krebs on security article on Lizard Squad” <
<https://krebsonsecurity.com/2014/12/lizard-kids-a-long-trail-of-fail/>>
 Accessed 15 March 2023.
- SSS. National Cyber Security Center <
<https://www.ncsc.gov.uk/cyberfirst/overview>> Accessed 6th April 2023.
- TTT. National institute of Justice, <
<https://nij.ojp.gov/topics/crime/property-crimes>> Accessed March 30, 2023.
- UUU. O'Brien Darcy., “Crime is the biggest problem facing our society today” (2002) The Hillside Stranglers <
<https://www.writework.com/essay/hillside-stranglers-darcy-o-brien-crime-biggest-problem-fa>> accessed 21st March, 2023
- VVV. “Obinwanne Okeke: Nigerian email fraudster jailed for 10 years in US” (2021) <
<https://www.bbc.com/news/world-africa-56085217>> accessed 15 march, 2023
- WWW. Organized crime, United Nations, <
<https://www.unodc.org/unodc/en/organized-crime/intro.html>> accessed 30 March 2023.
- XXX. Property Crimes, < <https://www.fbi.gov/news/press-releases/fbi-releases-2017-crime-statistics>> Accessed March 31, 2023.
- YYY. Popova Maria, Cyberspace, <
<https://www.themarginalian.org/2014/08/26/how-william-gibson-coined-cyberspace/>> (2014) Accessed 25 March, 2023.

- ZZZ. Stein Schonberg “The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva” (2008)
<https://www.researchgate.net/profile/Stein-Schjolberg/publication/267946947_The_History_of_Global_Harmonization_on_Cybercrime_Legislation_-_The_Road_to_Geneva/links/556f05b008aefcb861dd4adb/The-History-of-Global-Harmonization-on-Cybercrime-Legislation-The-Road-to-Geneva.pdf>Accessed 8th April 2023.
- AAAA. Sobowole Rasheed., “Exposé: How Nigerian internet scammer pursues his million dollar dream” (2020)
<<https://www.vanguardngr.com/2020/03/expose-how-nigerian-internet-scammer-pursues-his-million-dollar-dream/>> accessed 18th March, 2023
- BBBB. Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho, “The Internet of Things in the Cybercrime Underground”
<<https://media.rbcdn.ru/media/reports/wp-the-internet-of-things-in-the-cybercrime-underground.pdf>> accessed 18th March, 2023.
- CCCC. Samuel Onyekanmi, Nigerian National Bureau of Statistics 2021. Accessed 21st March 2023.
- DDDD. Types of Crime: About the different types of Criminal offences.
<<https://www.lawtonslaw.co.uk/resources/categories-of-offences/>>Accessed 30 March 2023.
- EEEE. “Things to do before the next big thing: How the financial industry reacts to cyber threats,” <https://www.kaspersky.com/blog/how-the-financial-industry-reacts-to-cyberthreats/6610/#mktoForm_10582>Kaspersky, Accessed 23 March, 2023.
- FFFF. United States Attorney, Central District of California; Chair, Attorney General’s Subcommittee on Cyber and Intellectual Property Crimes, 2005-Present.
- GGGG. United States Attorney, Central District of California; Chair, Attorney General’s Subcommittee on Cyber and Intellectual Property Crimes, 2005-Present.
- HHHH. UNODC, Cybercrime topic,
<<https://www.unodc.org/unodc/en/cybercrime/index.html>>Accessed 24 March 2023.

- iii. “Unauthorized Computer access (Hacking)” <<https://www.bayarea-attorney.com/unauthorized-computer-access-otherwise-known-as-hacking>>
Accessed 18 March 2023

A COMPARATIVE APPROACH: LEGAL FRAMEWORK OF CYBERCRIME IN NIGERIA

ORIGINALITY REPORT

17%	16%	8%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.clrwc.com Internet Source	4%
2	hdl.handle.net Internet Source	1%
3	www.coursehero.com Internet Source	1%
4	digitalcommons.law.ggu.edu Internet Source	<1%
5	docs.neu.edu.tr Internet Source	<1%
6	epdf.pub Internet Source	<1%
7	www.researchgate.net Internet Source	<1%
8	ebin.pub Internet Source	<1%
9	professorrajahidsiddique.blogspot.com Internet Source	<1%