CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

In an era defined by the omnipresence of digital technologies, the proliferation of cybercrime poses an ever-growing threat to individuals, businesses, and nations worldwide. From sophisticated hacking operations targeting critical infrastructure to the insidious spread of online fraud and identity theft, the landscape of cyber threats is constantly evolving, challenging traditional notions of security and law enforcement. As the digital realm becomes increasingly intertwined with daily life, the imperative to develop and strengthen a comprehensive legal framework for combating cybercrime has never been more urgent.

The phenomenon of cybercrime is not a recent development but rather a product of the rapid expansion and democratization of information technology over the past several decades. What once may have been considered isolated acts of digital vandalism or theft have evolved into highly organized and sophisticated criminal enterprises, often operating across international borders with impunity. Moreover, the interconnected nature of the internet means that the impact of cybercrime transcends geographical boundaries, posing unique challenges to law enforcement and legal systems around the globe.

Against this backdrop, governments, international organizations, and legal experts have sought to develop a coherent and effective response to the scourge of cybercrime. One of the central pillars of this response is the establishment of a robust legal framework that delineates the rights and responsibilities of individuals, businesses, and governments in the digital domain. Such a framework encompasses a wide range of legal instruments, including international treaties, regional agreements, and domestic laws, aimed at preventing, detecting, and prosecuting cybercriminal activities.

This research endeavor seeks to explore and evaluate the current state of the legal framework for fighting cybercrime, examining both its strengths and shortcomings in addressing the multifaceted challenges posed by digital threats. By delving into the historical evolution of cybercrime legislation, analyzing key international conventions and national laws, and assessing the effectiveness of legal mechanisms for combating cyber threats, this research aims to provide valuable insights into the ongoing struggle to safeguard cyberspace.

Furthermore, this research will explore the emerging trends and future directions in cybercrime law and policy, considering the rapid advancements in technology and the evolving tactics employed by cybercriminals. By identifying areas for improvement and proposing recommendations for enhancing the legal framework for fighting cybercrime, this research seeks to contribute to the ongoing discourse on cybersecurity and law enforcement in the digital age.

In summary, the quest to combat cybercrime requires not only technological innovation and law enforcement prowess but also a robust legal framework that reflects the complex realities of cyberspace. Through comprehensive research and analysis, this endeavor aims to shed light on the critical role of law in addressing the challenges posed by cyber threats and fostering a safer and more secure digital environment for all.

Cybercrime is one of the most dangerous threats faced today by nations involving the application of the internet and computer related devices across the globe. It is an unlawful act wherein the computer is either a tool or target, or both.[1] It involves using computers, the internet, online services and dating sites by individuals or groups to commit a crime.[2] Cybercrime is the unlawful use of cyberspace to commit fraudulent financial or violent crime

[1] K. Dasshora, 'cybercrime in the society: problems and preventions, *Journal of Alternative perspectives in the social science* (2011) 3 (1), 240-259

[2] Z. Komorosky, dating sites are full of scammers, <www.e-businesscardexchange.com.diakes> 1st of March, 2024

through the internet, computer, phones and other smart or android electronic information or telecommunication devices or gadgets and is a global phenomenon threatening the nation's economies.[3]

Nigeria enacted the cybercrime (prohibition, prevention) Act in 2015. This legislation criminalizes various forms of cybercrime, including unauthorized access to computer system, online fraud, cyber-stalking, and identity theft. The Act also provides for the establishment of the National Computer Emergency Response Team (CERT) and the National Cyber Security Fund. Nigeria has also engaged in international co-operation to fight cybercrime. The country is a signatory to the African Union Convention on Cyber Security and personal data protection, demonstrating its commitment to addressing cyber threats at a regional level. Efforts have been made to enhance the capacity of Law enforcement agencies to investigate and prosecute cybercriminals., this includes training programs for law enforcement personnel and within the police force to handle cybercrime cases.[4]

The Nigerian government has recognized the importance of public-private partnerships in combating cyber threats. Collaboration with private sector entities, such as telecommunications companies and financial institutions has been emphasized to strengthen cyber security measures and improve incident response capabilities. Despite these efforts, the effectiveness of the legal framework for fighting cybercrime in Nigeria faces several challenges. These include the need for greater resources and technical expertise within law enforcement agencies, as well as the need for continuous updates to legislate to address emerging cyber threats.[5]

Addressing cybercrime is crucial for Nigeria's economic development, as a secure cyberspace is essential for attracting foreign investment and fostering a thriving digital

[3]A. Ojilere, 'cyberspace, cybercrime and cyber policing in Nigeria central issues and challenges; *University of Port Harcourt Journal of Private Law* (2020) 5 (1) 159-178
[4] A.B.F.D Hassan, 'Lass and Makinde, Cybercrime in Nigeria: Causes, Effects and the way Out, ARPN,' *Journal of Science and Technology* (2012) 2 (7) 626-631.
[5] *ibid*

economy. Also, there is a need to enhance cyber security awareness among the general public, businesses, and government institutions to mitigate the risk of falling victim to cybercrime. The cybercrime Act 2015 provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria, the Act also ensure the protection of critical national information infrastructure and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The rise of technology opens a world of opportunities in the realms of communication, education, and industrial science. However, it simultaneously created a new era of corruption: cybercrimes. From professional hacking and virus writing to identity theft and fraud, cyber criminals are rapidly discovering new ways to threaten the internet - so rapidly that it is hard for law enforcement agencies to keep with them.[6]

Historically, the criminal abuse of information technology and the necessarily legal response have been discussed ever since the technology was introduced.[7] Over the last five decades, various solutions have been implemented at the national and global level. Cybercrimes did not spring up as a problem overnight. In the early days of computing and network, computers were million-dollar huge mainframes with limited number of users.[8] By that time, average criminal possess neither the necessary hardware nor the technical expertise to benefit from such digital opportunity. In the 1950s, students of Massachusetts Institute of Technology (MIT) established the basis for what would emerge as the hackers of culture.[9] In the 1960s, the introduction of transistor-based computer systems which were smaller and less

[6]K.Tatera, 'Using Artificial Intelligence to Take Down Cyber Criminals' (2015) <http://thescienceexplorer.com/technology/usingartificial_intelligence> accessed 1st of March, 2024
[7] K.Mamandi and S. Yari., 'A Global Perspective on Cybercrimes' *Humanities and Social Sciences* (2014) 2 (2) <http://article.sciencepublishinggroup.com/pdf/> accessed 1st of March, 2024
[8] F. Hoscheidt and E.F Eichner 'Legal and Political Measures to Address Cybercrime' (2014) <http://www.ufrgs.br.ufrgsmun/2014/files/ws12.pdf> accessed 1st of March, 2024
[9] *ibid*

expensive than the vacuum-tube based machines led to an increase in the use of computer technology. At this stage, offences focused on physical damage to computer systems and store data.[10] In 1961, the first hackers group came about at the MIT. The members of the group used to program for a sheer joy of it, which the original essence of the term was hacking. Between the 1960s and early 1970s, hacking became associated with radical movement and took on a negative tone.[11]In the 1970s, the use of computer system and computer data increased further. The first affordable personal computer became available, the Altair 88000. From that moment on, it was possible for individual to buy their own computers and learn how to program. Altair gave birth to hacking as it is known today.[12]

In 1988, the wakeup calls for security occurred as Robert Morris J., a doctoral (PhD) candidate at Cornell University, released the first internet worm over the U.S., infecting thousands of computers and shutting down a large portion of the internet.[13] From that moment on, internet users realized that someone in their midst harbored malicious intent. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patent. Viruses started to appear in the 1990s. The 1990s personal computers became popular and the number of potential targets for criminals increased. For the first time, the target included a broad range of critical infrastructure. The interconnection of the computer systems brought about new types of offences. Networks enabled offenders to enter a computer system without been present at the crime scene. In addition, the possibility of distributing software through networks enable offenders to spread malicious software and computer viruses were discovered. Countries started the process to update their legislation so

[10] For example, in Canada, student riot caused a fire that destroyed computer data hosted at the University
[11] *Ibid*
[12] *Ibid*
[13] *Ibid*

as to meet the requirement of the changing criminal environment, International organizations also got involved in the process. Organization for Economic Cooperation and Development (OECD) and the Council of Europe set a study group to analyze the phenomenon and evaluate possibilities for legal responses.[14]

From the foregoing, it is established that Cybercrime is a major concern to the global community and the introduction, growth and utilization of information and Communication technologies (ICTs) have been accompanied by an increase in criminal activities. Cybercrime is increasingly astronomical each day as the internet continues to permeate every nook and cranny of our society and no one can predict the next dimension. The crime usually attracts attention globally because its impacts are ubiquitous just as its negative effect is devastating to the economy and due to several security breach cases on e-money systems, many entrepreneurs have been forced to shut down their online businesses due to fear of being attacked. Conversely, a lot of foreign investors have declined offers to invest in Nigerian firms due to insecurity reasons.[15] Hence, many e-commerce and e-businesses have suffered a drastic breakdown in the last few years.

The proliferation of Information and Communication Technology (ICT) in Nigeria (just as in other countries) has brought tremendous changes in socio-economic growth and development in different facets of Nigerian economy, banking, insurance, stock market, law, production services etc.[16] Paradoxically, ICT has also evolved to become a sophisticated tool in the hand of criminals for perpetuating different forms of Cybercrime. Unintended consequences such as email scam, identity theft, child pornography, organized crime and solicitation for prostitution, fake lotteries and scam text messages (more frequent on social networks like Facebook) as well as cyber piracy are few of the vices that have become

[14] *ibid*
[15]E. Bash, 'Ethical Hacking and Countermeasures: Spamming' *JSTOR* (2015) 1 (3) 5-20
[16] A.O Obuh , 'Cybercrime Regulation: The Nigerian situation' Delta state university (2010)

recurring indices on the internet. This ugly trend acts as a cankerworm against economic development in Nigeria and has compounded the challenges facing Nigeria in the fight against corruption and other vices. [17] It may not be out of place if it is asserted that cybercrimes represent security threat to Nigeria as a country.

1.2 Statement of the Research Problem

The contribution of internet to the development of nation has been marred by the evolution of new waves of crime.[18] The internet has also become an environment where the most lucrative and safest crime thrives.[19] Cybercrime has become a global threat from Europe to America, African to Asia. It impacts negatively to every facet of our nation life; it scares investors and discourages local and foreign investment; it also erodes public confidence in the financial sector and discourages hard work in academic environment.

Despite the lofty provisions and as beneficial as the Cybercrime Act 2015 appears to be, there exist problems therefrom. Take for example kidnapper like Chukwudumeje Onwuamadike aka "Evans" were still able to move huge ransoms, often in hard currencies about. One big challenge is that the Nigerian criminal legal regime is pluralistic in nature. By pluralism, it is meant that a situation in which more than one legal regime operates in the jurisdiction. There are various law used in the prosecution of cybercrime offences in the country. These include: The Nigeria Criminal Code Act 1990; Penal Code Law (Laws of Northern Nigeria 1963); Economic and Financial Crimes Commission Act 2004; Money Laundering (Prohibition) Act 2011; Advance Fee Fraud and Related Offences Act 2006; and the Corrupt Practices and other Related Offences Act 2000. There have continued to be conflicts on which of these statutes should be used in prosecuting cyber related offences, which most often results in different charges being brought against the specified defendants,

[17] *ibid*
[18] D. Yang and B. Hoffstadt , 'Countering the Cyber-Crime Threat' *American Criminal Law Review,* (2006) 43 (2) 34
[19] O. Ehimen and A. Bola., 'Cybercrime in Nigeria' *Business Intelligence Journal* (2010) 3 (1), 93-98

and later struck out on the application of the defendant or Counsel for constituting an abuse of court process. For instance, where an accused person has committed online fraud, there are bound to be confusion on which applicable law to use.

Unfortunately, Nigeria's image has also suffered as a result of the unscrupulous activities of some Nigerians using the internet as a channel for the perpetration of criminal activities.[20] The major implication of the unconscious acceptance of this menace in the Nigerian society in the nearest future has created a high level of disinterest in education and touting among the youths. In recent times, Nigeria has been labeled as a corrupt nation. There is a need for the Nigerian government to do something fast and urgent to curb this menace of cybercrime. [21]

This inadequacy is evidenced by gaps in legislation, limited enforcement capacity, and the inability to keep pace with technological advancements, thereby impeding the country's ability to protect individuals, businesses, and critical infrastructure from cyber threats. This research poses to critically assess the existing legal framework for addressing cybercrime in Nigeria. The analysis intends to focus on identifying specific deficiencies in legislation, law enforcement capabilities, and the overall adaptability of the legal system to effectively fight cyber threats. By addressing these inadequacies, the research raises two fundamental questions:

1. What are the legal framework in tackling cybercrime in Nigeria?
2. How has Cybercrime affected society: positively or negatively?

1.3 Aim and Objectives of the Study

The aim of this research work is to examine the regulatory framework for tackling Cybercrimes in Nigeria and the fundamental objectives of the research work are:

[20] *ibid*
[21] *ibid*

1. To ascertain the efficacy of the present regulatory framework on cybercrime in Nigeria
2. To comparatively analyze the situation in Nigeria with other jurisdictions having developed legal regimes on cybercrime
3. To examine the challenges hindering the combatting of cybercrimes as well as proffer recommendations and solutions to identified problems and loopholes in relation to curbing cybercrime.

1.4 Scope and Limitation of the study

The territorial scope of this research study is Nigeria; while the examination of the regulatory framework for tackling cybercrime in Nigeria will be the crux of examination, especially by reasons of effects of cybercrime and challenges faced in curbing cybercrime, emphasis will also be made from other jurisdictions where and when it is imperative.

In respect of the limitations of the study; the data used for this research study will be retrieved from existing literatures which discuss issues relating to the topic under discourse here. Based on that, the probability exists that the present research study will encounter specific literatures which contain a wholly biased study of the author(s). Where there are such literatures, it implies that this present research study needs to apply credible efforts to decipher the biases, state opinions and verifiable findings which are ethically made without biases. Aside the limitations already stated; other limitations encountered by the research study are majorly financial constraints, epileptic electric power supply and high data consumption. Disappointing to know that there is dearth of comprehensive materials on specific subject matters and concepts covered in the study.

1.5 Significance of Study

The study is significant as its findings:

1. A broad spectrum of stakeholders including researchers, students, lawmakers, stakeholders, government officials, regulatory bodies, and the general public. It serves as a catalyst for necessary reforms in addressing cybercrime.
2. A foundational base for academia, providing a comprehensive guide and reference point for evaluating Nigeria's regulatory framework concerning cybercrime. Additionally, it offers judicial advice for governmental bodies such as the Law Reform Commission, the National Assembly, and relevant agencies, facilitating informed decision-making in legal reforms.
3. Sheds light on the impact of cybercrime on contemporary realities, emphasizing its relevance to global competitiveness and the Nigerian economy.
4. Addresses deficiencies in the legal framework, the study contributes to enhancing Nigeria's competitiveness in the digital age and promoting sustainable development.

1.6 Research Methodology

Research methodology refers to the systematic and structured process of conducting research. It involves the collection of data, analysis, and interpretation of the results, and the development of conclusions and recommendations. Research methodology encompasses the techniques, tools, and strategies used to design, implement, and evaluate research projects.

There are two types of research methodology, and they are the doctrinal and non-doctrinal methods. Doctrinal research methodology refers to the study and analysis of legal principles and concepts as found in statutes, case law, and other legal texts. It involves the interpretation and analysis of legal rules, principles, and concepts to understand the legal system and its application. Doctrinal research methodology is typically used in legal studies, such as in the study of jurisprudence, legal theory, and legal history. Non-doctrinal research methodology, on the other hand, refers to research methods that are not primarily focused on

legal texts or principles, but instead on empirical or theoretical analysis. Non-doctrinal research methods can be used to investigate legal phenomena, such as the social, economic, or political factors that influence legal decision-making or the impact of legal reforms on society. Examples of non-doctrinal research methods include surveys, case studies, empirical analysis, and comparative legal analysis.

The methodology for this research work is doctrinal and analytical and will combine the use of primary and secondary sources of law which includes case laws, statutes, newspaper publications, articles, textbooks, journals, legislations, online law reports and online based sources and materials.

1.7 Chapter Analysis

This research work would be divided into five chapters including the introduction;

Chapter one; contains issue such as the general introduction, the background to the study, aims and objective of the study, research methodology, the scope of the research, significance of study, literature review as well as the research structure of the research.

Chapter Two; will examine conceptual clarification and definitions of key concepts in this research work such as cybercrime, cyber law, cyber terrorism, cyber space etc. It shall also analysis theoretical framework and literature review

Chapter three; will address extensively. Frameworks for combating cybercrimes in Nigeria. The examination here was limited to developments of cybercrimes legislation in Nigeria as well as the *Advance Fee Fraud Act 2006*, *Economic and Financial Crimes Commission Act 2004* and the recently enacted *Cybercrimes Act, 2015.* An examination was also made on the developments of global best practices in some selected municipal jurisdictions because of the progress made by the countries in cybercrimes legislation and

their geographical spread, this chapter will also address the Modern trends in combatting Cybercrime.

Chapter four; will deal on the challenges in combating cybercrimes, by identifying the problems associated with cybercrimes in Nigeria.

Chapter five; contains summary, observation, conclusion and recommendation to the research work.

CHAPTER TWO
CONCEPTUAL, THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Conceptual Clarification

Today's world is often referred to as "the jet age." We are now in a world where information is readily at everyone's disposal and at the fingertip, thanks to the internet. Thus, this section shall deal on clarification of conceptual framework of key terms relevant to this research.

2.1.1 Cybercrime

Cybercrime is a fairly new type of crime that has only become possible with the advent of the internet and advanced digital technologies. Cybercrime is defined as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.[1]

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.[2]

---

[1] N. Jamine, 'International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene, I Xingan Li,(Ed.)' *Webology*, 4(3) (2007): 2-6

[2] Britannica Online (2012), Cybercrime <conspiracy | Britannica> accessed 15 February, 2024.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.[3]

2.1.2 Cyber-Law

Cyberlaw is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).”[4] Law is a term which has no universally acceptable definition. However, law is seen as a system of rules and guidelines which are enforced through social institutions to govern behaviour.[5] Laws can be made by legislatures through legislation, the executive through decrees and regulations, or judges through binding precedents (normally in common law jurisdictions). The formation of laws themselves may be influenced by a constitution (written or unwritten) and the rights encoded therein.[6]

Cyberlaws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.

---

[3] *ibid*
[4] Definition of Cyberlaw<What is Cyberlaw? - Definition from Techopedia> accessed on 24 January 2024
[5] Definition of Cyberlaw<definitions.uslegal.com/c/cyber-law/-Cyber Law & Legal Definition> accessed 24 January 2024
[6] *ibid*

2.1.3 Cyberspace

Cyberspace**,** amorphous, supposedly "virtual" world created by links between computers, Internet -enabled devices, servers, routers, and other components of the Internet's infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state. The term *cyberspace* was first used by the American-Canadian author William Gibson in 1982 in a story published in *Omni* magazine and then in his book Neuromancer. In this science-fiction novel, Gibson described cyberspace as the creation of a computer network in a world filled with artificially intelligent beings.[7] As an internet metaphor, cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network, so that a website, for example, might be metaphorically said to "exist in cyberspace." According to this interpretation, events taking place on the Internet are not happening in the locations where participants or serves are physically located but in the cyberspace.[8]

2.1.4 Cyber Terrorism

Cyberterrorism is any premeditated, politically motivated attack against information systems, programs, and data that threatens violence or results in violence. It might include any cyberattack that intimidates or generates fear in the target population of a country, state, or city, usually by damaging or disrupting critical infrastructure that's vital to social, economic, political, and business operations.[9]

Cyberterrorist acts are carried out using computer servers, other devices and networks visible on the public internet. Secured government networks and other restricted networks are

[7] Definition of Cyberspace<https://www.britannica.com/topic/cyberspace> accessed 26 January 2024
[8] M. Graham, "Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Realities?" *The Geography Journal*, 179 (2) (2014): 177-188.
[9] Definition of Cyberterrorism, Available at <https://www.techtarget.com/searchsecurity/definition/cyberterrorism> accessed 26 January 2024

often targets of such acts. Other targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.[10] Mainstream media coverage often discusses the possibility of a large attack making use of computer networks to critical infrastructures with the aim of putting human lives in a danger or causing disruptions on a national scale either directly or by disruption of the national economy.[11] Assigning a concrete definition to cyber terrorism can be quite complex due to the difficulty of defining the term terrorism itself. Multiple organizations have created their own definitions, most of which are overly broad. There is also controversy concerning overuse of the term in the media and by security vendors trying to sell "solutions."[12]

However, cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of lives or significant bodily harm, in order to achieve political gains through intimidation. It is also sometimes considered as an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.[13] Cyber terrorism is a controversial ter. Some authors opt for a very narrow definition relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption. Other authors prefer a broader definition which includes cybercrime. By some definitions, it might be difficult to distinguish which instances of online acclivities amount to cyber terrorism or not.[14]

---

[10] *Ibid*
[11] *Ibid*
[12]K. Hardy, "What is 'cyber terrorism? Computer and Internet Technology in Legal Definitions of Terrorism." Cyber Terrorism. Springer, New York (2014): 1-23. Available at< https://link.springer.com/> accessed 26 January 2024
[13] *Ibid*
[14] *Ibid*

Again, cyber terrorism can also be defined as the intentional use of computers, networks and public internet to cause destruction and harm for personal objectives. Experienced cyber terrorists who are very skilled in terms of hacking can cause massive damage to government systems, hospital records and national security programs which might leave a country, community or organization in tuN10il and in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror.[15] There have been several major and minor instances of cyber terrorism. Al-Qaeda utilized the internet to communicate with supporters and even to recruit new members. Estonia, a Baltic country which is constantly evolving in terms of technology, became a battleground for cyber terror in April, 2007 after disputes regarding the removal of a Second World War (WWII) soviet statue located in Estonian capital, Tallinn.[16]

Terrorism is a growing menace all over the world today and Nigeria is also by terrorists' activities. [17] For example, it is used to indoctrinate the supporters and would-be supporters alike. Cyber terrorists use information technology to attack civilians and draw attention to their cause. This may mean that they use information technology, such as computer systems or telecommunications, as a tool to orchestrate a traditional attack. More often, cyber terrorism refers to an attack on information technology itself in a way that would radically disrupt network services. For example, cyber terrorists could disable networked emergency systems or hack into networks housing critical financial information.[18] Today it is known that terrorists use ICTs and the Internet for:

2.1.5 Cyber-Warfare

Terms such as "cyber war" and "cyber terrorism" have been extensively used in the media, in the official governmental reports and amongst academics. Even if they have been

[15] *Ibid*
[16] *Ibid*
[17] International Telecommunication Union Cybercrime Legislation (2009) "Understanding Cybercrime, Guide for Developing Countries, 48.
[18] *Ibid*, 51-52.

often hyped, experts agree that it is unlikely that cyber war will occur in the future.[19] Nonetheless. They do acknowledge that cyber threats are real, and that various cyber tools and techniques are becoming increasingly important in international conflict, including those used for sabotage, espionage and subversion. Common element between the two is the lack of an internationally accepted definition.[20] A United States of American government security expert defines "cyber warfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." The Economist describes "cyber warfare" as "the fifth domain of warfare.[21]

Cyber-warfare describes the use of ICT in conducting warfare using the Internet. It shares a number of features in common with cyber terrorism.[22] Discussions originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks. Until now, there have been limited reports on the substitution of armed conflicts by Internet-based attacks. During the last general election in the United States of American it was widely reported how Russia interfered in that electoral exercise. This is seen as cyber war perpetuated by the latter state against the former.[23]

2.1.6 Cyber-Laundering

Cyber laundering is a new phenomenon in Nigeria.[24] The Internet is transforming money laundering in Nigeria. With larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services provided by banks in Nigeria offer the option of enhancing multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on

[19] T. Rid and B. Scheneier; on the contrary, J. Carr, available at <https://www.goo.gl/images/VAsWg4> accessed 26 January, 2024.
[20] *Ibid*.
[21] R.A Clarke, in his book cyber war, available at <https://www.goo.gl/images/VAsWg4> accessed 26 January 2024
[22] *Ibid*
[23] *Ibid*
[24]E. Jonah 'analysis of Cybercrime' Available at <http:/ www.ireporterstv.co/president-goodluck-jonathan-awards-40-million-contract-t0-israeh-company-for-intemet-communication-monitoring -in-nigeria/> accessed on 28 January, 2024.

physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.[25]

2.2 Theoretical and Historical framework

It is fundamental in criminology to examine social or other factors that derive people into committing a crime.[26] Some of the crime theories relevant to cybercrimes inform us of the shift from conventional crimes to cybercrimes challenge or compete with law enforcement by taking advantage of information and telecommunication technology innovations in committing crimes. The theories are: Rational Choice Theory, also known as choice theory or rational action theory, is a model for understanding social and economic decisions and individual behaviour.[27] It was founded by Adam Smith, an economist who proposed an "invisible hand" moving free-market economies in the Mid-1770s.[28] He opined that is the rationality, free will and choice of a person to indulge in cybercrime after considering the benefits against the cost of the crime.[29]

The theory is rooted in the Utilitarian theory of law by Jeremy Bentham 1748-1832, an English Philosopher who propounded that, life is full of pain and pleasure and the law should be used as a tool of social engineering or means to increase human happiness to minimize pain. The law should be enacted to secure or ensure the happiness of the greatest possible number of people. The law should maximize human happiness by securing the

[25] Section 2 Of the Anti-Money laundering Act, 2011, Banks in Nigeria are required to report suspicious financial transactions to the EFCC Cyber-laundering makes this law difficult to enforce.
[26] M.I Ogu, 'Rational Choice Theory: Assumptions, Strengths, and Greatest Weaknesses in Application Outside the Western Milieu Context' *Arabian Journal of Business and Management Review* (2013), 1(3),90-99.
[27] G. Becker, *The Economic Approach to Human Behavior*, (Chicago and London, the University of Chicago Press, 1976), 3-14.
[28]A. Ganti, Rational Choice Theory, (2021), <available at https://www.investopedia.com/terms/r/rational-choice theory.asp> accessed 02nd March, 2024
[29] B. Steve, *Important Theories in Criminology, In Criminology for Dummies*, (First Edition, United Kingdom, John Wiley and Sons Ltd, 2009), 177.

greatest happiness of the greatest number of people. He opined that every person should be allowed to pursue happiness, the advantage to actualizing one's aspiration without interference by the state to support a free market economy.[30] The theory avers that whether any law was good or bad should be decided by assessing or evaluating its utility to the individual and society. The utilities every society should seek to promote are security, equality, liberty and abundance, and the National Assembly should weigh the interests of the individual against that of the state to promote the interest of the state or interest of the majority against that of an individual.[31]

The critics argue that when a person or a government must choose between two causes of action, they should choose the one that will lead to the greatest happiness for the greatest number of people by reforming the law. One is expected to choose the one with lesser painful consequences as man is moved by pain and pleasure. Critics further aver that many things a person can pursue in life cannot be called pleasure as all pursuits cannot be classified as pain and pleasures. The utilitarian argues that ran the wrong action to a good result done that the right or wrong of anything is not dependent on its nature but the circumstances under consideration. However, critics deviated and held that it is right and wrong and what is right is right and worth doing while what is wrong is wrong and is not worth doing except it is excused or allowed by law.[32]

The utilitarian school posited that law should increase the population's happiness, but critics argued that the theory failed to state how this can be effectively attained.[33]The flaws in utilitarian theory prompted the current author to utilise another theory called the social theory of law. Social Control Theory, by Travis Hirschi in 1969, without the influence of positive,

[30]E. Malemi, *The Nigerian Legal Method* (Princeton Publishing Co., Ikeja, Lagos,2016), 52.
[31] *ibid*
[32] *ibid*
[33]O.J Olujobi, and T.O Jolaosho, 'Strategies for Combating the Crimes of Money Laundering and Terrorism Financing in Nigeria: The Need for A Paradigm Shift' *University of Ibadan Journal of Private and Business law* (2019) 10, 27-64.

social control institutions such as mosques, churches, schools, family and workplaces, many people would ordinarily want to commit cybercrimes.[34] Tania posited that children and youths should be given a substitution to a life of crime which is important to social control theory.[35]

The Federal Government, the National Assembly and other policymakers should promote political, social and economic stability so that the people would not be pressurised into cybercrime in Nigeria due to unemployment, poverty, weak institutions, and negative peer influence are among which are the causes of cybercrime in Nigeria.[36] Desperate and vulnerable individuals are victims of cybercriminals antics.[37] The flaws in social control theory prompted the current author to utilise another theory called deterrence theory of law. The theorists challenged Nigerian government on the need for stringent cybercrimes legal regime and policing to deter and punish cybercriminals for stopping new advances.

Deterrence Theory by Cesare Beccaria and Jeremy Bentham in the 18th century opined that crime could be effectively combated via deterrence mechanisms or policy by inflicting stringent sanctions for non-compliance with accelerated fair hearing and certainty. It is emphasized that a severe legal regime, effective cyber policing with expertise in cybercrime detection, investigation, monitoring, prompt prosecution, and efficient judicial system will reduce if not combat cybercrime in Nigeria. Marxian Theory by Karl Marx, a German philosopher and economist in 1818-1883. He opined that crimes emanate from the capitalist system because it promotes individuals acquisition and ownership of property without considering the poor or others who are economically disadvantaged or vulnerable. This occasioned competition and inequitable society where corruption31 Exploitations,

---

[34] *ibid*
[35] U. Tania, Criminology Theories: The Varied Reasons Why People Commit Crime, <available online at www blog. udemy.com> March 2nd, 2024
[36] J.O. Aransiola, and S.O Asindemade, 'Understanding Cybercrime Perpetrators and the Strategic they Employed in Nigeria, , Cyberpsychology, Behaviour and Social Networking' *JSTOR* (2008) 14(12)759-763.
[37] *ibid*

greed, high rates of crimes thrive.[38] The theory postulates that socio-economic deprivation, political inequality, and endemic corruption occasioned some poor and unemployed youths to indulge in crimes.[39]

2.2.1 The Notion of Cybercrime

Technical experts, police, lawyers, criminologists, and national security experts understand the concept of "cybercrime" differently, in order to understand the Cybercrime at conceptual level, it is essential to scrutinize the definitional aspects of the word "Cybercrime". Cybercrime could be said to be a terminology that crept into the lexicon of our criminal jurisprudence at the advent of the internet.[40] However, cybercrimes could mean the terms "Computer Crimes" and "Cybercrime".[41] Computer crime or cybercrime is any crime that involves a computer and a computer network. The computer may have been used in the commission of a crime, or the computer itself could be the victim of criminal exploitation of the internet, which is also a cybercrime. Computer attacks can be generated by the criminals from anywhere in the world, and executed in other areas, irrespective of geopolitical location. Often, these criminal activities can be faster, easier and more damaging with the use of internet.[42]

The 10th United Nation Conference on the prevention of crimes and the treatment of offenders, cybercrime was classified into two categories and thus defined as;

1. Any illegal behavior directed by means of electronic operations that target the security of computer system and data processing by them and

[38]J.R Blau,and P.M Blau, The Cost of Inequality: Metropolitan Structured and Violent Crime, *American Sociological Review,* (1982) 47(1),114-129
[39] O.J Olujobi, Nigeria's Upstream Petroleum Industry Anti-Corruption Legal Framework: The Necessity for Overhauling and Enrichment, *Journal of Money Laundering and Control*, <https://www.emerald.com/insight/1368-5201.htm> accessed 2nd March, 2024
[40] M Wasik, *Crime and the Computer,* (Oxford University Press, 1991) 30.
[41] *Ibid.*
[42] *ibid*

2. Any illegal behavior committed by means of or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of a computer system or networks.[43]

Cybercrime, is a broad notion, in literature all kind of definition can be found of computer crime, computer-related crime, internet, amongst others. including discussions about which specific crimes should be considered as such, modern definitions of cybercrime describe cybercrime as concerning any crime for the commission of which the use of the internet was essential. This implies that even offences that do not include an explicit reference to information communications technology (ICT) or to the electronic environment, can nevertheless be considered as such if the criminal conduct was directed against other computers or where the facilities of the internet were used to disseminate or retrieved information "essential" means that ICT or the electronic environment is an essential element of the criminal conduct A murder in the computer room would not qualify as such.[44]

Under the notion of cybercrime, all kind of subcategories can be distinguished, including their refinement and details. The Council of Europe's Convention on Cybercrime (2001), that adopted the notion of cybercrime, does not provide a definition but distinguished in its substantive law part four categories of the cybercrime:[45]

1) CIA offences: dealing with conduct that is directed against computer systems (and networks) and the data processed, stored or transferred by it;
2) Computer-related offences, property crime committed by means of computer system.

[43] Crimes related to computer networks, background paper for the workshop on crimes related to computer networks, *10th UN Conference on the prevention of crimes and the treatment of offenders,* 2000, A/CONF/87/10, <www.uncjin.org/documents/confr10/10e.pdf> accessed 6th February, 2024

[44] Kaspersen Henrik., 'Cybercrime and internet jurisdiction Vrrje Universiteit Amsterdam*'* Economic crime Division, Directorate General of Human Rights and Legal Affairs (2009) 32 <www.coe.int/cybercrime> accessed 6th February, 2024

[45] *ibid*

3) Content-related offences, concerning the disclosure or making available by means of a computer system of illegal content; and as a separate category.

4) Offences related to intellectual property.[46]

According to *Osborne*, cybercrime are crimes committed on the internet using computer as either a tool or a targeted victim,[47] cybercrimes involve both the computer and the person behind it as victim, depending on which of the two is the target. Hence, the computer could be looked at as either a target or a tool.[48] Folashade, defined cybercrime as follows; "cybercrime is derived from two words "Cyber" and "Crime" cyber refer to any activities either sales or transaction of services in the cyber space while crime are unacceptable activities, when join together, it means all fraudulent, illicit and unacceptable activities related to cyber.[49]

Given the present state of technology advancement, there is hardly any electronic or digital device that is not now connected to the internet, whether remotely or directly. The duration of the connection, or whether the internet connectivity function of the device was enabled at the time the crime was committed, is a question of fact. For the present purposes, it is pertinent to adopt a working definition of cybercrime. Hence, cybercrime is defined as a financial crime involving the use of internet-enabled electronic or other devices and platforms. Therefore, for the present purposes, the scope of cybercrime is narrowed down to a subset of financial crime. The cybercrime could also refer to all type of crimes that exploit telecommunications network in computers or computer network are used for criminal

[46] *ibid.*
[47] *ibid*
[48] H.Q. Osborn, 'Fighting Cybercrime in Africa' *Computer science and Engineering Journal* (2012) (2) (5) <http://Journalsapub.org/computer.scientific&Academic> accessed 6th February, 2024
[49] *ibid*

activities. For example, designing a fake receipt on a computer system to extort funds from the government desk.[50]

From this exposition, the working definition of cybercrime can further be expounded as financial crime where internet-based computer or other devices and platforms serve as objects, subjects, tools and/or symbols. The peculiar challenge posed by cybercrime must form the backdrop of any analysis of this scourge. While the advancement in technology has aided legitimate activities and transactions, criminals have also taken it as a free ride to carry out criminal activities ubiquitously and anonymously.[51] The attempt to define cybercrime here is merely notional. For the sake of emphasis, it is reiterated that crime is what the law says it is. Thus, cybercrimes that are expressly established by statute will be considered subsequently.[52]

2.2.2 The Emergence of Trends of Cybercrimes

According to Luppicim[53] cybercrime is a relatively new area of research. The internet is, in most ways, a great development for our society. Unfortunately, it has other purposes and other uses, and young people are extremely vulnerable to things like cyber bullying, that, Luppicini calls cyber intimidation, cyber assault and to some terrible crimes, and most shockingly of all often crimes are committed in virtually complete anonymity. The learned author makes the case that governments have consistently made cracking down on crime a major priority, but that governments will be doing more to ensure that children are safe from online predators and from online exploitation. The scholar again states that governments need expediting a review of the extant legal regime on these very matters to identify potential gaps

[50] *ibid.*
[51] *ibid.*
[52] Mara, Marie Helen, *Cybercriminology* (Oxford University Press, 2016) 23.
[53]R. Luppicini, 'Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research,' *Global Media Journal*, (7)1 (2004):35-49.

with regard to cyber bullying, cyber intimidation and cyber assault, as well as the non consensual distribution of images.[54]

One of the main challenges within the contemporary field of criminology is concerned with the increasing role of technology in crime and how to conceptualize areas of criminal activity where the nature of human-technical relationships are deeply intertwined.[55] Part of the challenge lies in the paucity of theories of the techno-social to provide an adequate theoretical framework for the analysis of crime within criminal contexts where technology plays a strong role. Brown notes, "nowhere is captured the vision of the crucial nature of the world as a human/technical hybrid."[56] How can criminology deal with this new wave of crimes, like computer hacking, where many of the activities are carried out by non-human agents? Is cybercrime a new type of crime that requires a new approach? Brown[57] looks to Latour's Actor-Network Theory (ANT) as a means of removing false dichotomies that separate crime from cybercrime and viewing technological crimes as network activities defined by humans and non-human agency. This raises the question as to what does ANT contribute to current scholarship on cybercrime?

What is an actor-network and how do humans and non-humans come together and demonstrate agency? Latour's ANT provides an alternative theoretical lens for conceptualizing and analyzing the human-technical relationship.[58] This is becoming entrenched within the field of criminology.[59] Bruno Latour, Michel Callon, and John Law pioneered ANT during the mid-19-80s as an alternative conceptual framework for exploring

---

[54] *Ibid*
[55]S. Brown, Virtual criminology, in E. McLaughlin and J. Muncie (Eds.), The sage of Criminologv. Sage (2006): 224-258.
[56] *Ibid*, 224.
[57] *Ibid*
[58] J. Law *Complexity, Naming and Topology*, in J. Law and J. Hassard (Eds.), Actor- Network Theory and After,(Blackwell Publishers, 1999): 1-14.
[59] *Ibid*, (n.55)

collective socio-technical processes.[60]Actor-Network Theory helps to explain how socio-technical "human machine" networks (comprised of humans and technologies as actors) intersect through translation and create agency.[61] It is a sophisticated theoretical framework for exploring how ideas, values, and intentions of social actors become inscribed in technology.[62]

In terms of defining features, Actor-Network Theory is intended to allow researchers to trace the complex interplay of humans and digital technologies because it provides a focus on the relationships between non-humans and humans that captures the mediated nature of contemporary life within an evolving technological society.[63] One particularly interesting area where ANT is being applied revolves around the misuse of technology and growing proliferation of cybercrime around the world.[64]

2.3 Literature Review

This section reviews the related literature. It presents opinions of various scholars, writers, jurists and authors on their ample understanding of cybercrime. The intrinsic nature of this review is also to examine the concept of cybercrime. This research attempted a review of some of the earlier works on the subject of the study with the view to identifying their relevance and possible gaps.

Olayemi,[65] an erudite scholar who opines that the global information infrastructure creates unlimited opportunities for commercial, social and other human activities which are however increasingly under attack by cyber criminals with increasing number of cost and

[60] M. Callon, The Sociology ofan Actor-Network: The Case of The Electric Vehicle, in M Callon, J. Law and Arie Rip (Eds.), Mapping the Dynamics of Science und Technology, Macmillan press (1986): 19-34)
[61] *Ibid*, Law and Hassard
[62]M. Akrich and B. Latour, A Summary of a Convenient Vocabulary for the Semiotics of Human and Non-Human Assemblies, in W. E. Bijker and J. Law (Eds.), Shaping Technology Building Society: Studies in Socio-technical Change, MIT Press (1992): 259-264.
[63] Supra, Luppicini
[64] Supra, Jaishankar and McQuade.
[65]O.J Olayemi., 'A Socio-Technological Analysis of Cybercrime and Cybersecurity in Nigeria' *International Journal of Sociology and Anthropology* (2014) (6) (3) 116-125

sophistication at an alarming rate. Olayemi examined the sociological and technological factors that impact cybercrime and cyber security thereby articulating the relevant circumstances and threat of cybercrimes in Nigeria. He approached the issues of enforcement through agencies and governmental institutions and concluded that at the point of writing, that Nigeria has no existing regulatory framework that directly addresses cybercrimes. This study negates completely the view stated by Olayemi because there are regulatory frameworks in Nigeria that addresses cybercrime directly.

Babaji,[66] while examining the development of cybercrimes under Nigerian law noted that cybercrimes are new in Nigeria as well as in many parts of the world, for a number of reasons such as the absence of specific legislation or statute proscribing and punishing cybercrimes. That, by its nature, cybercrimes involves the use of cyberspace, internet, computer and other related information technology devices which are not known or understood by many Nigerians. He observed that the existing penal statutes do not have direct and adequate provisions on cybercrimes, though; they may not be totally ignorant of the concept and ideas of cybercrimes. The work, though recent, did not take into account nor referred to decided cases by Nigerian courts.[67] This study however, attempts to fill the gaps in Babaji's work by making reference to judicial authorities in Nigeria and other parts of the world. The work of Babaji is nonetheless very relevant and useful in the preparation of this research as it touches on some basic points this researcher would dwell on.

Hassan et al,[68] identified causes of cybercrimes in Nigeria to include urbanisation, unemployment, quest for wealth, negative role models, weak implementation of cybercrimes

[66] B.O Babaji, *The Law of Crimes in Nigeria* (A.B.U., Press Ltd., Zaria, 2010) 517 - 523
[67] The EFCC through its Head of Advance Fee Fraud Unit, Mr. Olaolu Adegbite boasted of securing 220 convictions out of the 460 cases of cyber and computer related crimes in Lagos alone
[68] Hassan et al. 'Cybercrime in Nigeria: Causes, Effect and the Way Out' *ARPN Journal of Science and Technology* (2012) (2) (7), 26

law and inadequate equipped law enforcement agencies.[69] He noted the effect of cybercrimes to include reducing the competitive edge of organisations, time wastage and slow financial growth, deformation of image, slow production time and add to overhead cost. This study accedes completely to the positions taken by Hassan *et al* above.

Bali,[70] *Ladan*,[71] *Ashaolu* and *Oduwale*[72] wrote on cybercrimes and cyber jurisdiction including the taxonomies of cybercrimes. Ashaolu and Oduwale took further steps by briefly discussing specific offences and challenges to prosecuting cybercrimes in Nigeria. Ladan posited that Nigeria is fast becoming a heavy user of the internet for commerce, information and communication, and is spending on the internet. He argued that with the expansion of internet Nigeria begins to experience rising tide of cybercrimes and the global news broadcast terrifying figures and instances of e-mail scams done by Nigerians. This study draws from their work to elucidate further the subject matter of the research.

Ladan[73] examined the effectiveness of legal and enforcement framework in fighting advance fee fraud and money laundering activities. He observed that the various forms of corporate fraud especially computer fraud or electronic fraud have assumed an alarming dimension in the world of financial crime. That advances in computer technology have made it possible for criminals to direct funds electronically away from their rightful owners. Besides, electronic fraud perpetrators came from every educational, geographical, racial, religious, gender and socio-economic backgrounds and they are often trained professionals who are good at stealing money and assets from people. Ladan concluded that advance fee

---

[69] *Ibid*

[70] O. Bali., *Information Technology and the Law: The Nigerian Perspective* (Legal Digest Publishing, Lagos, 2010) 8 – 10.

[71] M.T Ladan, *Introduction to Jurisprudence: Classical and Islami* (Faith Printers International, Zaria, 2013) 5 – 16.

[72] D.D Ashaolu. and O.A Oduwale *Policing Cyberspace in Nigeria: A Publication in Honour of Col. Sani Bello (Rtd)*. (Life Gate Publishing Co. Ltd., Ibadan, 2009) 17-18

[73] M.T. Ladan, 'The Effectiveness of Legal and Enforcement Framework in Fighting Advance Fee Fraud and Money Laundering Activities' (2014) A paper presented at the 3rd National Seminar on Economic Crimes <www.dawodu.com/Ladan2.htm> accessed 05 February, 2024.

fraud and related crimes cannot be fought by legislation alone. The moral tone of the society must also be raised by all and sundry. That effort should be made to remove the socioeconomic injustice and inequities in the society, provision of job opportunities and creation of right atmosphere for genuine business and investment to thrive. Ladan's work emphasised on advance fee fraud and money laundering offences only. However, this research work will discuss other types of cybercrimes such as cyber stalking, cyber terrorism, hacking, malicious codes, and child pornography among other offences. Nonetheless, the writer's work is relevant and shall be relied on in the course of writing.

Tokura,[74] discussed issues of definitional problems of computer crime, world situational and vulnerability of countries, jurisdictional issues, and computer related crimes and challenges of enforcement of law. The emphasis in Tokura's work is on commercial law aspects of cybercrimes instead of public law which is the domain of criminal law. That perhaps explained why he did not discuss specific cybercrime offences but focused on providing proposed lists of computer crimes by Organization for Economic Co-operation and Development (OECD) and Council of Europe (COE) in chapter two of his work. At no point in the entire work did the writer made reference to the *Advance Fee Fraud Act* which is an important legislation in cyber related crime in Nigeria. At the same time, the writer did not cite a single decision on cybercrimes by Nigerian courts. This study will address the problems identified in Tokura's work above.

Brill, *Baldwin* and *Munro*,[75] in three volume books made a collection of essays and articles on Computer crimes and Encryption Technology, Infrastructure Protection and Management Solutions, Cybercrimes and Security in the United States, Transnational Responses, U.S. Federal and State Legislation, U.S. Federal and State Judicial Decisions and

[74] S.S Tokura, *The Legal Regime of Cyber Security and Crime: Challenges of Enforcement in Nigeria*. (LL.M Thesis, Faculty of Law, A.B.U., Zaria, 2015) 56
[75]E.A Brill and F.N Baldwin , *Cybercrimes and Security* (Oceana Publications Inc., U.S.A., 2010) 12

Cybercrimes and Security in Europe amongst others. Although the works do not include cybercrimes experience in Nigeria, they are nonetheless relevant and shall be relied on in the writing of this study.

Ladan,[76] reviewed the Cyberlaw and Policy on Information and Communications Technology (ICT) in Nigeria and ECOWAS. In four chapters, he discussed the concept of cyberlaw, cybercrime, cyber security, information and communications technology and cyber jurisdiction. He further examined the legal and policy responses to ICT, cybercrime in Nigeria and ECOWAS and international and regional initiatives on cybercrimes, cyber security and ICT and by way of conclusion noted the need to develop safeguard mechanisms to counter cybercrime trends as cybercrime goes mobile, social networks and the need to cope with investigation and prosecution challenge in terms of cooperation with service providers or private sector in area of investigation and liability issues.[77] Ladan's work is relevant and pertinent to this study as it touches on cybercrimes, which is the basic theme of this study. However, the book is wider in terms of scope as it discussed both the civil and criminal aspect of cyber law and extends to ECOWAS jurisdiction. This study on the other hand is limited to cybercrimes experience in Nigeria.

Osinbajo,[78] and *Babaji*[79] examined the problems of proof of computer and other electronically generated evidence in local and international financial transactions, the legal basis for the admissibility of electronic evidence under Nigerian law and computer and electronically generated evidence respectively. Although, the works of the authors were in

[76]M.T Ladan, '*Cyber Law and Policy on Information and Communications Technology in Nigeria and ECOWAS.*' (A.B.U. Press Ltd., Zaria, 2015) 22
[77] *Ibid*.
[78] Y. Osinbajo., *Cases and Materials on Nigerian Law of Evidence* (Macmillan Publishers, Lagos 2010), 270-296.
[79]B. Babaji, *Admissibility of Documentary and Electronic Evidence under Nigerian Law. Ph.D Dissertation* (unpublished, Faculty of Law, A.B.U., Zaria,2013) 387-476.

respect of electronically generated evidence in both civil and criminal proceedings, the emphasis in this study shall be with respect to cyber and computer related crimes.

Longe et al,[80] and *Hassan et al*,[81] examined the concepts of internet crimes, cybercrime and criminality in Nigeria, nature of cybercrimes in Nigeria, types of cybercrimes, causes of cybercrimes in Nigeria, effects of computer crime and combating cybercrimes in Nigeria. The authors noted that Nigeria's image has suffered as a result of the nefarious activities some Nigerians who have turned the internet into cheap channel for perpetration of criminal activities, ranging from phishing, online trickery and advance fee fraud popularly known as "419 spam", That despite the laudable contributions of Internet Service Providers (ISPs) as facilitators of internet usage in Nigeria, the ISPs seemingly remain oblivious of the damaging implications resulting from the use of their infrastructures for online criminal activities. The level of security provided against the crime by ISPs is relatively low resulting in a positive relationship between the level of internet crime and the attitude of ISPs to protecting their networks. Hassan *et al* on their part identified some of the causes of cybercrimes to include urbanization, unemployment and weak implementation of cybercrime laws. The effect of which include reducing the competitive edge of organizations, waste of production time and damage to the image of the country. Thus, with Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized by taking reasonable steps to protect information technology infrastructures like networks and computer systems.

---

[80] Longe et al 'Internet Service Providers and Cybercrime in Nigeria -Balancing Services and ICT Development' *Journal of Information, Law and Technology* (2010) (7) (3) <www.jiti.net>accessed) 6th February, 2024

[81] A.N Hassan 'Cybercrime in Nigeria: Causes, Effects and the Way Out' *ARPN Journal of Science and Technology* (2012) (12) (7) < www.ejournalofscience.org> accessed 6th February, 2024

.

Reyes et al.,[82] study is a foundational text for the cybercrime community and discusses the hard questions cybercrime investigators often ask: What is Cyber Crime? This question the authors answered by examining the complex relationship between the public and private sector with regards to cybercrime. Against this background, they expounded issues relating to cybercrime definitions, the electronic crime scene, computer forensics, and preparing and hearing a cybercrime in court. According to Sackson,[83] cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the internet.

Ani[84] argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. This author[85] did a comparative analysis and critical review of Jurisdictions such as the USA, UK, India and Nigeria and states that lack of cybercrime specific laws and inadequate equipment of law enforcement agencies militate against the fight against cybercrime. Ani also seeks to lay a roadmap for Nigeria's accession to the Budapest Convention. In considering relevant laws in fighting cybercrime in Nigeria, the author does consider the relevant provisions of the Anti Terrorism Act 2013 (as amended), the Advance Fee Fraud Act, 2006, Money Laundering Act, the National Identity Management Commission (NIMC) Act, 2007 and the cyber crime Act, 2015 which is Nigeria's effort to key into the international fight against cybercrime.

Stefan,[86] in his report titled "UK Cybercrime Report," a report from criminologists from specialist consultancy firm 1871 Ltd. Focuses on an estimated quantification of cybercrime in the United Kingdom. It discusses the cost and effect of cybercrime on the

[82] Reyes et. al 'Cybercrime investigations: bridging the gaps between security professionals, law enforcement, and prosecutors' (Rockland, MA,, USA: Syngress Publishing, 2007) 45
[83] M. Sackson, "Computer Ethics: Are Students Concerned," First Annual Ethics Conference, available online at http://www.maths.luc.edu/ethics96/paper/sackson.doc. accessed on 15 February, 2024
[84] L. Ani, Law and Security in Nigeria, E Azinge, et al (eds.) Nigerian Institute of Advanced Legal Studies Press, Lagos, 2011: 197-234.
[85] *Ibid*
[86] Available at http://www.garlik.com/file/cybercrime_report accessed on 15 February, 2024

Citizens of the United Kingdom. It also discusses relevant laws in the United Kingdom for combating cybercrime. Again it is observed that this report however, does not consider the possibility of cybercrimes like cyber terrorism or cyber warfare in spite of increase in use of the internet by terrorists to facilitate terrorism.[87]

Okonigene, et al.,[88] discuss cybercrime vis-à-vis the Economic and Financial Commission Act, 2004 and the Criminal code as laws available to combat cybercrime in Nigeria. The authors[89] state that the internet as an instrument to aid crime ranging from business espionage, to banking fraud, obtaining un-authorized and sabotaging data in computer networks of some key organizations. From this research, it is observed that even though these authors claim to have the inadequacies of the existing laws in combating cybercrime in Nigeria and proffer solutions, they only consider two laws of Nigeria,[90] i.e. the EFCC Act and the Criminal Code in considering the relevant laws to fight cybercrime in Nigeria and their research is limited to Nigeria. This work will take a step beyond this and examine other relevant aspects of cybercrimes in Nigeria. Price Waterhouse Coopers[91] study on the impact of cybercrime on organizations, their awareness of the crime and what they are doing to combat the risks. It also studies fraud, the fraudsters and the defrauded the types od economic crimes committed, how they are detected, who is committing them and what the repercussions are. This work reveals that though this article gives a great insight into the effect of cybercrime on businesses its scope is limited to the United Kingdom Nigeria

[87] *Ibid*
[88] In Their article title Cybercrime in Nigeria Available at http://www.saycoc orporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7 accessed on 15 February, 2024
[89] *Ibid*
[90] *Ibid*
[91] In the article titled "Cybercrime: Protecting against the Growing Threat; Global Economic Crime Survey United Kingdom," November, 2011 http://www.pwc.com/crimesurvey accessed on 16 February, 2024

Brenner[92] argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offenses for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation. Because cybercrime is often transnational in character, offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system takes measure to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. This research work reveals that the focus of this author[93] is only on law enforcement agents and how they can be trained to fight cybercrime.

International cooperation in fighting cybercrime like nations assisting each other in the fight against cybercrime is not discussed. Data Protection and Cybercrime Division of the Council of Europe in a document[94] gives an insight into the efforts of the council of Europe in 2012 and how far the Budapest Convention on Cybercrime has assisted in the global fight against cybercrime. This study again reveals that though this document is pivotal in showing the relevance of the Budapest convention in the fight against cybercrime, it does not show how the council of Europe intends to ensure that other nations of the world become party to the only treaty on cybercrime.

Mare and *Brenner*[95] analyze the challenges of archaic procedural and substantive law in fighting cybercrime. These issues are the focus of this article; it examines how they are being addressed at the national and international levels and assesses the measures that are being taken in an effort to resolve them.

---

[92] In her book titled Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law, University of Dayton Law School, Dayton http://www.unpan1.un.org/..//unpaan003073 accessed on 16 February 2024.

[93] *Ibid*

[94] Global Project on Cybercrime: Cooperation against Cybercrime in 2012, Activities on 17 January 2024

[95] In their book titled The Emerging Consensus on Criminal Conduct in Cyberspace. Available at http://www.coe.int/cybercrime.Strasbourg accessed on 18 January, 2024

Alexander in his article[96] gives guidelines for harmonized international legislation on cybercrime, framework for international cooperation and vector for capacity building.

Gbenga, et al.,[97] discuss the effect of cybercrime on the Nigerian economy, efforts of the Nigerian National Assembly to provide laws to fight cybercrime and the need to fight cybercrime to encourage e-trade and salvage the nation's battered image. Though the writer discusses the cost of cybercrime to Nigerian consumers, he does not postulate how to nip it in the bud as proposed in this work.

Adejoke in his work[98] examines the impacts and challenges of information and communication technology in diverse aspects of commerce, banking and business activities in Nigeria. The paper concludes that while ongoing legislative interventions are desirable, the highly fragmented nature of emerging ICT laws and multi-layer regulatory institutions will unnecessarily complicate the legal and institutional landscape, and defeat the purpose of certainty and simplicity.

Jonathan in his book[99] gives a deeper understanding of the legal principles which are applied to "cybercrimes," whether they are academics, legal practitioners, law enforcement officers or students. The unique feature of this book is that the various offences are analyzed across four major common law jurisdictions: Australia, Canada, the United Kingdom and the United States. This study reveals that aside form jurisdictional issues, the author does not address the law of criminal investigation, procedure or evidence and it is restricted to issues of cybercrime in Canada, United States and the United Kingdom.

---

[96] Budapest Convention on Cybercrime Available at <http://www.cto.int//Alexande.Sager> accessed on 18 January, 2024

[97] In the article title "Economic Cost of Cybercrime," available at <http://www.unodc.org> accessed on 18 January, 2024

[98] "The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions," British <http://www.bjournal.co.uk/BJASS.aspx> accessed 18 January 2024

[99] Principle of Cybercrime, available at <http://www.cambridge.org/./principles> accessed on 18 January, 2024

The word cyber-crime is a hybrid word. It is made of "cyber" and "crime" According to Sackson,[100] cyber-crime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet.

The first step in answering these questions is parsing out what "cybercrime" is and what it is not. When we do this, we see that the definition quoted above needs to be modified for two reasons.[101] One is that this definition assumes that every "cybercrime" constitutes nothing more that the commission of a traditional "crime," albeit by different means (by using a computer network).[102] The point being made here is that while most of the cybercrime we have seen to date is simply the commission of traditional crimes by new means, this is not true of all cybercrime.

In February of 2000, someone launched DDoS attacks that effectively shut down Amazon.com and eBay, among other sites.[103] DDoS attacks are increasingly used for extortion; someone launches an attack on a website, then stops the attack and explains to the owner of the website that attacks will continue unless and until the owner pays a sum for "protection" against such attacks. This simply represents the commission of an old crime (extortion) by new means. It is a tactic the Mafia was using over half a century ago, though they relied on arson instead of DDoS attacks.[104] But a "pure" DDoS attack such as the 2000 attacks on Amazon.com and eBay is not a traditional crime. It is not theft, fraud, extortion, vandalism burglary or any crime that was within a pre-twentieth century prosecutor's repertoire. Brenner, in "Is There Such a Thing as Virtual Crime?" states that it is an example of a new type of crime – a "pure" cybercrime.

---

[100] M. Sackson, (1996) Computer Ethics: Are Students Concerned, First Annual Ethics Conference available at <http://www.maths.luc.edu/ethics96/papers/sackson.doc >accessed 24 January 2024
[101] *Ibid*
[102] *Ibid*
[103] *Ibid*
[104] *Ibid*

As such, it requires that we create new law which makes it a crime to launch such an attack. Otherwise, there is no crime, which was the case in the United Kingdom of Great Britain and Northern Ireland (UK) until very recently on Espiner. The U.K. Outlaws Denial-of-Service Attacks, the 1990 Computer Misuse Act outlawed hacking and other online variants of traditional crime, but it does not address DDoS attacks.[105]

To summarize, one reason why the definition quoted above is unsatisfactory is that it does not encompass the proposition that cybercrime can consist of committing "new" crimes – crimes we have not seen before and therefore have not outlawed, as well as "old" crimes. The other issue with this definition is that it links the commission of cybercrime with the use of a "computer network." This is usually true; in fact, the use of computer networks is probably the default model of cybercrime. But it is also possible that computer technology, but not network technology, can be used for illegal purposes. A non-networked computer can, for example, be used to counterfeit currency or to forge documents. In either instance, a computer, but not a computer network is used to commit a crime. Here the computer is used to commit an "old" crime but it is at least conceptually possible that a non-networked computer could also be used to commit a "new" crime of some type.[106]

A better definition of cybercrime then, is that it constitutes the use of computer technology to commit "crime." That is, to engage in an activity that, as noted earlier, threatens a society's ability to maintain internal order. But while cybercrime involves the commission of "crime" in the generic sense, particular cybercrimes may not be proscribed by a society's criminal laws. It is therefore advisable for every society to conduct a periodic

[105] *Ibid*
[106] T. Smith, "Hacker Jailed for Revenge Sewage Attacks," The Register (10 October, 2001), available at <http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/> accessed 26 January 2024

review of its criminal laws to ensure that they are adequate to deal with evolving threats, such as DDoS attacks.[107]

The works of the authors are paramount to this study as they relate to the subject of the study, which is cybercrimes and combatting of cybercrimes in Nigeria. Notwithstanding the contributions made by the aforementioned writers, this research work improved on the existing literature and provided a more up to date analysis and conclusions.

2.4 Discussion on Identified Gaps

Upon delving into the extensive literature surrounding the legal framework for combating cybercrime, a myriad of gaps emerge, casting shadows on the efficacy of current strategies and regulations. These gaps, drawn from a comprehensive review of scholarly works, reveal systemic deficiencies and challenges that impede the effective prevention, detection, and prosecution of cybercriminal activities.

First and foremost, jurisdictional ambiguities loom large, exacerbating the complexity of addressing cybercrimes that transcend geographical boundaries. Scholars have underscored the perplexing maze of jurisdictional issues that arise in cyberspace, where determining the appropriate jurisdiction for investigation and prosecution becomes a Herculean task. Such jurisdictional quagmires not only lead to legal uncertainties but also hamper seamless collaboration among law enforcement agencies across different jurisdictions, thus hindering the swift apprehension of cybercriminals.

Moreover, the lack of consensus on the definition and classification of cybercrimes emerges as a glaring gap in the legal framework. Various studies have highlighted the heterogeneous landscape of cybercrime definitions and categorizations across nations,

[107] B. Wallace, "Next Major Attack Could Be over Net," San Francisco Chronicle (12 November, 2001) Available at <http://dictionary.reference.com/browse/cybercrime> accessed 26 January 2024

leading to inconsistencies in legal standards and impediments to international cooperation. Rapid technological advancements further compound this issue, as new forms of cyber threats continually emerge, often eluding existing legal definitions and regulatory frameworks.

In the realm of procedural and evidentiary challenges, scholars have shed light on the daunting obstacles faced by law enforcement agencies in investigating cybercrimes. Digital evidence, characterized by its ephemeral nature and susceptibility to manipulation, poses formidable hurdles in the collection, preservation, and authentication process. Furthermore, the dearth of specialized training and resources among law enforcement personnel exacerbates these challenges, leaving investigators ill-equipped to navigate the intricacies of digital forensics and cybercrime investigations.

International cooperation, touted as a linchpin in the fight against cybercrime, remains stymied by a host of impediments. Despite the existence of mutual legal assistance treaties (MLATs) and extradition agreements, scholars have highlighted the sluggishness and inefficiencies inherent in cross-border cooperation mechanisms. Delays in obtaining crucial evidence and the reluctance of some nations to extradite cybercriminal suspects underscore the urgent need for streamlined and expedited international cooperation protocols.

The capacity and resource gap in combating cybercrime looms large on the research landscape, particularly in the context of developing nations. Scarce funding, inadequate technological infrastructure, and a dearth of trained personnel hobble law enforcement agencies' ability to effectively combat cyber threats. The absence of specialized cybercrime units and forensic laboratories further exacerbates this capacity shortfall, leaving investigators ill-prepared to tackle the burgeoning tide of cybercriminal activities.

Lastly, legislative and regulatory frameworks exhibit notable lacunae that render them ill-suited to address the evolving landscape of cyber threats. Scholars have pinpointed legislative gaps in areas such as corporate cybersecurity standards, data protection regulations, and liability frameworks for cyber incidents. Outdated laws and regulatory frameworks fail to keep pace with the rapid evolution of cyber threats, leaving individuals, businesses, and societies vulnerable to exploitation by cybercriminals.

In light of these gaps delineated by the literature review, it becomes evident that a concerted effort is imperative to fortify the legal framework for combating cybercrime. Addressing jurisdictional ambiguities, harmonizing definitions and classifications, bolstering procedural capabilities, enhancing international cooperation mechanisms, bridging capacity shortfalls, and updating legislative frameworks represent critical imperatives in the ongoing battle against cyber threats. Only through concerted action and collaboration can policymakers and stakeholders hope to navigate the intricate labyrinth of cybercrime and safeguard the digital realm against nefarious actors.

CHAPTER THREE
LEGAL FRAMEWORK FOR COMBATING CYBERCRIMES

3.1 Legal Framework for tackling Cybercrimes

As a result of the nature of cybercrimes and an undeveloped national legal framework on the topic, cybercrimes often occur internationally.[1] Cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries.[2] As Professor James Boyle noted, if the King's writ reaches only as far as the King's sword, then much of the content on the internet might be presumed to be free from the regulation of any particular sovereign.[3] For instance, cyber criminals across the United States and Europe were indicted by a federal grand jury in May, 2000 for allegedly conspiring to infringe the copyright of more than 5000 computer software programs. These programs were made available through a hidden internet site located at a university in Quebec and Canada.

In the world today, the activities of cyber criminals have become a threat to the society. With the arrival of information age, legislatures have been struggling to redefine laws that fit crimes committed by cyber criminals. The aim of this chapter is therefore to discuss the legal framework of cybercrime in international sphere and in Nigeria and also engage in a comparative analysis with two other selected jurisdictions with reference to the Cybercrime Act and other related Act.

3.2 National Legal Frameworks for Tackling Cyber Crime in Nigeria.

Recent trend to legal responses to Cybercrime and Cybersecurity in Nigeria the first sets of relevant legislations are: -

---

[1]M. Keyser, 'The Council of Europe Convention on Cybercrime' *Journal of Transnational Law and Policy* (2003)' 12 (2),287-326

[2] D. Johnson, and G. David, 'Law and Borders-The Rise of Law in Cyberspace' *Stanford Law Review*, (1996) 48 (13), 67

[3] J. Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' *University of Cincinnati Law Review* (1997) l (66),177

A. Economic and Financial Crimes Commission (EFCC) Act 2004;

This Act was enacted to repeal the Financial Crimes Commission (Establishment) Act, 2002. Section 1 of the Act establishes a body known as the Economic and Financial Crimes Commission (EFCC). Section 5 of the Act charges the commission with the responsibility of the enforcement and the due administration of the Act, the investigating of all financial crimes including advance fee fraud money laundering, counterfeiting, illegal charge transfers and also the prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation. Criminal activities that would come under these economic crimes would include the activities of the 'Yahoo boys' whose activities are sabotage on the economy of the country.[4]

Section 5 has been the basis for various actions of EFCC including Emmanuel Nwude (the accused) in the case of *Federal Republic of Nigeria v. Chief Emmanuel & Ors.*[5]The accused in the case was reputed to have carried out the third world biggest single scam with numerous others pending in count. In this case, the accused persons were charged to the High Court of Lagos State. A 57count charge was proffered against the accused persons including the scamming to the tune of US $181.6 million and they were all found guilty and sentenced accordingly. In addition to this sentence, their assets were forfeited to the Federal Government of Nigeria and the sums of money recovered and returned to their owners.

Sections 14-18 stipulate offences within the remit of the Act. This includes offences in relation to financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to economic and financial crimes.

Section 46 of the Act defines 'economic crime' as the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either-individually or in a

[4]O. Ehimen, and A. Bola, 'Cybercrime in Nigeria' *Business Intelligence Journal* (2010) 3 (1), 95
[5] Suit No: CA/245/05 <http://www.cenbank.gov.ng/419/cases.asap> accessed 2nd March, 2024

group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse dumping of toxic wastes are prohibited.

From the aforementioned provisions, it can be clearly seen that though the EFCC act effectively deals with internet related fraud, the Act still does not go a long way in dealing with cybercrimes. This is because internet related fraud is only a piece of the puzzle. Cybercrime encompasses internet-related fraud and involves other crimes such as hacking, cyber-stalking, child pornography among other crimes.

B. Money Laundering (Prohibition) Act (MLA) 2011 (as amended):

Another related law regulating internet scam is the Money Laundering (Prohibition) Act.[6] It makes provisions to prohibit the laundering of the proceeds of crime or an illegal act. Section 14 (1) (a) of the Act prohibits the concealing or disguising of the illicit origin of resources or property which are the proceeds of illicit drugs, narcotics or any other crime.

Section 17 and Section 18 of the Act also implicates any person corporate or individual who aids or abet illicit disguise of criminal proceeds. Section 10 makes life more difficult for money launderers by mandating financial institutions to make compulsory disclosure to National Drugs Law Enforcement Agency in certain situations prescribed by the Act. In the same way, if it appears that a customer may not be acting on his own account, the financial institution shall seek from him by all reasonable means information as to the true

[6] Money Laundering (Prohibition) Act Cap M18, LFN 2011.

identity of the principal. This enables authorities to monitor and detect suspicious cash transactions and these Sections can be used against criminals who use the internet as a means of unlawfully transferring large amount of money from one account to another.

This Act "makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of a crime, or an illegal act." All financial institutions are required to report transactions made that are above specified thresholds for individuals and corporate bodies. The threshold is billed at US$10,000 or its equivalent shall be reported to the Central Bank of Nigeria, Security and exchange Commission or the Commission in writing within 7 days from the date of transaction. The Act is essentially structured to enable the authorities monitor cash transactions in a bid to tackle money laundering.[7]

From the above provisions, it is very clear that the Act provides elaborately for cyber security and measures to guard against cybercrimes especially in the financial institutions. However, the Act fails to create its own agency for the enforcement of its provisions. Rather the provisions are to be enforced by the Economic and Financial Crimes Commission.[8]Therefore activities and investigations which require the invoking of the provisions if the Act are done via the EFCC or other relevant agencies, and this goes to show another role or responsibility been saddled on EFCC as an agency. Some other relevant laws to the fight against cyber crimes worthy of mention are The Nigerian Evidence Act, 2011,The Criminal Code Act, The Penal Code Act, The Terrorism (Prevention) (Amendment) Act, 2013,The National Identity Management Commission Act.

[7] D. Ashaolu, *Combating Cybercrimes in Nigeria* in D., Ashaolu, (ed) *Basic Concepts in Cyberlaw,* (Velma Publishers, 2012) 54
[8] Section 7 EFCC Act.

C. Advance Fee Fraud and Other Related Offences Act 2006:

The Act was enacted to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences and to repeal other Acts related therewith. Advance fee fraud is a vexing threat and a major problem in Nigeria today.[9] The Act provides for ways to combat cybercrime and other related online frauds. The Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretence, use of premises, fraudulent invitation, laundering of fund obtained through unlawful activity, conspiracy, aiding among other crimes.

Section 2 makes it an offence to commit fraud by false pretence, Section 7 deals with a person who conducts or attempts to conduct a financial transaction which involves the proceeds of a specified unlawful activity. Furthermore, Section 13 vests this responsibility on industry players, including internet service providers (ISPs) and cybercafé operators, among others. While the EFCC is the sub-sector regulator, the Act by virtue of Section 12 prescribes that henceforth, any user of internet services shall no longer be accepted as anonymous. Through what has been described as due care measure, cybercafés operators and ISPs will henceforth monitor the use of their systems and keep a record of transactions of users.[10]

D. An Overview of Cybercrimes (Prohibition, Prevention etc.) Act, 2015

This is an Act that provides for the prohibition, prevention, detection, response and prosecution of cybercrimes and other related matters. The Act is divided into eight parts. Part I provides for the objectives and application of the Act, Part II provides for the protection of critical national infrastructure, part III provides for offences and penalties, Part IV provides for duties of service providers, Part V provides for administration and enforcement, Part VI of

[9] M. Chawki, 'Nigeria Tackles Advance Fee Fraud' *Journal of Information, Law & Technology* (2009) 1 (5), 4.
[10] E. Adomi, 'Combating Cybercrime in Nigeria' *The Electronic Library* (2008) 26 (5), 290.

the Act provides for search, arrest and prosecution, Part VII provides for jurisdiction and international co-operation and Part VIII provides for miscellaneous.

The objectives of the Act are to-

1. Provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
2. Ensure the protection of critical national information infrastructure; and
3. Promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

Before the enactment of this Act, the legal and institutional framework regulating cybercrime in Nigeria was not unified. But through this Act, the legal, regulatory and institutional framework for the combating of cybercrime would be unified. The application of the provisions of the Act would also apply throughout the Federal Republic of Nigeria.[11]The Act looks into the position of the nation with reference to information and communication where it provides for the designation of certain computer systems or networks as critical information infrastructure.[12]

It further provides that: The president may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure.[13]The presidential order made under subsection (1) of this Section may prescribe minimum standards, guidelines rules or procedure in respect of the protection

[11] Cybercrime Act, Section 2.
[12] Cybercrime Act, Section 3.
[13]Cybercrime Act, Section 3.

or preservation of critical information infrastructure; the general management of critical information infrastructure; access to, transfer and control of data in any critical information infrastructure, infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national informational infrastructure; the storage or achieving of data or information regarded critical national information infrastructure, recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and any other matter required for the adequate protection, management and control of data and other resources in any critical information infrastructure.

Through this aforementioned provision of the Act, national security is secured and enhanced by the protection of critical information infrastructure.[14]Part III of the Act provides the offences and penalties in relation to cybercrimes. Through these provisions, crimes committed through computer and computer networks are codified and thus punishable under Nigerian law. Before the enactment of these provisions, only internet related fraud was actually a punishable cybercrime. But this Part of the Act provides for offences and penalties in relation to cybercrimes.

The Act provides for offences against critical national infrastructure. And any person who commits any offence against any critical national information infrastructure, pursuant to Section 3 of the Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.[15] Where the offence committed under subsection (1) of this Section results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of fifteen years without option of fine.[16] Where the

[14]J. Brierly, *The Law of Nations: An Introduction to the International Law of Peace* 6th ed, (Oxford University Press, 2003) 67
[15]Cybercrime Act, Section 5 (1).
[16] Cybercrime Act, Section 5 (2).

offence committed under subsection (1) of this Section results in death, the offender shall be liable on conviction to death sentence without an option of fine.[17]

Critical national information infrastructure is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on national economic strength, national image, national defiance and security, government capability to functions and public health and safety.[18] The critical national infrastructure is therefore a major asset for the nation, and Section 5 (1) would therefore help in promoting national security.

The Act further criminalizes unlawful access to a computer and the crime is punishable with a term of imprisonment of not less than two years or to a fine of not less than five million naira or to both fine and imprisonment.[19] The Act further provides that where the crime of unlawful access to a computer was committed with the intent of obtaining and securing access to any computer data, program, commercial or industrial secrets or confidential information, the offender shall be liable to a term of imprisonment of not less than three years or to a fine of not less than seven million naira or such offender shall be liable to both fine and imprisonment.[20]

The Act discusses unlawful interception of communications, where it further provides that any person, who intentionally and without authorization or in excess of authority intercepts any data from a computer to or from a computer, computer system or connected system or network commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than five million naira or to both fine and

[17]Cybercrime Act, Section 5 (3).
[18]*ibid*
[19]Cybercrime Act, Section 6 (1).
[20]Cybercrime Act, Section 6 (2).

imprisonment.[21] Section 7 aims to secure the internet which is a collection of information, protect data and protect the privacy of individuals in relation to the information they transfer through the net.

The Act also establish numerous other crimes, including unauthorized modification of a computer program or data,[22] system interference,[23] misuse of devices,[24] computer-related fraud,[25] identity theft or impersonation,[26] cyberstalking,[27] and cybersquatting.[28] Section 17 of the Act also criminalizes cyberterrorism and provides that any person who accesses or causes to be accessed any computer system for the purpose of committing a terrorist act as defined under Terrorism (Prevention) Act 2011 as amended commits a cyberterrorism offence and he is thus liable to life imprisonment upon conviction.

The Act also criminalizes child pornography and creates two classes of offenses under this category. The first involves the use of a computer network for the purpose of, among other activities, the possession, production, and/or distribution of materials depicting a minor, a person appearing to be a minor, or images representing a minor engaged in sexually explicit conduct.[29] The second involves the use of 'information and communication technologies' to engage in such acts as luring and meeting (here the crime requires two elements to exist: communicating with a child online followed by an in person meeting) with a child for the purpose of engaging in sexual activities or recruiting a child to participate in a pornographic performance.[30] The penalties for the offences would range from a five to ten year prison term

[21]Cybercrime Act, Section 7.
[22] Cybercrime Act, Section 8.
[23]Cybercrime Act, Section 9.
[24] Cybercrime Act, Section 10.
[25]Cybercrime Act, Section 12.
[26] Cybercrime Act, Section 13.
[27] Cybercrime Act, Section 15.
[28]Cybercrime Act, Section 16.
[29] Cybercrime Act, Section 14.
[30] *Ibid*

or fines ranging from ten to twenty million naira, or both, depending on the particular offense.[31]

The use of a computer system or network to distribute racist or xenophobic materials, materials that deny, approve, or justify acts that constitute genocide or crimes against humanity, or the use of a computer system or network for racist or xenophobic insults, would constitute an offense under Section 18 of the Act, and upon conviction, the offender would be subject to a sentence of at least five years in prison and or a minimum of ten million naira fine.

Part IV of the Act which makes provision for the duties of service providers requires internet and phone service providers to retain and make available to government agencies customer information, including traffic data as well as subscriber information.[32] If a service provider fails to cooperate with government agencies in this regard, it would be subject to a fine of at least N10 million, and its director/manager/officer would be prosecuted and, on conviction, be subject to at least three years in prison and/or a N7 million fine.[33]

The legislation also affords law enforcement officers broad search, arrest, and seizure powers, including some that do not require judicial oversight. This occurs when there is what the legislation calls a 'verifiable urgency' that a cybercrime is about to be committed or that there is an 'urgent need to prevent the commission of an offence,' and obtaining a warrant would take time and be prejudicial to public safety order.[34] In such a circumstance, a law enforcement officer would have the authority to enter any premises or vehicle that he reasonably suspects is being used or likely to be used for the commission of a crime or that

[31] *Ibid*
[32] Cybercrime Act, Section 21.
[33] Cybercrime Act, Section 23.
[34]Cybercrime Act, Section 28.

contains evidence of the commission of a crime.[35] Once the officer is in control of the premises or vehicle, the officer does not have to wait to obtain a warrant; he may conduct searches, seize items, or arrest persons he 'reasonably suspects' to be connected to the crime.[36]Section 33 of the Act also vests authority on the Federal High Courts to try and sanction offences committed under this Act.

The Nigerian Cybercrime Act, enacted in 2015, represents a significant step towards addressing cyber threats and safeguarding digital activities within the country. However, a critical examination of the legislation reveals several notable gaps and shortcomings that warrant attention and action.

Firstly, the Act lacks clarity in defining certain key terms and concepts related to cybercrimes. This ambiguity can lead to confusion among law enforcement agencies, prosecutors, and judges, hindering the effective identification and prosecution of cyber offenders.

Secondly, there are concerns regarding the Act's provisions on jurisdiction and extraterritorial application. Cybercrimes often transcend national borders, necessitating robust mechanisms for cross-border cooperation and enforcement. However, the Act's jurisdictional framework may not adequately address the complexities of prosecuting cybercrimes that originate or have effects outside Nigerian territory.

Thirdly, while the Act provides for the establishment of specialized cybercrime units and the training of law enforcement personnel, there are concerns about the adequacy of resources and capacity-building efforts. Limited funding, outdated technology, and a shortage of skilled personnel may impede the effective implementation of the Act's provisions.

[35] *Ibid*
[36] *Ibid*

Moreover, the Act's provisions on penalties and sanctions for cybercrimes have been criticized for their severity and potential impact on individual rights and freedoms. There are concerns that overly harsh penalties may discourage reporting of cyber incidents and deter individuals from engaging in legitimate digital activities.

Additionally, the Act's focus on criminalizing cyber offenses may overshadow the importance of prevention, education, and awareness-raising initiatives. There is a need for complementary measures to promote cybersecurity hygiene, responsible digital behavior, and the protection of personal data.

Furthermore, the Act's provisions on international cooperation and mutual legal assistance may need to be strengthened to facilitate collaboration with foreign counterparts in investigating and prosecuting cross-border cybercrimes.

Finally, while the Nigerian Cybercrime Act represents a positive step towards addressing cyber threats, there are significant gaps and challenges that must be addressed to enhance its effectiveness. These include clarifying definitions, improving jurisdictional frameworks, enhancing capacity-building efforts, ensuring proportionate penalties, promoting prevention and awareness-raising initiatives, and strengthening international cooperation mechanisms. Addressing these gaps will be crucial in effectively combating cybercrimes and safeguarding Nigeria's digital ecosystem.

3.3 International Legal Frameworks on Cybercrime

The international sphere is wide and as such there are several legal frameworks regulating cybercrime internationally which will be discussed below.

A. The European Legal Framework

The European legal framework is concerned with the repression of cybercrime. This matter has been subject to intervention by a number of international institutions worldwide, such as the United Nations, the G8, the Organization for Economic Cooperation and Development (OECD), the Commonwealth, the Council of Europe and the European Union.[37] From a European perspective, two international agreements are of particular relevance both for their European focus and their legal effect: the 2001 Council of Europe Convention on Cybercrime and the 2005 European Union Framework Decision on attacks against information systems.

I. The Council of Europe Convention on Cybercrime (CoECC)

The Council of Europe Convention on Cybercrime (CoECC) was adopted on 8 November 2001 and opened for signatures at a Conference in Budapest. It remains an historic milestone in the legal control of Cybercrime and has been ratified by 48 states and entered into force on 1 July 2004.[38] This Convention, which is commonly referred-to as the Budapest Convention, breaks new ground by decisively dealing with computer-related crimes and economic crimes. The Convention also aims to achieve three outcomes at a global level. These are:

1. Reducing friction through harmonization and approximation of Cybercrime legislation by providing law enforcement with the tools and new investigative measures;
2. Facilitating co-operation through minimum rules in a more complex framework;
3. Striving for effective implementation.[39]

[37]S. Gordon, and F. Richard 'On the definition and classification of cybercrime' *Journal in Computer Virology*, (2006) 2 (1), 13-20.
[38]S. Schjølberg and Ghernaouti-Hélie global protocol on CyberSecurity and CyberCrime' *CyberCrimelawS.A journal* (2009) 1 (2), 14.
[39]*ibid*

The Convention criminalizes conduct against the integrity, availability and confidentiality of computer systems as well the misuse of computer systems.[40]It clarifies to the technological neutrality and futuristic posture by the Convention, providing a platform for international collaboration across states, apart from the distinctive foresight feature of the Convention portrayed in the administrative provisions.[41] Upon signing or ratifying the Convention, States agree to ensure that their municipal laws criminalize the conduct prohibited by the substantive provisions of the Convention as well as establish systems and procedures to ensure investigation and prosecution of prohibited conduct.[42]

The Convention deals with the substantive law provisions that provide for the criminalisation of computer related offences, content related offences and copyright related offences. Furthermore, the treaty provides for procedural matters to the balance between protection of human rights and providing computer data necessary for prosecutions. Lastly it provides for international cooperation to facilitate the investigation and prosecution of criminal offences, including extradition for trial in member country.[43]

With regard to the CoE Convention, its global reach appears difficult. Indeed, in order to prevent safe havens for cybercriminals, the Convention should be adopted by far more countries than the current signatories/Parties.[44] Remarkably, some of the most important Members of the Council of Europe or signatory Parties in terms of population and GDP have not yet ratified or acceded to the treaty. They include Russia and Turkey (which did not even sign the treaty) as well as Poland, Spain, the United Kingdom, Canada and Japan (which have

[40]S Snail kaMtuze 'CyberCrime in South Africa: Hacking, cracking and other unlawful online activities' *Journal of Information, Law and Technology* (2009) 1 (2), 10.
[41]*Ibid.*
[42]*Ibid.*
[43]Papadopoulos, and S.L Snail. *Cyberlaw @ SA III: The law of the Internet in South Africa* (Van Schaik Press: Pretoria,2012), 102.
[44]K. Archick, Cybercrime: The Council of Europe Convention<http://www.usembassy.it/pdf/other/RS21208.pdf> accessed 2nd March, 2024

not yet ratified it). This points out the difficulties in the implementation of the CoE Convention even within the group of countries which are its main targets, at least in theory. Furthermore, in a global perspective, the current level of implementation is even lower. The majority of the world countries with the highest number of internet users have not signed/ratified the Convention.[45] Even if the pace of ratification/accession is rather rapid compared with other international treaties, the current situation exhibits several shortcomings in the implementation of the international framework on cybercrime.

II. The European Union (EU) Directive

In further strengthening the security of information systems within the EU, the European Commission in 2005 sponsored a proposal[46] for a European Union Directive focusing on data retention through enforcing a duty on internet service providers to retain data traffic necessary for the identification of criminal actors in Cyberspace. The proposal was adopted by the EU.[47] The EU Directive provides for the criminalization of instigating, aiding and abetting and attempting to commit one of the three offences described above. The sentences entail a minimum penalty of at least between one and three years of imprisonment for illegal system interference and illegal data interference. The Directive also provides for aggravating circumstances, at least between two and five years of imprisonment for offences committed within the framework of a criminal organisation. The Directive further underscores the duty of Internet Service Providers (ISPs) to retain traffic data necessary for identifying criminal actors in the Cyberspace.[48]

The efficacy of the legal instrument is compromised by the current realities that the majority of countries globally with the highest number of internet users have not signed or

[45] McQuade III, and C. Samuel. *Understanding and Managing Cybercrime* 3rd edn, (Boston: Allyn and Bacon Press, 2006), 23
[46] *ibid*
[47] *ibid*
[48] *ibid*

ratified the Convention and the pace of ratification is relatively slow in Africa, compared to other international legal instruments. It has been observed that at a global level, implementation is even lower.[49] Notwithstanding its uncertain global reach, the CoECC shows a remarkable indirect impact in influencing domestic legislation and as such, is recognise as a worldwide benchmark for Cybercrime legislation.[50]

B. The African Union (AU) Convention on Cybersecurity and Data Protection

Before the adoption of the African Union (AU) Convention, some efforts on data protection had been achieve. These efforts commenced in 2011 with the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa (AUCLCS)[51] a draft which was subsequently reviewed in 2013. It has been observed[52] that the AUCLCS which gives substance to a Resolution of the last session of the Assembly of Heads of State of Governments of the African Union, with specific purpose on harmonising African Cyber Legislations on E-commerce personal data protection, Cybersecurity promotion and Cybercrime control, profiles Cybersecurity and Cybercrimes provisions on as opposed to enablement and regulation of E-commerce in Africa. The second draft was the African Union Convention on Confidence and Security in Cyberspace. The absence of consultation during the drafting of these legal instruments was at the core of the criticism levelled against them by the private sector, civil society organisations and privacy advocates.[53] Nigeria tops the chart in Africa as the country with the highest number of

[49] F. Cassim, 'Formulating specialised legislation to address the growing spectre of CyberCrime: A comparative study' *PER: Potchefstroom Electronic Law Journal* (2009) 12 (4), 36-79.

[50] *ibid*

[51] African Union Commission, Draft African Union Convention on the Establishment of a Credible Legal Framework for CyberSecurity in Africa (2011) African Union Commission.

[52] *ibid*

[53] L.A Abdulrauf and C.M Fombad, 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa' *Journal of Media Law* (2016) 8 (1), 70-76.

internet users.[54] Africa also hosts four of the ten countries with the highest Cybercrime levels in the world.[55] To augment the inadequacy of Cyber legislations in Africa, the AU Convention on Security in Cyberspace and Personal Data Protection (AUCSCPDP)[56] was sign on 27 July 2014 in Malabo, Equatorial Guinea. The Convention seeks to harmonise and strengthen African Cyber Legislations on electronic commercial organisations, personal data protection, Cyber Security promotion and Cybercrime control. It also sets broad guidelines for incrimination and repression of Cybercrime. The African Union has fifty-four-member States.[57]

Unlike the Council of Europe Convention on Cybercrime (CoECC),[58] the AUCSCPDP[59] relates directly to the challenges that prevail in the African context by:

a. Prohibiting identity flexibility and associative anonymity in e-commerce;

b. Outlawing spam (unsolicited electronic commission);

c. Addressing the use of encryption in Cybercrime; and

d. Prohibiting key forms of online discrimination.

While all these challenges currently constitute Africa's biggest vulnerability in Cyberspace, the AUCSCPDP further provides for independent expert vulnerability testing of internet services; an initiative that introduces an essential process through which Africa's ICT development will proactively incorporate online security measures.[60]The threefold

[54]*ibid*
[55]*ibid*
[56] African Union Convention on Cyber Security and Personal Data Protection. Date of adoption 27 June 2014. Date of last signature: 04 July 2017 <https://au.int/en/.../african-union-conventioncyber-security-and-personal-data- protection>accessed 2nd March, 2024
[57] U.J Orji 'RegionalisingCyberSecurity governance in Africa: An assessment of responses' *IJOR* (2016) (1) (2), 203.
[58] Budapest Convention on CyberCrime (ETS 185) <https://www.coe.intConventions> accessed 2nd March, 2024.
[59] African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) <https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf>accessed 2nd March, 2024
[60]*Ibid*

provisions permitting non-consensual interference with private, personal and sensitive data; the interference with online traffic or content data; and the issuance of search and seizure warrants that permit inappropriate and broad ongoing investigation. The fact that judges will have to be mandated will inadvertently undermine the values that the AUCSCPDP is seeking to protect, such as the rights to privacy and freedom of expression.[61]

3.4 Comparative Analysis of the Nigerian Legal Framework on Cybercrime with select Jurisdictions

This Section of the study attempts a comparative study of some select jurisdictions. The justification selected for the purposes of this analysis are; Kenyan and South Africa. The comparison is further justified based on the fact that cybercrimes goes beyond national boundaries. Although by numerous numbers of literature shows that a formidable or computer repression of cybercrimes requires a global cooperation. Material laws and agencies are expected to be a reflection of this cooperation.

A. Kenya

The Kenyan Cybercrimes Act clarifies in its explanatory memorandum the intention of its drafters to 'provide for offences related to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters; and for connected purposes'. Read as a whole, the Kenyan Cybercrimes Act has two closely related aims: (i) to protect the confidentiality, integrity and availability of computer systems, programs and data; and (ii) to facilitate the detection, investigation, prosecution and punishment of cybercrimes.

[61] *Ibid*

The Kenyan Cybercrimes Act provides, in Part III, for the criminalisation of 27 offences. This far exceeds the number of offences in the Nigerian Cybercrime Act,[62] This greater number of offences results from splitting cybercrimes to highlight specific criminalised conduct as well as from the criminalisation of conduct relating to the fraudulent or wrongful use of electronic data. Although this approach is not without some merits, the overall impact of stipulating many offences leads to unnecessary duplication of offences.

Section 14(1) of the Kenyan Cybercrimes Act criminalises unauthorised access, which entails intentional infringement of security measures with intent to gain unlawful access to a computer system, and with the knowledge that such access is unauthorised.[63] This provision is welcome to the extent that it specifies the material element of the offence that must be satisfied before criminal liability attaches: it requires the actual or attempted breach of security measures of a computer system. However, it offers no elaboration of the acts that constitute gaining or securing access. This is an omission that may present some difficulty when adjudicating alleged cybercrimes. By contrast, with the Nigerian Cybercrimes Act provides a detailed exposition of the instances in which it can accurately be alleged that a person has intentionally and unlawfully secured access to data, a computer program, a computer data storage medium and a computer system. This provides an instructive basis for amending the text of section 14(1) to strengthen its currently defective material element. Also, the wording of the mental element of the offence of unauthorised access is inelegant, legally defective and inadequate.[64] In particular, it fails to specify the qualitative nature of intent as either fraudulent or dishonest, and it does not disclose the motive of such access.

[62] J. Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation'. Monash *University Law Review*(2014) 40(3): 698

[63] 'A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.

[64] Clough, *Principles of Cybercrime*. (Cambridge: Cambridge University Press, 2015) 34

Section 14(3) of the Act is also defective because it distorts the relevance of intent as a core element of the crime and renders it irrelevant what the criminal motive or objective is.

A constructive method of illustrating the deficiency of section 14 of the Cybercrimes Act is to juxtapose it with an equivalent provision that is more comprehensively drafted. Article 2 of the Nigerian Cybercrime Act criminalises illegal access to a computer system and also imposes an obligation on each of the states parties to: establish as criminal offences, under its domestic law, when committed intentionally, the access to the whole or any part of the computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Like section 14(1) of the Kenyan Cybercrimes Act, the above provision specifies the mental elements of the offence: it must be committed 'intentionally' and 'without right'. However, unlike section 14(1), article 2 of the Nigerian Cybercrime Act further specifies that the nature of the intent must be dishonest. More importantly, it draws a connection between these mental elements and the underlying criminal objective by clarifying, in inclusive language, that the ultimate motive of the illegal access should be to obtain computer data or for other dishonest ends.

It is thus recommended that section 14 of the Kenyan Cybercrimes Act be amended to better clarify the specific mental elements of the dishonest intent to gain access to a computer system for the purpose of obtaining computer data, or to commit or facilitate the commission of another offence. Despite its imperfect drafting, section 14 of the Kenyan Cybercrimes Act creditably seeks to define what constitutes 'unauthorised access'. Section 14(2)(a–b) states that access by a person to a computer system is unauthorised if that person (i) is not 'entitled to control access of the kind in question to the program or data'; or (ii) 'does not have consent from any person who is entitled to access the computer system through any function to the

program or data.' This makes it easier for law enforcement and judicial authorities to distinguish between lawful and unlawful access, and is thus a laudable merit of the Kenyan Cybercrimes Act.

Section 15(1) of the Kenyan Cybercrimes Act criminalises unauthorized access 'with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person'. Section 15(2) additionally stipulates that it is immaterial that the further offence was committed at the time when the unauthorised access was secured or at any other time. For an offence that exposes individuals upon conviction to a prison term of up to 10 years or a fine of up to Ksh 10 million, section 15 establishes a broad offence that fails to take sufficient account of the seriousness of the criminalised conduct or its temporal scope. The adverse implication here is that its penal regime does not distinguish between serious and less serious offences. This is an acute legislative flaw that calls for urgent reform.

Besides failing to criminalise only intent to commit a specific act of serious gravity, offences of the kind outlined in section 15 of the Kenyan Cybercrimes Act are not recognised in the Budapest Convention on Cybercrime or the Malabo Convention on Cyber Security. This omission may suggest that the conduct criminalised in section 15 of the Kenyan Cybercrimes Act could effectively be addressed within the offence of unauthorised access. Even so, the legislation from comparable jurisdictions indicates recognition of the need for a distinct offence of unlawful access with intent to commit specific criminalised conduct. Although not identical in wording to the equivalent Kenyan provision, section 36 of the Nigerian Cybercrimes Act 2015 criminalises gaining access, with the intent to defraud, to any device, attachment, email or website to obtain credit card details.[65]

[65] M. Chakwi, A. Darwish, M.A khan, and S. Tyagi, 'Cybercrime, Digital Forensics and Jurisdiction'. Studies in Computational Intelligence. *Springer* (2015) 34

In contrast to both the Kenyan and the Nigerian provisions, section 4 of the South African Cybercrimes Act 2020 criminalises only the unlawful and intentional securing of access. The most commendable aspect is that it crucially relates the criminalised act to other offences, including unlawful acts in respect of software (section 2(2)(c)) and the unlawful dealing in passwords, access codes or similar data or devices (sections 7(1) and 7(2)). This suggests that the drafters of section 15 of the Kenyan Cybercrimes Act likely envisaged the types of offences described in the equivalent cybercrime laws of South Africa and Nigeria, but the text of the resulting provision falls short of the requirements of specificity and legal certainty.[66] To remedy this defect, it is proposed that section 15(1) of Kenya's Cybercrimes Act also criminalise unauthorised access that is designed or intended to facilitate a specified range of offences. Guided by the imperative of legal certainty, it is further proposed that an inclusive list of further offences to which penalty applies on conviction be enumerated in the amended provision. The cross-referencing technique used in the South African Cybercrimes Act 2020 is also highly recommended. On the same rationale, section 15(2) of Kenya's Cybercrimes Act, which makes irrelevant the gravity or timing of the offence, should be struck out altogether.

In Kenya, cybercrime is addressed by the Computer Misuse and Cybercrimes Act, implemented in 2018. This legislation encompasses a broad spectrum of cyber offenses, such as unauthorized access, interception, disclosure, and identity theft. Punishments under this act range from fines of up to 10 million Kenyan shillings to lengthy prison terms, depending on the severity of the crime. For instance, unauthorized access to a computer system could result in a fine of up to 5 million Kenyan shillings or imprisonment for up to 10 years, or both. Similarly, identity theft carries penalties of fines or imprisonment for a maximum of 10 years.

[66] *R v Rimmington and Goldstein [2006] 1 AC 549, para. 33*

These punishments are determined by factors like the extent of harm caused and the value of assets involved.

On the other hand, Nigeria's approach to cybercrime is governed by the Cybercrime (Prohibition, Prevention, Etc.) Act, enacted in 2015. This legislation criminalizes various cyber offenses, including unauthorized access to computer systems, fraud, cyberstalking, and identity theft. Penalties under this act range from fines of hundreds of thousands to millions of Naira, coupled with imprisonment terms of up to 10 years or more, depending on the nature of the offense. Unauthorized access to computer systems, for instance, can lead to fines of up to 10 million Naira or imprisonment for up to 5 years. Similarly, identity theft may result in fines or imprisonment for a maximum of 3 years. As with Kenya, the severity of punishment in Nigeria is influenced by factors such as the degree of harm caused and the value of assets involved.

Both countries have made legislative efforts to combat cybercrime, but the effectiveness of enforcement, judicial practices, and resource allocation may vary, impacting the actual implementation of penalties.

B. South Africa

Nigeria has to draw lessons from the wider regional and international efforts that have been in place for a decade. Therefore, in developing an appropriate legal and regulatory framework, Nigeria has much to learn from South Africa. This is because the two countries face the same challenges in relation to cybercrimes. South Africa has been at the forefront of sub-Saharan countries for taking measures to combat cybercrime.[67]

[67] Law Reform Commission of Nigeria

The South African Criminal Justice System used to extend the common and statutory law as widely as possible to cybercrimes. However, due to the technological changes that have taken place in the world, the South African common law has been found lacking in many of the tools necessary for combating cybercrime. It was also evident that the common law provided for traditional crimes that were committed online but did not provide for cybercrime and legislation had to be introduced to criminalize conduct such as spamming, hacking and phishing[68]. It was also observed by the courts that the prevailing common law could not admit into evidence disputed documents containing information that has been processed and generated by a computer[69].

The South African Government in August 2002 implemented the Electronic Communications and Transactions (ECT) Act, which provided for the facilitation and regulation of electronic communications transactions[70]. Furthermore, the ECT Act contains specific statutory provisions on cybercrime relating to information systems and included unauthorized access to data and interception of or interference with data[71]. Section 86(1) read with the penalty clause in s 89(1) contains an anti-hacking and anti-interception provision that criminalizes unauthorized access to a computer or computer system, or the interception of information, whereas s 86(2) read with the penalty clause in s 89(1) prohibits unlawful modification of data. Section 86(3) read with the penalty clause in s 89(1) and 86(4) and with the penalty provision in s 89(2) contain anti-cracking provisions[72]. E-mail bombing and spamming is an offence under the provision of Section 86(5) and 45, whereas s 87 of the Act criminalizes cybercrimes of extortion, fraud and forgery.

---

[68] *ibid*

[69] *ibid.*

[70] The ECT Act comprises 14 chapters and 95 sections and addresses such issues as online contracts (chapter III), consumer protection (chapter VII), protection of personal information (chapter VIII) and limitation of liability of service providers (chapter XI). It makes specific provision in chapter XIII for the investigation and prosecution of Internet crimes.

[71] *ibid*

[72] *ibid*

At this juncture, for the purposes of drawing comparisons on criminal sanctions between the South African ECT Act and the Nigeria Cybercrime Act, it is interesting to note that in South Africa, Van der Merwe correctly criticized the criminal sanctions of the ECT Act for being too lenient to offenders[73], which appears also to be the case with Nigeria Cybercrime Act[74]. However, in the Electronic Communications and Transactions (ECT) Amendments Bill, 2012[75], maximum penalties of from 12 months to ten years' imprisonment, or fines of up to R10 million for contraventions of s 86(1) to 86(3) are being proposed.

Furthermore, it is important to note that the ECT Act has been in place for a decade, whereas the world has experienced significant increases in hacking, security breaches, data mining for financial purposes, misuse of personal information, cyber-security threats and cybercrime. In response to those challenges the South African government, through its Communications department, has introduced proposed amendments in the ECT Amendments Bill. The Bill seeks to amend the ECT Act to bring it into line with the international community with regard to communications. The Bill also seeks to align the ECT Act with current trends in legislation, such as the Consumer Protection Act[76]and the Protection of Personal Information Act[77]. The ECT Act has facilitated the investigation and prosecution of cybercrime and the admission of electronic evidence. For instance, in *S v Motata*[78]*,* the accused was charged with, *inter alia*, driving a motor vehicle while under the influence of alcohol. After the accused allegedly crashed into the boundary wall of a residential property that belonged to the complainant, the complainant in the matter made certain audio

[73] The penalty provisions of the ECT Act –, maximum periods of imprisonment of one year for most of the crimes prohibited by s 86 of the Act – seems woefully inadequate when compared with those of similar Acts, such as the RIC Act.

[74]Laughren,'Cyber-stalking:awarenessand education'<.http://www.acs.ucalgary.ca/dabrent/380/webproj/jessica.html>, accessed on 2nd March, 2024

[75] Department of Communications, Notice35821 published in *Government Gazette* of 26 October 2012.

[76] Act 68 of 2008

[77] Act 4 of 2013.

[78] Unreported case no. 63/968/07, Johannesburg district court at 622.

recordings on his mobile phone and took some photos on the scene of the accident with a digital camera. The audio recordings were later transferred from the mobile phone and stored on the complainant`s laptop. At the trial the court found that the audio recordings were documentary evidence and ruled them to be admissible.

However, in the subsequent application for review by the applicant, the High Court of South Africa stated that a video film, like a tape recording, 'is real evidence, as distinct from documentary evidence, and provided it is relevant, it may be produced as admissible evidence, subject to any dispute that may arise either as to its authenticity or the interpretation thereof [79]. In another remarkable case, concerning a South African music celebrity, one Molemo 'JubJub' Maarohanye and his co-accused Themba Tshabalala, the magistrate sitting at Protea magistrate's court[80] accepted electronic evidence in the form of cellphone video footage showing the accused persons drag-racing, during which one of their Mini Coopers ploughed into a group of school children on Mdlalose Drive, in Protea North on 8 March 2010. The duo were found guilty on 16 October 2012 on charges of murder and attempted murder and driving under the influence of drugs and alcohol and each sentenced to 20 years' imprisonment.[81]

[79]*Motata v Nair NO* 2009 (2) SA 575
[80]*ibid*
[81]*ibid*

CHAPTER FOUR
ISSUE AND CHALLENGES IN COMBATING CYBERCRIME

In an era where digital connectivity permeates every aspect of modern life, the proliferation of cybercrime poses a formidable challenge to individuals, businesses, and governments worldwide. The landscape of cyber threats continues to evolve, encompassing a myriad of sophisticated tactics designed to exploit vulnerabilities in technology and human behavior. From ransomware attacks crippling critical infrastructure to data breaches compromising personal information on a massive scale, the repercussions of cybercrime extend far beyond the digital realm, impacting economies, national security, and individual livelihoods. As society becomes increasingly reliant on technology, the complexities of combatting cyber threats only intensify, requiring innovative strategies, robust defenses, and international cooperation to safeguard against the ever-present dangers lurking in the digital domain.

4.1 Law Enforcement in Combating Cyber Crime (Skills, Knowledge, Techniques for Effective Investigation)

Innovative cybercrimes, new criminal tactics, and new investigative techniques have all emerged as a result of recent advancements in ICT. The capabilities of law enforcement authorities have significantly increased because to ICT advancements. The use of modern tools by criminals to thwart investigations and prevent identification, on the other hand, presents several difficulties in the world of cyberspace. The skills, expertise, strategies, and difficulties of combating cybercrime are the main topics of this chapter, which also discusses law enforcement and other security bodies.

Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.[1] It can prove difficult to automate investigation processes. While a keyword-based search for

[1] Giordano Maciag, 'Cyber Forensics: A Military Operations Perspective' *International Journal of Digital Evidence*, (2004) 2 (1) 20 <www.utivaacademia.com> accessed 24th February, 2024

illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed has not been modified.[2] Forensic software is able to search automatically for child-pornography images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification of offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face.[3] Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

It is crucial to explore the methods, abilities, and knowledge that law enforcement agencies use to combat cybercrime and to evaluate the efficacy of these methods. The methods employed by law enforcement agencies are listed below:

i. Use of ICTs and the need for new investigative instruments

Offenders use ICTs in various ways in the preparation and execution of their offences.[4] Law enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention) could interfere with the rights of

[2] Kerr, 'Searches and Seizures in a digital world' *Harvard Law Review*, (2005) (1) (19), 546.
[3] Interpol in Appeal to find Paedophile Suspect, The New York Times, (2007), <www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin> accessed 23rd February, 2024
[4] J. Howard , 'Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files' *Berkeley Technology Law Journal*, (2010) 1 (19), 123.

innocent Internet users.[5] If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries.

The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of a far reaching motivation, rather than a specific justification *per se*.

ii. Failure of Traditional Investigation Instruments

Investigating and prosecuting cybercrime requires Internet-specific tools and instruments that enable competent authorities to carry out investigations.[6] In this context, instruments to identify the offender and collect the evidence required for the criminal proceedings are essential.[7] These instruments may be the same as those used in traditional terrorist investigations unrelated to computer technology. But in a growing number of Internet-related cases, traditional investigation instruments are not sufficient to identify an offender. One example is the interception of voice-over-IP (VoIP) communication.[8] In recent decades, states have developed investigation instruments, such as wiretapping, that enable them to intercept landline as well as mobile-phone communications. The interception of traditional voice calls is usually carried out through telecom providers. Applying the same

[5]:Advocate General Opinion, 18.07.2007 < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top> accessed 23rd February, 2024

[6] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[7] Goerling The Myth of user Education, (2005) www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. accessed 23rd February, 2024

[8] The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols.

principle to VoIP, law-enforcement agencies would operate through Internet service providers (ISPs) and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data is transferred directly between the communicating partners.[9] Therefore, new technical solutions together with related legal instruments are necessary.

iii. Encryption Technology

Another factor that can complicate the investigation of cybercrime by law enforcement agencies is encryption technology, which protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime.[10] Encryption is a technique of turning a plain text into an obscured format by using an algorithm.[11] Like anonymity, encryption is not new, but computer technology has transformed the field. For a long time it was subject to secrecy. In an interconnected environment, such secrecy is difficult to maintain.[12]

The widespread availability of easy-to-use software tools and the integration of encryption technology in the operating systems now make it possible to encrypt computer data with the click of a mouse and thereby increases the chance of law-enforcement agencies being confronted with encrypted material.[13] Various software products are available that enable users to protect files against unauthorized access. But it is uncertain to what extent offenders already use encryption technology to mask their activities. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used

[9] ibid
[10] K.O Swale, 'Measures for Ensuring Data Protection and Citizen Privacy Against the threat of Crime and Terrorism – The European Response' *IJOR* (2007) 2 (7) 23
[11] Bellovin and others, 'Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP' (2006) www.lawenforcementagenciesandcybercrime accessed 23rd February, 2024
[12] *ibid*
[13] Singh; The Code Book*:* The Science of Secrecy from Ancient Egypt to Quantum Cryptography; D"Agapeyen, Codes and Ciphers – A History of Cryptography, (2006)www.csecst. gc.ca/documents/about-cse/museum.pdf. accessed 23rd February, 2024

encryption technology, but experts highlight the threat of an increasing use of encryption technology in cybercrime cases.[14] Depending on encryption technique and key size, this process could take decades.[15] For example, if an offender uses encryption software with a 20-bit encryption, the size of the key space is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption. In 2002, the Wall Street Journal was for example able to successfully decrypt files found on an Al Qaeda computer that were encrypted with 40-bit encryption.[16]

Using a 56-bit encryption, a single computer would take up to 2 285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billions years to break it. The latest version of the popular encryption software PGP permits 1 024-bit encryption. Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft's operating systems, for example, allows the encryption of an entire hard disk.[350] Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them,[17]the widespread availability of this technology for any user could result in greater use of encryption. Using software tools, offenders can encrypt messages and exchange them in pictures or images – this technology is called steganography.[354] For investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.[18]

---

[14] *ibid*
[15] Zanini Edwards, 'The Networking of Terror in the Information Age, in Arquilla/Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy' (2018) < www.academia/networksandterrors.com> accessed 23rd February, 2024
[16] Finkelhor Mitchell, 'Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, (2015) www.missingkids.com/en_US/publications/NC144.pdf accessed 23rd February, 2024
[17] Rogaway , 'Introduction to cybercrime'< www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.> accessed 23rd February, 2024
[18] *ibid*

The availability and use of encryption technologies by criminals is a challenge for law-enforcement agencies. Various legal approaches to address the problem are currently under discussion,[19] including: potential obligations for software developers to install a back-door for law-enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations. But encryption technology is not only used by offenders – there are various ways such technology is used for legal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks, self-protection is an important element of cyber security.[20]

iv. Investigation Coordination and Consistency problems

Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations. The mechanisms available to facilitate investigations are often inefficient and lack oversight as to the process by which cybercriminals are pursued. An example of one such mechanism is the use of Mutual Legal Assistance Treaties, commonly known as MLATs. Under an Mutual Legal Assistance Treaties (MLAT), prosecutors in one country may request assistance from their counterparts in a foreign country in order to perform tasks including the investigation of suspects and the collection of evidence.[21] Once provided by the foreign counterpart, the collected evidence may be used in a prosecution in the requesting attorney's country. While simple in concept, the MLAT process is often difficult and time-consuming to accomplish.[22]As an example, for an attorney from the United States to seek subpoena information, execute a search warrant, or gain compliance with a court order under an

[19]I.J Jackson , Blind steganography detection using a computational Immune: A Work in Progress*, International Journal of Digital Evidence,* (2012) 2 (5) 12 www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2- accessed 23rd February, 2024
[20] *ibid*
[21] Funk Marcus, 'Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges' *JSTOR* (2014) 2 (23) 45
[22] *ibid*

MLAT, the attorney must provide a specific request (which must be approved by the foreign nation's courts) identifying, among other information, the requesting agency, a description of the subject matter and nature of the investigation (including the specific criminal offenses suspected to have been committed), and a description of the evidence, information, or other assistance sought.[23] The detailed nature of this request and the requirement for international approval can often complicate and impede efforts at information gathering. This can be particularly true early in an investigation, when the theories driving a prosecution effort may still be in the process of development.

Despite these challenges, the MLAT process remains preferable to the use of "letters rogatory," the predominant alternative method for gathering information across international borders. Under an MLAT, a request for information is made based upon a binding treaty guaranteeing cooperation between the contracting nations; in comparison, a letter rogatory is merely an informal request that relies on the goodwill of foreign courts and law enforcement officials to be properly executed.[24] While it is widely accepted that the formal MLAT procedures will require reform to be effective against cybercrime, the Game over Zeus case provides a fantastic example of how informal international cooperation can and will help provide effective prosecutorial outcomes. In an area where technology consistently outpaces the laws that govern it, such collaborative action will likely be needed to ensure governments keep pace with cybercriminals going forward.[25]

v. Difficulties with Identification and Disclosure of Traffic Data

Separate from inter-country inefficiencies, nearly all cybercrime investigations encounter a common impediment – the anonymity of the internet, and the ability of criminals

[23] *ibid*
[24] Pengelley, Pamela. "A Compelling Situation: Enforcing American Letters Rogatory In Ontario," *La Revue Du Barreau Canadien*, (2019) 8 (5), 346.
[25] J.K Botnet "U.S. Leads Multi-National Action Against "Gameover Zeus" and "Cryptolocker" Ransomware, Charges Botnet Administrator," *U.S. Department of Justice,* (2014) 1 (5) 24

to cover their tracks. Since 1998, the International Corporation for Assigned Names and Numbers, or ICANN, has been responsible for, among other tasks, "coordinating the allocation and assignment of three unique identifies for the internet" – domain names, IP addresses, and protocol port and parameter numbers.[26] In plain English, this means that ICANN directly or indirectly oversees how and where individuals and their computers are identified on the Internet. Under current standards, ICANN effectively allows anonymous registration of domains, and does not appear to independently verify contact information provided to it by thirdparty registrar companies.[27]

Minor changes to the operation of ICANN could provide significant barriers to the use of computer networks for criminal purposes. For example, if ICANN were to require the submission and verification of a government-issued identification in order to register a domain name, the pool of individuals who submit false information would almost certainly shrink. As ICANN's registration requirements evolve over time, the organization will have no choice but to weigh privacy concerns against the need for effective tracing of criminal actions online. Apart from ICANN's registration requirements, much other inefficiency exist in pursuing the identities of cybercriminals. International cybercrime cases often involve tracing a hack through multiple IP addresses around the world, which can, in turn, mean digging through multiple layers of anonymity. Because speed is key to keep online "trails" from growing cold, some intergovernmental organizations have recognized a special need for expedited disclosure of cyberspace traffic data across international lines. One such effort in this area has been spearheaded by the Council of Europe, who requires (with few exceptions) that where a "tracing" request is made between Council member-states, "a sufficient amount of traffic data" must be "expeditiously disclose in order "to identify the service provider and

[26] "Bylaws for Internet Corporation for Assigned Names and Numbers," *ICANN*, July 30, 2014.
[27] "Verifying Contact Information for ICANN Validation," *GoDaddy, Inc.*, undated (verifying only that a user has provided GoDaddy with an "active and accurate" e-mail account in order to confirm ICANN validation).

the path through which the communication was transmitted.[28] Ultimately, if the global community is able to meet the unique challenges presented by cybercrime, it will do so because sovereign nations band together, combine their resources, and recognize that cybercriminals rarely restrict themselves to the borders of a single nation. By embracing a policy of openness, and by placing an emphasis on efficient and effective collaboration, the world be best able to beat back the ever-growing and increasingly sophisticated plague of hackers lurking online.

4.2 Legal Challenges in Tackling Cybercrime

Despite the legislative and regulatory measures to counter cybercrime, there are a few legal challenges that remain. These will be considered in turn.

i. Jurisdictional Problems

Simply put, jurisdiction can be defined as scope of authority. It is the inauguration of legal authority.[29] Jurisdiction is arguably the most topical issue in Nigerian jurisprudence and „probably one of the most contested issues in the regulation of cyberspace.[30]Prior to the enactment of the Cybercrime Act, the trial of a financial cybercrime would have raised complex jurisdictional issues, given the recent decisions of the Court of Appeal in *Okey Nwosu v FRN*[31]and *Akingbola v FRN*[32] that criminal jurisdiction over matters delineated in Section 251 of the Constitution belongs exclusively to the Federal High Court. This issue is far from settled, as a decision of the Supreme Court is in the offing.[33] However, with respect to cybercrimes, the Cybercrime Act has expressly stipulated exclusive jurisdiction for the

[28] "Convention on Cybercrime," *Council of Europe*, Budapest, 23.XI.2001, Article 30.
[29] S. Dorsett and S McVeigh, *Jurisdictioal challenges cybercrime* 4th edn. (Jurisdiction Routledge, O.N publishers, 2013) 4.
[30] *ibid*
[31] (2013) LPELR-22143.
[32] (2014) LPELR-24258.
[33] The decision in *Okey Nwosu v FRN* is now on appeal to the Supreme Court.

Federal High Court in respect of offences created under the Act.[34] The vesting of powers to hear offences of cybercrimes under section 50 of the Cybercrime Act creates a burden on the Federal High Court where is already inundated with cases already specified under S.251 of the Constitution, but in our opinion there should be a special division for such case to aid smooth and fast dispensation of justice this is because it can cause delay in the prosecution of cybercrimes in Nigeria.

The jurisdictional challenge emphasises the need for regional and/or international harmonisation of anti-cybercrime regulations and laws. With particular reference to banking, the challenge is exacerbated by globalisation and the attendant blurring of traditional territorial borders in financial markets. Realistically, establishing an international anti-cybercrime regime might not go beyond the level of soft law.[35] It has been aptly observed that international financial law comprises mostly of soft law, with a system of equal and sovereign states whose actions are limited only by rules freely accepted as legally binding.[36] Harmonisation is perhaps more realistically feasible on a regional rather than on an international level, as there is likely to be more convergence of regulatory and legislative objectives at the regional level.[37] The CECC has emerged as a relatively successful model at the European level because of the EC legislative framework.[38] Such standardised framework is yet to be put in place in Africa. Perhaps, policy makers can explore the more feasible option of bilateral arrangements. Again, the ratification and domestication of the CECC will enable Nigeria to take advantage of the mutual assistance and reciprocity provisions. A major limitation of the provisions of section 50 of the Cybercrime Act is the fact that other foreign States are not bound to enforce them.

[34] Section 50 of the Cybercrime Act
[35] V.D Degan, *Sources of International Law* (Nijhh off Publishers London, 2007) 238.
[36] *ibid*
[37] In recent years, regional cooperation and institutions have developed faster and easier than international systems.
[38] J. Goddard et. al, European Banking: An Overview *Journal of Banking and Finance* (2007) 2 (7), 191

While S. 51 of the same Act provide that "offences under the Act shall be extraditable where the extradition Act. Though under the international laws, a country has no obligation to turn over a criminal to the requesting entity. Section 52 of the Cybercrime Act, recognises the need for international cooperation. Perhaps, this provision might be utilised for cross-border cooperation agreements, with provisions for information sharing and cooperation in investigation and prosecution. Such agreements will ensure mutual recognition of domestic regulatory and legislative provisions, so that cybercriminals do not find jurisdictional safe havens by exploiting discrepancies in national laws.[39]

Electronic robbers and forgers leave fewer clues than white-collar criminals who alter checks or intercept promissory notes. For example, a skilled forger who adds zeroes to a check leaves more clues than a digital thief. The use of false email headers, offshore sites, and anonymous e-mailers also make catching cybercriminals more difficult. Because cybercrime is borderless by its nature, it creates new methods of concealing wrongdoing.[40] "Dual criminality and jurisdictional conflicts" is a principle of international criminal law under which an accused individual may be extradited "only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations." *U.S. v. Saccoccia***,** This principle often provides a direct roadblock to prosecution of international cybercrime, and it was a key factor in barring prosecution of the Love Bug attack – the extradition treaty between the Philippines and the United States demands dual criminality.[41] As a result of the Philippines‟ lack of computer crime statutes, the actions of the GRAMMER Soft ring were not considered a punishable offense outside of its borders; thus,

[39] R. Pratt and H. Schiffman, (2007) „Cross-Border Cooperation and Information Exchange: Overcoming the barriers to Regulatory Cooperation‟ in Working Together: Improving Regulatory Cooperation and Information Exchange, Monetary and Financial Systems Department IMF Washington DC.
[40] P. Weil, Toward Relative Normativity in International Law, *77 American Journal of International Law* (2007) 2 (2) 413;
[41] U.S. Treaty Doc. 104-16, Extradition Treaty with the Philippines ("Article 2(1) defines an extraditable offense as one punishable under the laws of both Contracting Parties by deprivation of liberty for a period of more than one year, or by a more severe penalty").

investigators from the United States were unable to extradite members of the Grammer Soft hacking ring to face prosecution.

In response to these frequent dead-ends, the international community has taken steps to help encourage greater cooperation between nations with respect to cybercrime, including passage of UN General Assembly Resolution 55/63, designed at combating international "criminal misuse of information technologies." Resolution 55/63 specifically calls on all member states to "eliminate safe havens for those who criminally misuse information technologies," and further establishes that "law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States." UN General Assembly Resolution 55/63, "Combating the criminal misuse of information technologies."[42] These global efforts have been echoed on the regional level as well, with groups such as the Organization of American States calling upon its member-states to create a framework for enacting laws that protect information systems, prevent the use of computers to facilitate illegal activity, and punish cybercrime.[43] Despite these efforts, there remains significant resistance to abandoning the "dual criminality" principle, as nations are loath to expose their citizens to international criminal liability when such acts are not illegal under (and sometimes condoned by) the accused's native government. Moreover, as seen in the Sony hack, many nations (including the United States) recognize the utility of cyber warfare as a key method of non-military aggression, and they may be resistant to allowing foreign governments to extend jurisdiction over such actions.[44]At this time, jurisdictional and other issues related to "dual criminality" seem likely to persist into the future; insufficient incentives exist for governments to change

[42] *ibid*

[43] Organization of American States Resolution AG/RES 2004 (XXXIV-O/04), "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cyber Security: A Multidimentional and Multidisciplinary Approach to Creating a Culture of Cyber Security.

[44] Hancock, David. "Feds Out-Hack Russian Hackers," *CBS News*, May 12, 2002 (discussing the Invita operation, the FBI counter-hacking sting of Russian nationals engaged in the theft of credit-card information).

current practices and allow greater international oversight over their online actions and the actions of their citizens. Despite this, countries may find themselves needing to weigh the advantages of jurisdictional sovereignty against their ability to effectively combat an ever-increasing number of cross-border cybercrime attacks.

ii. Evidential Issues

Although the Evidence Act 2011 had significantly ameliorated the hitherto major obstacle to the admissibility of evidence, the problem is not over, S. 126 and 127 of the Act[45] requires all facts to be proved in court by direct oral evidence unless with regards to the contents of a document. The implication is that witnesses and victims of cybercrime must be in Nigeria for such trial, considering the cost implications. The Act has not make provision for the adoption of technology for taking aid or transmission of testimonies, for example, through video conferencing etc., for this challenges to be mitigated. S. 15 also gave judge discretion to exclude some evidence obtained improperly or in contravention of law unless the judge deem same to be desirable.

Section 84 of the Evidence Act (EA) 2011 provides for the admissibility of computer-generated evidence. It makes computer-generated evidence admissible in any proceedings upon the fulfilment of certain conditions including the production of a certificate identifying the document and the information contained in it were produced by proper operating computers. There is no gain saying that all evidence to be tendered in proceedings bordering on cybercrime will be of a computer-generated nature.

[45] Evidence Act 2011

Consequently, section 84 of the EA must be complied with. In *Kubor v Dickson,*[46] the Supreme Court held that for computer-generated evidence to be admissible in court, all the conditions set out in section 84 of the EA must be fulfilled.

Prior to the promulgation of section 84 of the EA, attempts to tender computer-generated evidence met with admissibility bottlenecks.[47] The precise nature of the requirement of section 84 of the EA remains unclear and it is certain that the admissibility of computer-generated evidence will still remain a challenge. Moving forward, specific provisions in the CA dealing with admissibility of evidence should facilitate the trial of offences established under the Act. S. 15 of the Act[48] which provides that the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence on the mere grounds that it is constituted by a data message. It further mandates that information contained in data messages must „be given full evidential weight. So long as the Evidence Act remains applicable to the Cybercrime Act, admissibility issues will continue to hinder the expedited prosecution of cybercrimes.

iii.Legality of the BVN Directive

The BVN is aimed at checkmating both cybercrime and money laundering. However, the irony of the BVN requirement is that it triggers the inherent risk of leaving bank customers vulnerable to cybercrime attacks. The BVN requirement involves the storage of sensitive biometric data, which in itself is the target of cybercriminals. A more fundamental issue is the legality of the BVN Directive itself. The Directive was made pursuant to powers conferred by section 57 of Banks and Other Financial Institutions Act (BOFIA). This power to make guidelines is intended for the furtherance of the general objects of BOFIA. By the tenor of the provisions of BOFIA, the powers of the CBN are exercisable only over licensed

[46] (2013) 4 NWLR (Pt. 1345) 534.
[47] *Yesufu v African Continental Bank Limited* (2012) 1 BFLR 757.
[48] South African Electronic Communications and Transactions Act 25 of 2002 (ECT)

banks and other financial institutions. Before exercising such powers the requirement for notices had to be observed.

iv. Privacy concerns

The 1999 Nigeria Constitution[49] as amended guarantees the right to privacy of citizens. This right must extend to the most private and sensitive data and information of citizens, including biometric data. This raises a two-fold concern. The first relates to the constitutionality of the requirement for personal information under the KYC and BVN initiatives. This requirement might be considered intrusive and a breach of the constitutionally guaranteed right to privacy, particularly given the multiplicity of biometric data requests by various regulators in Nigeria.[50] The study, suggests that there should be harmonization among service provider and for the government to have a centralized data base which could aid in checkmating the excesses of customers and to eschew multiplicity biometric data.

The second implication raised by the constitutional right to privacy is the obligation placed on government and its agencies to safeguard the various data and information banks and their customers. A failure to protect the information of citizens from cyber attacks will constitute a fundamental breach of the constitutionally enshrined right to privacy.

v. Social networking new platforms for cybercrime

Social networking sites and the number of users expanded considerably in recent years,[51] and are now also used for spreading malware, offer targets for other form of

[49] Section 37 of the 1999 Constitution of Nigeria as amended.
[50] The National Identity Management Commission, Federal Road Safety Commission, Nigerian Communications Commission (NCC), National Immigration Service and other public as well as private institutions have initiated compulsory biometric data registration requirement.
[51] J.Y Subra, Facebook alone claimed some 845 million active users in December 2011 (2012)<http://www.facebook.com/press/info.php?statistics> accessed 23rd February, 2024

cybercrime and constitute security risks. According to *Sophos*,[52] social networks have become a viable and lucrative market for malware distribution with Web 2.0 botnets stealing data, displaying fake antivirus alerts and generating income for criminals. The proportion of companies reporting spam and malware attacks via social networking increased by 70% in 2009. Employees logging on to social networking sites thus pose serious security risks to the information systems of their companies or institutions by opening them up for spam, phishing, malware and data infiltration.[53]

vi. Availability of devices and access

Only basic equipment is needed to commit computer crimes. Committing an offence requires hardware, software and Internet access. With regard to hardware, the power of computers is growing continuously.[54] There are a number of initiatives to enable people in developing countries to use ICTs more widely.[55] Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes. Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection.[56] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.[57] The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in

[52] Sophos Security Threat Report 2010 (August 2010). <http://www.sophos.com/security/topic/security-report-2010.html> accessed 23rd February, 2024
[53] *ibid*
[54] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. accessed 23rd February, 2024
[55] *Ibid*
[56] Kerr, 'Searches and Seizures in a digital world', *Harvard Law Review*, 2005, (2) 9 23
[57] In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime.

developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so-called "wardriving". The term describes the act of driving around searching for accessible wireless networks.[58] The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks, hacked networks and prepaid services without registration requirements. Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users.[59] However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce.[60]

It has been suggested that this limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case *Autronic v. Switzerland,*[61] the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

---

[58] J. Ryan, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, *Virginia Journal of Law and Technology*, (2004) 9 (2) <www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf> accessed 23rd February, 2024

[59] *ibid*

[60] K. Burnheim, The right to communicate, The Internet in Africa, (2013)www.article19.org/pdfs/publications/africa-internet.pdf accessed 23rd February, 2024

[61] ECHR 12726/87

CHAPTER FIVE
CONCLUSION

5.1 Summary of Findings

This research work has succeeded in giving a conceptual analysis on ‘cybercrime’ by discussing the different definitions on ‘cybercrime’ proffered by different scholars. It also enunciated the substantive and substantial characteristics of cybercrime, in order to depict that it is a distinct phenomenon from what is known as traditional crimes. The work also conducted an analytical discussion on the typologies of cybercrime and other related concepts such as ‘cyber-attack’ and ‘cyber-warfare’. The research discussed the international legal framework on cybercrime focusing on the 'convention on cybercrime' and other relevant framework regulating cybercrime in international sphere. In addition, the research work also discussed the various Nigerian statutes and institutions regulating cybercrime, making a comparative analysis with the foreign jurisdictions, with particular reference to the Kenya jurisdiction and the South Africa jurisdiction

In the course of the research, certain loopholes and gaps within the legal framework regulating cybercrime in Nigeria were observed. The loopholes that were observed include the inability of the Cybercrime Act to effectively deal with the creation and distribution of viruses, the inability of the Cybercrime Act to effectively deal with email spam, etc. Nigeria has made significant strides in enacting legislation to address cybercrime, notably with the passage of the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015. The Act criminalizes various cyber offenses and provides legal mechanisms for investigation and prosecution.

However, implementation and enforcement remain key challenges, with limited resources, institutional capacity, and coordination among law enforcement agencies hindering effective responses to cyber threats.

Comparative analysis with Kenya and South Africa reveals varying approaches to cybercrime legislation and enforcement across the region. While Nigeria's Cybercrimes Act represents a significant step forward, gaps and inconsistencies exist compared to the more comprehensive legal frameworks in Kenya's Cybercrimes Act of 2018 and South Africa's Cybercrimes and Cybersecurity Bill.

The research identifies several issues and challenges faced in tackling cybercrime in Nigeria: Limited awareness and understanding of cyber threats among the general populace, law enforcement agencies, and judicial authorities. Inadequate technical capacity and resources for effectively investigating and prosecuting cybercrimes. Jurisdictional complexities and coordination challenges, particularly in cross-border cyber investigations.

Concerns regarding the protection of civil liberties and privacy rights amidst efforts to enhance cybersecurity measures. The proliferation of cyber threats, including phishing, ransomware, and identity theft, necessitates continuous adaptation and reinforcement of legal frameworks.

In conclusion, the research underscores the importance of strengthening Nigeria's legal framework for combating cybercrime through enhanced implementation, capacity building, and international cooperation. Addressing the identified challenges requires a multifaceted approach, including raising awareness, improving technical capabilities, and fostering collaboration among stakeholders. Furthermore, lessons gleaned from comparative analyses with Kenya and South Africa can inform efforts to refine and augment Nigeria's cybercrime legislation, ensuring it remains effective and responsive to evolving threats in the digital age. With respect to these loopholes, certain recommendations have been suggested to help remedy these shortcomings.

5.2 Recommendations

i. Legislation relating to cybercrime must be enacted with much precision in order to deal effectively with the acts of the cybercriminals. Information technology

professionals should be involved at the law-making process so as to help make laws that would be in line with the present level of technology.

ii. The public should also be well enlightened on how exactly computer systems and computer data can be protected. For example, the use of anti-viruses and passwords among the public should be encouraged. There are cases where the breaking into of a computer system is made to look as if it is from an unknowing victim who is unaware of anything, which is usually due to a virus installed on the 'unsuspecting victim's computer or easy access to the 'unsuspecting victim's computer due to lack of comprehensive security such as lack of comprehensive firewall, passwords and anti-viruses. The use of anti-viruses and passwords among the public would go a long way in enhancing computer security.

iii. It is recommended that in order to reduce the scourge of cybercrime in the country, financial institutions in the country should establish fraud detection departments. There is a need to reconsider the prohibitive aspects of our laws. The inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most cyber-crimes and their conventional network. There is a need to develop a comprehensive internet legislation to regulate electronic financial transactions and prevent electronic crimes. As long as there is an absence of a centralized electronic databank containing specific information on each individual resident and visitor to Nigeria, exposure of criminal intentions before they are executed and the effective investigation of crimes committed would continue to pose a serious challenge to security agencies.

iv. They ought to be legislative reforms and amendment of legislation in combating cybercrime and full harmonization with international legislation in order for legislation on cybercrime in Nigeria to keep pace with e-crime, especially as it becomes more prevalent and sophisticated hence there is the need to develop a common platform to address cyber security since cybercrime crosses borders and cannot be fought by one country. There is need for the National Assembly to amend the cybercrime Act by inserting a provision prescribing punishment under section 7 that relates to operation of cybercafés to make effective and efficient, the law making body should also expedite action to pass necessary Bills, that could help in curbing internet related crimes including the Economic and Financial Crimes Commission Act (Amendment) Bill 2010, Electronic Transactions Bill, 2015 and Payment System Management Bill 2015 all these are yet to become law and it relates to Cybercrimes.

5.3 Contribution to knowledge

This dissertation contributes to knowledge in the following ways:

a. This research contributes to the expansion of knowledge in the field of cybercrime regulation, offering valuable insights for policymakers, legislators, law enforcement agencies, legal practitioners, academics, and other stakeholders. By fostering a deeper understanding of the regulatory challenges and opportunities in combating cyber threats, this work seeks to inform evidence-based policy interventions and shape the future trajectory of cybercrime governance.

b. This research presents an extensive and innovative exploration of the regulatory landscape governing cybercrime, and to significantly contribute to the depth of knowledge in this

critical domain. As the digital realm continues to evolve, so too do the complexities and challenges associated with combating cyber threats, necessitating a comprehensive understanding of the regulatory frameworks in place.

c. By synthesizing insights from legal scholarship, policy analysis, and empirical research, this work sheds light on the multifaceted nature of cybercrime regulation. It dissects the intricacies of legal definitions, jurisdictional boundaries, procedural requirements, and enforcement mechanisms, offering nuanced insights into the challenges and opportunities inherent in regulating cyber activities.

5.4 Area for Further Studies

The following are the necessary area for further studies;

1. International Cooperation: Investigation on the role of international cooperation mechanisms, such as mutual legal assistance treaties (MLATs), extradition agreements, and international conventions, in addressing transnational cybercrime. Assessing the challenges and opportunities associated with cross-border cooperation among law enforcement agencies, judicial systems, and other relevant stakeholders. Exploring ways to strengthen collaboration and coordination at the global level to effectively combat cyber threats.
2. Privacy and Human Rights: Examination of the intersection of cybercrime laws with principles of privacy, data protection, and human rights. Evaluate the balance between law enforcement objectives and individual rights in the context of cybercrime investigations, surveillance measures, and data retention policies. Consider the implications of legal frameworks for protecting digital freedoms and safeguarding civil liberties in the digital age.

3. Corporate Liability: Exploring the legal responsibilities and liabilities of corporations and other entities in preventing and mitigating cybercrime. Analyze the adequacy of existing regulations governing cybersecurity practices, data breach disclosure requirements, and corporate accountability for cyber incidents. Consider potential legal reforms or regulatory frameworks to incentivize proactive cybersecurity measures and enhance corporate accountability in combating cyber threats.
4. Capacity Building and Training: Investigation on the role of capacity building initiatives, training programs, and technical assistance efforts in strengthening legal frameworks for combating cybercrime. Assess the effectiveness of educational programs for law enforcement officials, prosecutors, judges, and other relevant stakeholders in understanding and addressing cyber threats. Identify gaps in knowledge and skills and propose strategies for enhancing capacity building efforts to improve cybercrime investigation and prosecution.

5.5 Conclusion

Cybercrime is a great threat to the Nigerian economy and even to its national peace and security. The study has shown that the abuse of computer technology threatens national security, public safety and even devastates the lives of affected individuals. However, Nigeria like most African countries has a weak legal framework and a weak legal enforcement to effectively combat cybercrime. As shown in the research work, the legal framework regulating cybercrime in Nigeria is not as comprehensive like other developed jurisdictions. The Nigerian legal system in this regard, though above average, still has certain loopholes as already identified in this work.

Our extensive examination of the regulatory framework surrounding cybercrime reveals a complex and dynamic landscape shaped by a myriad of legal,

technological, and socio-political factors. Throughout this study, we have explored the evolution of cybercrime regulation, scrutinized the effectiveness of existing legal instruments, and identified key challenges and opportunities in combating cyber threats.

Our analysis underscores the critical importance of a multifaceted approach to cybercrime regulation that integrates legal, technological, and policy perspectives. While significant strides have been made in developing national, regional, and international laws to address cyber threats, gaps and inconsistencies persist, hindering effective enforcement and cooperation.

One of the central challenges identified is the rapid pace of technological innovation, which continually outpaces regulatory responses. Emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things, present new opportunities for cybercriminals while posing unprecedented challenges for law enforcement and regulatory agencies.

Moreover, the transnational nature of cybercrime complicates regulatory efforts, necessitating enhanced international cooperation and coordination. Jurisdictional issues, differences in legal frameworks, and varying levels of technical capacity further exacerbate the complexities of cross-border cyber investigations and prosecutions.

Furthermore, the protection of fundamental rights, including privacy, freedom of expression, and due process, must remain paramount in the development and implementation of cybercrime regulations. Balancing the imperatives of security with respect for individual liberties is essential to building public trust and legitimacy in regulatory efforts.

Moving forward, addressing these challenges will require a concerted and collaborative effort involving governments, law enforcement agencies, international

organizations, the private sector, civil society, and academia. Innovative approaches, such as public-private partnerships, capacity-building initiatives, and information-sharing mechanisms, hold promise in enhancing cyber resilience and promoting a more robust regulatory framework.

Additionally, ongoing research and dialogue are essential to staying abreast of evolving cyber threats and regulatory best practices. By fostering interdisciplinary collaboration and knowledge exchange, we can better adapt regulatory responses to the dynamic nature of the cyber landscape and effectively confront emerging challenges.

In conclusion, while the task of regulating cybercrime is formidable, it is not insurmountable. By embracing a holistic and forward-thinking approach, grounded in principles of legality, proportionality, and human rights, we can work towards a more secure, resilient, and inclusive digital future. In this respect, it is submitted that if the succeeding recommendations in this Chapter are implemented, it would go a long way in combating cybercrimes in Nigeria, thus enhancing computer security and cyber security.

BIBLOGRAPHY

BOOKS

Ashaolu D.D. and Oduwale O.A, *Policing Cyberspace in Nigeria: A Publication in Honour of Col. Sani Bello (Rtd)*. (Life Gate Publishing Co. Ltd., Ibadan, 2009).

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

Babaji B, '*Cybercrimes under Nigerian Law'* (2010, A.B.U., Press Ltd., Zaria) 517 - 523

Babaji B., *Admissibility of Documentary and Electronic Evidence under Nigerian Law. Ph.D Dissertation* (unpublished, Faculty of Law, A.B.U., Zaria,2013) 387-476.

Bali O., *Information Technology and the Law: The Nigerian Perspective* (Legal Digest Publishing, Lagos, 2010) 8 – 100.

Brierly, J., *The Law of Nations: An Introduction to the International Law of Peace* (Oxford University Press, 6th ed, 2003)

Brill E.A and Baldwin F.N. and Munro R.J *Cybercrimes and Security* (Oceana Publications Inc., U.S.A., 2010)

Cambridge Advanced Learner's Dictionary (3rd edn, Cambridge University Press, 2008) 284

Cambridge Advanced Learner's Dictionary (3rd edn, Cambridge University Press, 2008)

Clifford R**.**, *Cybercrime: The Investigation, Prosecution and Defence of a Computer-Related Crime* (Caroline Academic Press, 2001).

Ferrera,G. *CyberLaw: Texts and Cases* (Southwestern College Publishing Co, 2001).

Garner B. Blacks Law Dictionary, (9th edn, Thompson Reuters Business, 2004) 427

Jaishankar K., *Space Transition Theory of Cyber Crimes, Crimes of the Internet*, (Pearson, ISBN-13:9780-13-231886-0, 2008) 283.

Ladan M.T, '*Cyber Law and Policy on Information and Communications Technology in Nigeria and ECOWAS.*' (A.B.U. Press Ltd., Zaria, 2015).

Ladan M.T, *Introduction to Jurisprudence: Classical and Islami* (Faith Printers International, Zaria, 2013) 5 – 16.

Loftness, S. *Responding to" Phishing" Attacks*. (Glenbrook Partners, 2004).

Mara, Marie Helen, *Cybercriminology* (Oxford University Press, 2016) 23.

McQuade III, and Samuel C. *Understanding and Managing Cybercrime* (Boston: Allyn and Bacon Press, 2006), 23

Osinbajo Y. *Cases and Materials on Nigerian Law of Evidence* (Macmillan Publishers, Lagos 2010), 270-296.

Papadopoulos S, and Snail SL, *Cyberlaw @ SA III: The law of the Internet in South Africa* (Van Schaik Press: Pretoria,2012), 102.

Peters, *Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection* (Multimedia, 2007; ITU Global) 217

Tokura S.S *The Legal Regime of Cyber Security and Crime: Challenges of Enforcement in Nigeria*.

Tudor J.K., *IS security Architecture, An Integrated Approach to Security in the Organization*. (Auerbach Publications, USA, 2001).

Wasik M, 'Crime and the Computer', (Oxford University Press, 1991) 30.

JOURNALS

Adomi E, 'Combating Cybercrime in Nigeria' (2008) (26) (5) *The Electronic Library,* 290.

Barclay Corlane, 'Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica' (2017) (43) (1) *Commonwealth Law Bulletin*, 77-107.

Bash E., 'Ethical Hacking and Countermeasures: Spamming' (2015) (1) (3) *Law Journal series* 5

Brummer C. , *Soft Law and the Global Financial System, Rule Making in the 21st Century* (Cambridge University Press, 2012),

Carter D. 'Computer Crime Categories' (2005) (64) (21) *FBI Law Enforcement Journal,* 271.

Chawki, M., 'Nigeria Tackles Advance Fee Fraud' (2009) (1) *Journal of Information, Law & Technology,* 4.

Conley C.H, 'Cybercrime' (2004) (6) (218) *NIJ Reports*, 3.

Ehimen O. and Bola A., 'Cybercrime in Nigeria' (2010) (3) (1) *Business Intelligence Journal*, 93-98

Ellison L. and Akdeniz Y., 'Cyberstalking: The Regulation of Harassment on the Internet' (2009) (1) (29) *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet.*

Gordon S. and Richard F. 'On the definition and classification of cybercrime' (2006) (2) (1) *Journal in Computer Virology*, 13-20.

Hassan.B et al, 'Cybercrime in Nigeria: Causes, Effect and the Way Out' (2012) (2) (7) *ARPN Journal of Science and Technology,* 26

kaMtuze S Snail *A Comparative Review of Legislative Reform of Electronic Contract Formation in South Africa* (2015) 83.

LA Abdulrauf and CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa' (2016) (8) (1) *Journal of Media Law,* 70-76.

Longe O.B and others, 'Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities' (2009) (6) (3)*; International Journal of Computer Science and Information Security,* 25.

Longe O.B, and Chiemeke S.C, Beyond Web Intermediaries: Framework for Protecting Web Contents on Clients Systems (2007) (1) (5) *International Conference of the International Association of* Engineers.

Longe, O.B and Chiemeke S.C., 'Cybercrime and Criminality in Nigeria- What roles are internet Access Points in Playing' (2006) (6) (4) *European Journal of Social Sciences*.

Mansfield E D, and Milner H.V, 'The New Wave of Regionalism' (2004) (53) (3) *International Organization*, 589.

Olayemi O.J, 'A Socio-Technological Analysis of Cybercrime and Cybersecurity in Nigeria' (2014) (6) (3) *International Journal of Sociology and Anthropology,* 116-125

Orji UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) (1) (2) *Securing CyberSpace,* 203.

Schjølberg S and Ghernaouti-Hélie S 'A global protocol on CyberSecurity and CyberCrime' (2009) (1) (2) *CyberCrimelawS.A journal,* 14.

Sergeant J. 'Police Raid on Global Internet Child Pornography Club' (2006) (1) (1) *Computer Pornography,* 16.

Sharma Ravi, 'Study of the latest trends on Cybersecurity and its challenges to Society' (2012) (3) (6) *International Journal of Scientific and Engineering Research*, 1.

Snail kaMtuze S 'CyberCrime in South Africa: Hacking, cracking and other unlawful online activities' (2009) (1) (2) *Journal of Information, Law and Technology,* 10.

Yang D. and Hoffstadt B., 'Countering the Cyber-Crime Threat' (2006) (43) (2) *American Criminal Law Review,* 34

OTHER SOURCES

Obuh A.O., 'Cybercrime Regulation: The Nigerian situation' Delta State University a project presented to the faculty of law (2010)

WEBSITES

African Union Convention on Cyber Security and Personal Data Protection. Date of adoption 27 June 2014. Date of last signature: 04 July 2017 <https://au.int/en/.../african-union-conventioncyber-security-and-personal-data- protection> accessed 2nd March, 2024

APWG (Anti-Phishing Working Group) (2004) Phishing Activity Trends Report<http://www.antiphishing.org> accessed 2nd March, 2024

APWG (Anti-Phishing Working Group) (2008). *Phishing Activity Trends Report*. <http://www.antiphishing.org> accessed 2nd March, 2024

Archick K., Cybercrime: The Council of Europe Convention<http://www.usembassy.it/pdf/other/RS21208.pdf> accessed 2nd March, 2024

Collin B.C., 'The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge' (2006*) 11th Annual International Symposium on Criminal Justice Issues* <http://www.thefutureofcyberterrorism.com> accessed 2nd March, 2024

Crimes related to computer networks, background paper for the workshop on crimes related to computer networks, *10th UN Conference on the prevention of crimes and the treatment of offenders,* 2000, A/CONF/87/10, <www.uncjin.org/documents/confr10/10e.pdf> accessed 2nd March, 2024

Cybersecurity Agenda / High-Level Experts Group (2008) *Global Strategic Report*, 39 <www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html> accessed 5th March, 2024

David Ashaolu, 'Combatting Cybercrimes in Nigeria' (2011) <https://blogs.law.harvard.edu/mcash/2011/12/27/combating-cybercrimes-in-nigeria-ii/> accessed 2nd March, 2024

Facebook alone claimed some 845 million active users in December 2011. <http://www.facebook.com/press/info.php?statistics> accessed 5thMarch, 2024

Forcepoint, 'What is Malware? Malware defined, explained and explored' (2021) < https://www.forcepoint.com/cyber-edu/malware> accessed 3rd March, 2024

Gordon F., 'the Definition and Classification of Cybercrime' (2005) (2) (1) *Journal in Computer Virology* <www.crimeresearch. org/articles/cybercrime-in-France-overview> accessed 22nd February, 2024

Hoscheidt M.M. and Eichner E.F 'Legal and Political Measures to Address Cybercrime' (2014) <http://www.ufrgs.br.ufrgsmun/2014/files/ws12.pdf> accessed 22nd February, 2024

Kaspersen Henrik., 'Cybercrime and internet jurisdiction Vrrje Universiteit Amsterdam' (2009) (12) Economic crime Division, Directorate General of Human Rights and Legal Affairs <www.coe.int/cybercrime> accessed 24th February, 2024

Kochems A., and Keith L, 'Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft' (2006) <http://www.prevetinvetechnologiesandidentitytheft.html> accessed 24th February, 2024

Ladan M.T, , 'The Effectiveness of Legal and Enforcement Framework in Fighting Advance Fee Fraud and Money Laundering Activities' (2014) A paper presented at the 3rd National Seminar on Economic Crimes <www.dawodu.com/Ladan2.htm> accessed 24th February, 2024

Litan A. 'Phising attack victims likely targets for identity theft' (2004) <http://www.gartner.com/DisplayDocument> accessed 26th February, 2024

Longe O.B and Longe F.A., 'The Nigerian Web Content: Combating the Pornographic Malaise Using Web Filters (2005) (5) (2) *Journal of Information Technology Impact*. <http//: www.jiti.net.> accessed 24th February, 2024

Mamandi K. and Yari, S. 'A Global Perspective on Cybercrimes' (2014) (2) (2), *Humanities and Social Sciences*, <http://article.sciencepublishinggroup.com/pdf/> accessed 25th February, 2024

Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response A Guide for Developing Countries' (2013) <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> accessed 24th February, 2024

NiBusiness, 'Common Cybersecurity measures' (2020) <https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures>

Oxford Dictionaries (2013) < http://oxforddictionaries.com> accessed 24th February, 2024

Phishing Activity Trends, Report for the Month of April 2007,

Science and Technology < www.ejournalofscience.org>. accessed 24th February, 2024

Osborn, H.Q., e tal 'Fighting Cybercrime in Africa' (2012) *Computer science and Engineering Journal* <http://Journalsapub.org/computer.scientific&Academic> accessed 22nd February, 2024

Sophos Security Threat Report 2010 < http://www.sophos.com/security/topic/security-report-.html> accessed 24th February, 2024

Tatera, K. 'Using Artificial Intelligence to Take Down Cyber Criminals' (2015) <http://thescienceexplorer.com/technology/usingartificial_intelligence> accessed 24th February, 2024

The communicator Magazine: <www.ncc.gov.ng/thecommunicator> accessed 24th February, 2024

The WiMAX Forum <www.wimaxforum.org;> accessed 24th February, 2024

UNODC, 'Draft Comprehensive Study on Cybercrime.' (2019) <https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/references.html> accessed 25th February, 2024

Victor. T and Olumide O. 'E-crime in Nigeria; Trends, Tricks and Treatment' (2015) <www.Openj.gate/search/searchresults/articles> accessed 28th February, 2024

WSIS Geneva Plan of Action, (2003) <www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0> accessed 25th February, 2024

WSIS Tunis Agenda for the Information Society, 2005, <www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.> accessed 24th February, 2024