AN ANALYSIS ON THE EFFECTIVENESS OF LAW IN AVERTING CYBERCRIME IN AFRICA: A COMPARATIVE STUDY OF NIGERIA AND UGANDA

ANAZODO CHUKWUEBUKA OGOCHUKWU

AS21B11/248

A DISSERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY

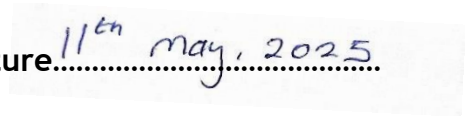
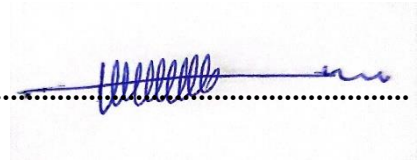
May,2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I ANAZODO CHUKWUEBUKA OGOCHUKWU, do hereby declare that this dissertation was carried out in accordance with the requirement of the University's Regulation and Code of Practice for Research and that it has not been submitted for any other academic award. Other works cited and referred to are accordingly acknowledged.

Signature  .....**Date**  .....

ANAZODO CHUKWUEBUKA

ABSTRACT

As the continent undergoes rapid digitalization, cyber threats remain on the rise. While many countries have enacted cybercrime laws and ratified international conventions, enforcement remains inconsistent due to gaps in legislation, in terms of technical capacity and limited cross-border harmonization. This study examines the strengths and weaknesses of the current cyber legislations in selected African countries, evaluates the role of regional instruments, as well as international instruments in averting cybercrime within Africa. This paper argues that while legal efforts have made progress in establishing foundational protections, the effectiveness of these laws in deterring and prosecuting cybercrime is currently limited.

ACKNOWLEDGEMENT

I thank the Almighty God for granting me the strength, courage, and wisdom to pursue this project. I also acknowledge my supervisor, **Mr. Oscar Boban Owakubariho** for his patience, and careful guidance through the course of writing this dissertation.

Specifically, great appreciation is due to my parents, Sir Engr. Osita Anazodo and Lady Barr. Mrs. Chinelo Anazodo, for the support they gave me in the writing of this dissertation and indeed throughout my degree. I thank Mrs. Chinelo Anazodo-Ogbogu, Engr. Somtochukwu Anazodo, Engr. Chukwuemeka Anazodo and Mr. Chukwuzitelum Anazodo for the constant encouragement they offered.

APPROVAL

I vouch for **ANAZODO CHUKWUEBUKA**, who has carried out the study and authored this report with my guidance.

The report was submitted for assessment with my approval as a university supervisor.

Signature..... **Date**14/05/2025.....

Mr. Oscar Boban Owakubariho **DATE**

SUPERVISOR

TABLE OF CONTENTS

CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The internet is a system architecture that has been in perpetual development for decades now. It is defined as an electronic communications network that connects computer networks and organisational facilities around the world.[1] The development of the internet can be traced back to the sabre in the 1960s, which is still operational till date[2]. At this time, computer systems were only created for a specific purpose, for which the sabre was created as an airline reservation system. The general-purpose networks came into existence in the late 1960s and early 1970s following the creation of the Advanced Research Projects Agency Network (ARPAnet), in 1969. The ARPAnet however was not an open-source service, in that it was limited to a certain category of individuals who had contracts with the defence department.[3] As a result of the nature of ARPAnet, other networks were created to cater for individuals who had no access to the ARPAnet, but wanted information exchange. In the 1970s, Vinton Gray Cerf and Robert Elliot Khan invented a new communication protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). This protocol allowed for different networks to

[1] "Internet." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/Internet. Accessed 17 Dec. 2024.
[2] https://www.sabre.com/
[3] https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,to%20communicate%20with%20each%20other. Accessed 17 Dec. 2024.

communicate with each other. This protocol was adopted by ARPAnet in 1983 which was considered the birth of the internet.

Subsequently, the internet made its way into Africa. In Nigeria, it began with the provision of limited E-mail services in 1991 and in July, 1995, the regional information network of Africa together with rose clayton Nigeria Limited, provided internet services such as; E-mail, telnet and gopher.[4]

The internet arrived Uganda on the 5th of august, 1995 when the first internet service provider, infomail Uganda came online, along with other internet service providers following shortly after.

The evolution of the internet has opened a gateway for various opportunities and innovations throughout the vast fields of study. The internet has also fostered an immense level of accessibility through electronic means in the fields of medicine, banking, governance, education, etc.

Unfortunately, the internet, like any other phenomenon harbours disadvantages, and in this research, the researcher would focus on the criminal aspect of the internet.

One of the main characteristics of the internet is that it grants anonymity to its users. This allows users to operate and transact on the internet without having to reveal their identity. While this anonymity can be beneficial, it is very often used as a cover to commit computer crimes, otherwise known as cybercrimes, on the cyberspace.

The term 'computer crime' is defined as a crime involving the use of a computer, such as sabotaging or stealing electronically stored data.[5]

---

[4] Adomi, E.E. (2005), "Internet development and connectivity in Nigeria", Program: electronic library and information systems, Vol. 39 No. 3

[5] Bryan Garner. 8th Edition Black's law dictionary, page 1120

On the other hand, the term 'cyberspace' is a term that was coined by American-Canadian author, William Gibson in 1982, in his book the Neuromancer. The cyberspace is then defined as the online world of computer networks and especially the internet.[6] In light of the above, Cyberlaw could be said to be the field of law dealing with the internet, encompassing cases, statutes, regulations, and disputes that affect people and businesses interacting through computers.[7]

1.2 STATEMENT OF THE PROBLEM

As a result of the constant evolution of the internet, new methods of committing cybercrimes are constantly discovered, and as a result, the law makers are unable to provide concrete laws to cater for the victims of these cybercrimes.

The Nigeria constitution provides that "the privacy of citizen, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected"[8]. Similarly, the constitution of the republic of Uganda provides that "no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property"[9].

The above provisions, by extension, shows that it is the obligation of the state to ensure that laws are in place to protect these rights, particularly the rights on the cyberspace. African countries have indeed provided laws which prohibit cybercrimes, however, they

[6] "Cyberspace." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyberspace Accessed 17 Dec. 2024.
[7] Bryan Garner. 8th Edition Black's law dictionary, page 1168
[8] Section 37 of the constitution of the Federal Republic of Nigeria, 1999.
[9] Article 27(2) of the constitution of the Republic of Uganda, 1995.

have certain flaws and ambiguity which prevent the protection of the rights of individuals in the cyberspace to be fully realised.

Regardless of the already existent laws, cybercrime remains on the increase. This is as a result of the little to no technological advancement within law enforcement agencies to curb cybercrimes. It also stems from the fact that nearly the whole world operates on an open border system on the cyber space. These raises a question, which this study aims to address, on the effectiveness of the law in averting cybercrimes in Africa.

1.3 PURPOSE AND OBJECTIES

1.3.1 GENERAL OBJECTIVES

This study is going to analyse the efficacy of cyber laws in Africa, using Nigeria and Uganda as case study.

1.3.2 SPECIFIC OBJECTIVES

- To examine the position of common law in averting cybercrimes
- To outline domestic laws in Nigeria and Uganda, aimed at averting cybercrimes
- To examine the effectiveness of the cyber laws in Africa
- To examine the flaws of cyber laws in Africa

1.4 RESEARCH QUESTIONS

- What is position of common law in the prevention of cybercrimes?
- What are the exact laws in Nigeria and Uganda aimed at averting cybercrimes?
- Whether the above laws are effective in averting cybercrimes?

1.5 SCOPE OF THE STUDY

1.5.1 GEOGRAPHICAL SCOPE

This study will cover the Federal republic of Nigeria and the republic of Uganda.

1.5.2 SUBJECT SCOPE

This study is on the legal structure of cyber laws in Africa, including international conventions and regulations, and the laws of Nigeria and Uganda in averting cybercrimes used as a point of reference.

1.6 SIGNIFICANCE AND JUSTIFICATION OF THE STUDY

1.6.1 JUSTIFICATION

The cyberspace has been in constant evolution for decades, and has become an avenue for criminal undertakings, by people who have perfected their understanding of computer. These undertakings typically end up in the victimisation of another internet user.

1.6.2 SIGNIFICANCE

This study will analyse the laws which are aimed at averting crimes in the cyberspace, ascertain its effectiveness to the protection of internet users and the provision of remedies to victims of cybercrimes.

1.7 LITERATURE REVIEW

Various researches have in the past, been conducted on the topic of cyber law, development, as well as its flaws in Africa, specifically Uganda and Nigeria. This will review the researches that has been made by observing the different positions of researchers on the legislations relating to cyber law in both countries, as well as at common law.

Caroline Bongiwe Ncube (2004)[10] argues that many African countries lack comprehensive cybercrime laws, leaving them vulnerable to various forms of cybercrimes, including hacking, data breaches and internet fraud. She further argues that the lack of collaboration between African countries is a key factor making the aversion of cybercrime challenging, stating that African countries need to work together to create harmonized policies, intelligence and cooperate in prosecuting cybercriminals. She underscores the profound role of the internet in fostering economic opportunities, particularly for individuals in developing countries, but also highlights the vulnerabilities that arise without appropriate regulatory framework. Her work is particularly notable as it intersects with broader themes of technological advancement, human rights protection, and the necessity for a robust legal framework.

Dr. Mohammed Chawki & Dr. Ezekiel Uzor Okike (2009)[11] argue that the radical development within the cyberspace, significantly undermines the relationship between the legal framework and physical location. They go on to state that the development

[10] Ncube, Caroline B., Africa Confronts Cyber-Crime (2004). 2004 (2) Speculum Juris 312-317, Available at SSRN: https://ssrn.com/abstract=2758582

[11] Mohammed Chwaki & Ezekiel Uzor Okike, "Fighting Cybercrime: issues for the future", Vol. 1 No.1 African journal of crime and criminal justice 114 – 140 (2009).

within the cyberspace negatively affects the power of the state governments to regulate online behaviour, basing on the geographically unchained nature of the internet. They further argue that cybercrime's potential to morph into new and various form of criminal activities that evade the reach of existing penal law creates challenges for legislations around the world.

Jonathan Clough (2010)[12] argues that the digital environment is a fertile ground for committing crimes, given that the factors necessary for the commission of crime are the supply of motivated offenders, availability of suitable opportunities, and the absence of capable guardians. This poses a major conundrum due to the fact that the cyberspace is in constant evolution and growth, making the availability of the factors necessary for the commission of crimes profuse. He further asserts that the most significant limitation lies in the ability to enforce on the basis of jurisdiction. This is because, in civil actions, the principle of '*forum non conveniens'* applies, however, in criminal actions, it is substantially reduced to a question of who has the defendant in custody?[13]

Marc Goodman and Susan Brenner (2002)[14] opined that within the cyberspace, it is difficult to locate evidence. Hence, even if officers were attuned to the presence of a cybercrime, it would be difficult for them to take it into custody, given that most police agencies around the world are vastly underprepared for this type of investigation. While this position has overtime, seen some developments, a vast majority of African countries remain unable to effectively tackle cybercrimes. They further asserted that

[12] Jonathan Clough, Principles of Cybercrime, page 5.
[13] Ibid., p. 413
[14] The emerging consensus on the criminal conduct in cyberspace, Marc Goodman and Susan Brenner (2002).

in a bid to retain customers, cybercrime victims (specifically companies), refuse to report the matter to authorities, which in the long run, hinders sustainable developments towards the aversion of cybercrimes.

Emmanuel Obidimma and Richard Onyekachi (2023)[15] argue that the success or failure when it comes to the detecting of crime, preventing of crime, apprehension of offenders, investigation of crime and prosecution of offenders, by the law enforcement agencies are dependent on the number of resources available at their disposal. In African countries like Nigeria, investigators often find themselves with their arms tied when it comes to matters dealing with investigation of cybercrimes. This is because addressing cybercrimes require investigators to collect and store data evidence, realisation of which requires a certain extent of financial muscle.

Yee Fen Lim (2002)[16] approached the effectiveness of cyber legislations on an international scale. He classifies the challenges into parts. The first is the substantive international criminal law, wherein he argues that when one country criminalizes high-tech and computer-related crimes and another country's laws does not, cooperation to solve cybercrimes as well as the extradition of the malefactor becomes out of the question. Secondly, multilateral efforts, wherein he states that it is a more effective way to develop international policy and cooperation in averting cybercrimes. The rational for this position stems from the very nature of the internet, consolidated with the fact that there are over 200 countries with access to internet, and criminals can route their connections through any of these countries. Hence, the challenges with

[15] Emmanuel Obidimma and Richard Onyekachi Ishiguzo, Legal and institutional framework for cybercrime investigation and prosecution in Nigeria, Vol. 2 No. 1, International Journal of Comparative Law and Legal Philosophy, (2023).

[16] Cyberspace Law, commentaries and materials, Yee Fen Lim, (2002), p. 273 – 275

enforcement must be addressed on as broad a basis as possible, which could require assistance from any of the countries.

Florence Tushabe and Nyamureeba Venansius (2007)[17] define cybercrimes as crimes that are committed on the cyberspace. In their view, potential victims on the cyberspace are protected by the laws governing the cyberspace as they act as a deterrent to cybercriminals and also, they serve as a means for possible compensation to the victims. They also go on the argue that cybercrime is silent yet common in developing countries like Uganda. This notion is based on Two main reasons. The first is that only few Countries have enacted acts against cybercrimes, and even the ones that have, does not conclusively cover all aspects of cybercrimes. Secondly, obtaining evidence that is admissible before courts is lacking in most countries because they do not have the necessary forensic skills to verify the authenticity of computer evidence, especially due to the fact that computer evidence is easily altered from truth.

Andrea Verteş-Olteanu[18] argues that internet investigation poses a difficulty in its execution because the lot of interconnected computers can transmit data instantly and as such, criminals can delete any and all traces of evidence on the internet before the investigators can lay hands on them. She refers to the internet as the "wild west". This is because it exposes the web users to dangers which are new, difficult to police and difficult to prevent.

[17] Florence Tushabe and Venansius Baryamureeba, Cybercrime in Uganda: Myth or reality? World academy of science, engineering and technology international journal of computer science and systems engineering, Vol. 1 No. 8 (2007) pg. 377 – 381.

[18] Evolution of the criminal legal frameworks for preventing and combating cybercrime, Dr. Andrea Verteş-Olteanu, journal of eastern-European criminal law No. 1 (2014) pg. 84 – 96.

1.8 RESEARCH METHODOLOGY

1.8.1 RESEARCH DESIGN

The research would be approached from a qualitative methodological stand point, in making findings and analysis. Secondary data derived from articles, textbooks, online sources, journals and other pertinent primary data garnered by the researcher.

1.8.2 ETHICAL CONSIDERATIONS

In the perusal of all the data to be used by the researcher, the researcher would, through all phases of the research would be neutral and objective.

All source which will be employed by the researcher would be properly cited and referenced in this research

1.9 CHAPTER SYNOPSIS

The research will highlight the faults and challenges within the legal framework wherein countries like Uganda and Nigeria has found it difficult to avert the occurrence of cybercrimes within their cyberspace. In pursuance of the above, this research will consist of four chapters;

Chapter one introduces the topic, giving a brief history of cybercrimes as well as the internet as a macrocosm of computers. This chapter also answers the question on how and why this research would be carried out as well as addressing ethical consideration which the researcher has observed within the research.

Chapter two looks at the theoretical or non-legal framework which aids this research in review of the flaws within Africa's legal framework the current successes of the cybersecurity within the African cyberspace.

Chapter three observes the different legal frameworks made available in different African countries in a bid to avert cybercrimes, considering their successes as well as the lacunas which they have failed to address.

Chapter four concludes the research, giving a summary of the findings from the research, putting into consideration the already established literature. This chapter is a conclusive part of this research, giving recommendations as to how the cyber legislations could be better equipped or structured to avert cybercrimes.

CHAPTER TWO

2.0 THE NON-LEGAL ASPECTS OF CYBERCRIME

2.1 DEFINITION OF KEY TERMS

2.1.1 CYBERCRIME

Cybercrime, otherwise known as a 'computer crime', entails a crime involving the use of a computer, such as sabotaging or stealing electronically stored data[19]. It is a multifaceted term that entails a wide array of illegal activities associated with computers and the internet, including, but not limited to identity theft, unauthorized access to personal data, illegal publications relating to children among others.

2.1.2 COMPUTER

Section 1 of the computer misuse act defines a computer as an electronic, magnetic, optical, electrochemical or other data processing device or groups of such interconnected devices performing logical, arithmetic or storage functions.[20] In this context, computers are considered to play different roles when it comes to cybercrimes, that is to say;

- Computers can be the tool or instrument of attack, whereby malwares or other software used to perpetuate the desired cybercrime is deployed from.

[19] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 1120.
[20] Computer misuse act Cap. 96

- Computers can also be the target of attack whereby the software of the computer is targeted to make it inoperable or degrade its usability. This also applies in instances wherein the computed is used as a storage device, and data is stolen from it.
- Lastly, computers can be the object of attack in instances wherein hardware components of the computer, or even the computer as a whole, is stolen.

2.1.3 CYBERCRIMINAL

A cybercriminal is a person who commits crime using computers or the internet.[21] These are otherwise known as the perpetrators behind cybercrimes.

2.1.4 CYBERSPACE

The cyberspace is a world of computer networks and especially the internet.[22] It can further be referred to as a virtual interconnected digital environment formed by networks of computers and electronic systems.

2.1.5 CYBERLAW

This Is the field of law dealing with the internet, encompassing cases, statutes, regulations and disputes that affect people and businesses interacting through computers.[23] This is the law relating to internet and computer offences.[24] It can

[21] "Cybercriminal, N." Oxford English Dictionary, Oxford UP: Accessed, 24th April, 2025, https://doi.org/10.1093/OED/1195961306.
[22] "Cyberspace." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyberspace. Accessed 24 Apr. 2025.
[23] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 1168.
[24] "Cyberlaw, N." Oxford English Dictionary, Oxford UP, March 2025, https://doi.org/10.1093/OED/8944188690. Accessed 24th April, 2025.

otherwise be said to be the body of law governing the use of the internet and digital technologies.

2.2 INTRODUCTION

Cybercrime is not just a 21st century phenomenon. It dates as far back as the 19th century, with the first recorded incident being in 1834, before the conception of the internet[25]. This type of crime has become a pressing global issue due to the rapid advancement of information and communication technology, which has exposed vulnerabilities within the cyberspace and attracted malicious actors seeking to exploit these weaknesses. The evolution of society towards an information-centric model has transformed cybercrime into a multifaceted phenomenon with significant implications for daily life, commerce and national security. Cybercrime poses far-reaching consequences which extend beyond financial loss, impacting the victims' emotional well-being and the broader economy. The estimated cost of cybercrimes by 2025 was said to reach 10.5 trillion USD globally[26], and is said to continue to climb, as cybercrime rapidly expands in complexity and scale.

2.3 CHARACTERISTICS OF CYBERCRIME

2.3.1 DYNAMIC

Cybercrime is inherently dynamic, as it is constantly developing and evolving with new technologies and tactics. That is to say cybercrime is not static in nature, but rather a

[25] 'A Brief history of cybercrime' | RedTeam Labs' accessed 24th April, 2025: https://theredteamlabs.com/a-brief-history-of-cybercrime/

[26] 'Cybercrime to cost the world $9.5 trillion USD Annually in 2024 | Cybercrime Magazine accessed 3 April, 2025: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

fluid landscape that requires ongoing adaptation and innovation in prevention of the act and a response for when it is committed. However, due to the speed at which it evolves, cybercrime develops faster than the cyber laws, resulting in cybercrimes which are yet to be regulated. Given that the law does not apply retrospectively, instances are created wherein offenders are able to go unpunished for unacceptable behaviors on the cyberspace as a result of these regulatory lacunas.

2.3.2 TRANSNATIONAL

The internet is a global computer network. Meaning that the use of the internet to commit crimes is an international problem, rather than a domestic one. Technological advancements have effectively eliminated the need for physical proximity to commit crimes. As a result, cyber-attacks can be launched across jurisdictions. This was the case in privacy international v the United Kingdom[27] wherein the applicants who were from different countries (London, Germany and South Korea), sued the United Kingdom secret service on grounds of violation of the computer misuse act for the offence of unauthorized access, carried out through hacking.

2.3.4 PERVASIVE

As the world evolves into a global village, it turns every individual on the cyberspace into a potential victim of cybercrime. This is to the effect that it could occur individually or on a large scale. This was depicted in the MMM Global Ponzi scheme which was launched in 2011 and was popular in African countries like South Africa, Nigeria, Zimbabwe, Kenya and Ghana. Wherein it was estimated that 3 million Nigerians

[27] Privacy International and Others v the United Kingdom, Application No. 46259/16 ECHR (2020)

had lost ₦18 billion in the scheme. On an individual basis, the pervasive nature of cybercrime was illustrated in the Ugandan case of Hesse Brian v Senyonga & Ors[28] wherein the plaintiff had suffered an income loss amounting to $240,000 before it came to his attention that the defendants had been intercepting his financial transactions via hacking.

2.4 CLASSIFICATION OF CYBERCRIME

The forms of cybercrime preface the question, "against whom can cybercrimes be committed?". While it is on a broad spectrum, it can primarily be categorised into three (3) main forms based on the target of offence.

2.4.1 CYBERCRIME AGAINST INDIVIDUALS.

This category encompasses crimes that are directly targeted at private individuals. These crimes are personal in nature, such that it aims at sabotaging or stealing the data or information of a particular person. A common example of this form of cybercrime is defamation, which involves the publication of false statements that causes harm to a person's reputation.

2.4.2 CYBERCRIME AGAINST PROPERTY.

Cybercrime is habitually committed via the internet; therefore, it is implied that the target of these crimes are virtual targets as well. However, cybercrime can also target physical property. Such offenders may engage in tactics such as distributed denial of service (DDoS) which disrupts the function of services such as, internet, online services

[28] Hesse Brian v Senyonga & Ors, Civil Suit No. 612 of [2014] (2015) UGCommC 90.

or computers, depending on the nature of the attack as well as the intent of the offender, forcing it to go offline. Here, internet crimes can also lead to the destruction of hardware components of devices, where viruses are deployed to cripple or make inoperative, components of a computer(s).

2.4.3 CYBERCRIME AGAINST PRIVATE ORGANISATIONS

Cybercrime against organisations can take a number of forms, including but not limited to business email compromise, malware attacks, distributed denial of service (DDoS), amongst others. An example of this is portrayed in the first recorded online bank robbery. It was led by a young Russian programmer named Vladmir Levin, who hacked into the electronic systems of Citibank, a major U.S. bank and began secretly stealing money, amounting to a total sum of $10 million.[29]

2.4.4 CYBERCRIME AGAINST THE GOVERNMENT

Cybercrime against the government entails illegal activities carried out through digital means that specifically target governmental institutions, systems, or data. These crimes pose a threat to national security, public safety and the proper functioning of the state. It is considered an attack on the nation's sovereignty and an act of war. It includes but not limited to, data breaches, cyberterrorism, espionage, cyberwarfare.

[29] 'A Byte out of History: $10 million Hack' | FBI' Accessed 25th April, 2025: https://www.fbi.gov/investigate/cyber/major-cases

2.5 TYPES OF CYBERCRIMES

As discussed earlier, due to the vast and fast-growing nature of the cyberspace, cybercrimes can appear in a countless number of ways, depending on the classification which it falls under. Hence, the most common types of cybercrimes will be discussed below, including but not limited to:

2.5.1 HACKING

This is the act of surreptitiously breaking into a computer, network, servers, or database of another person or organization.[30] It is the illegal access to computers and information stored within, without authorization. It is important to note that while hacking in its self is an offence, it is a different offence to hack as a means to commit another offence or to facilitate the commission of another offence.

2.5.2 DEFAMATION

Defamation is the act of harming the reputation of another by making a false statement to a third person.[31] It is the publication of a statement which tends to lower a person in the estimation of right-thinking members of society generally, or which makes them shun or avoid the victim.[32]Cyber defamation or cyber smearing occurs when the offender informs the third party of the defamatory statement with the help of the internet or a computer.

[30] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 2086.
[31] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 1260.
[32] Percy Henry Winfield | Law of Tort, 5th edition. Pg. 242

In order for one to show that the offence of defamation (cyber) was committed against them, the following elements must be proven;

- That there was an internet publication of a statement
- That there was reference to the plaintiff within the statement
- That the statement was substantially untrue
- That the statement caused actual or presumed damage to the plaintiff

2.5.3 ELECTRONIC FRAUD

Fraud is a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[33] Internet fraud on the other hand involves the deceptive or criminal use of electronic mediums such as computers, mobile devices, or the internet with the intent to gain money, data, or any other benefits unlawfully. In countries like Nigeria, this type of crime is commonly referred to as 'yahoo'.

2.5.4 CYBER SQUATTING

This is the act of reserving a domain name on the internet, specifically which would be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it.[34]

[33] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 1950.
[34] Ibid, pg. 1169.

2.5.5 CYBER STALKING

Cyber stalking is the act of threatening, harassing or annoying someone through multiple e-mail messages, through the internet, specifically with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient's family or household.[35]

2.5.6 CYBER TERRORISM

This is an act of terrorism committed by using a computer to make unlawful attacks and threats of attack against computers, networks, and electronically stored information and actually causing the target to fear or experience harm.[36]

2.5.7 CHILD PORNOGRAPHY

Child pornography entails materials depicting a person under the age of 18 engaged in sexual activity.[37] Thus any activities that involve children in such acts or any materials involving children in such acts are not allowed in Uganda as well as the cybercrime act in Nigeria and any persons involved in such actions stand to be punished.

2.5.8 IDENTITY THEFT

This is the fraudulent use of key pieces of information, such as social security, identity card, licenses, etc., of another person which was obtained illegally. The method commonly used to perpetuate the crime is known a phishing which occurs when an individual is tricked into sending their confidential information commonly by contacting

[35] Ibid.
[36] Ibid, pg. 4605.
[37] Ibid, pg. 3684.

the target via fake websites, email, telephone or SMS, posing as a legitimate institution to get victims to provide vital information.

2.6 CONCLUSION

The aforementioned types of cybercrimes, as well as many others which are still emanating or are peculiar to certain regions and countries have been found to be illegal in countries like Nigeria, Uganda and various other African countries, with cases reaffirming this position.

CHAPTER 3

3.0 LEGAL ASPECTS OF CYBERCRIME IN AFRICA

3.1 INTERNATIONAL LEGAL FRAMEWORK

The international legal framework looks at treaties and conventions which have been held to address the issue of cybercrimes. It is categorized into primary international legal framework and secondary international legal framework. The primary international legal framework focuses on the international conventions which were held specifically for issues relating to cybercrime, which aims to tackle the same directly. On the other hand, the secondary international legal framework looks at conventions which, although were not held to tackle cybercrime directly, still indirectly addresses cybercrime through some articles or provisions within the convention.

3.1.1 Primary International Legal Framework

The council of Europe's Convention on Cybercrime

Otherwise known as the Budapest convention, the council of Europe's convention on cybercrime[38] is the first international treaty which specifically addresses cybercrime. It is a convention open to both member and non-member states to ratify and was passed on the 1st of July, 2004. It recognizes the need for cooperation between state parties to combat cybercrimes and the need to protect legitimate interest in the use and development of new technologies. Being the first of its kind, it provides guidelines for

[38] Council of Europe Treaty Series – No. 185

countries to develop domestic laws against cybercrime and establishes a foundation for international cooperation between parties to the convention.

The Budapest convention is supplemented by two additional protocols which are binding on the state parties to the main convention. The first additional protocol is the 'First additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems'[39] which was entered into force on the 1st of March 2006. It concerns the criminalization of xenophobic and racist propaganda on the cyberspace and the prosecution of offenders.

The second additional protocol is the 'Second additional protocol to the convention on cybercrime on enhanced cooperation and disclosure of electronic evidence'[40], which emphasizes international cooperation achieved by addressing some of the challenges that come with transnational implementation of cyber laws and cyber security. This protocol addressed the issues which comes with accessing electronic evidence from service providers in foreign jurisdictions where law enforcement powers are limited.

United Nations Convention Against Cybercrime

The United Nations convention against cybercrime[41] is the most recent international convention on cybercrime, which took place from 29th July 2024, to 9th August, 2024. Similar to the Budapest convention, the primary purpose of the United Nations convention against cybercrime is to strengthen international cooperation and establish a framework for preventing and combating cybercrime globally. It aims to address the

[39] Council of Europe Treaty Series – No. 189
[40] Ibid. No. 224
[41] A/RES/79/243

perpetual evolution of cybercrime by providing a common set of standards and measures for states to implement.

African Union Convention on Cyber Security and Personal Data Protection

Otherwise referred to as the Malabo convention[42], it is the regional framework that was adopted with the objective of addressing cybercrime and data protection in Africa. The preamble of the convention emphasizes the urgent need to establish a mechanism to address the dangers and risks derived from cybercrimes, and foster the use of computers in a manner that balances respect of privacy and freedoms as well as the development of technological industries of the different member states. It provides for national and international approaches to cyber security under section 1, chapter 3 of the convention. It is also worth mentioning that it provides guidance on preventive measures for cybercrimes that violate the right to privacy through breaches of personal data like hacking and identity theft.

A lot of African states have ratified the convention, with Nigeria being the most recent, ratifying the convention in 2024. While this convention has not been ratified by some African states including Uganda, it still serves a persuasive and influential role in Uganda's laws on cyber security and cybercrime.

3.1.2 Secondary International Legal Framework

Universal Declaration of Human Rights

The universal declaration of human rights (UDHR) is one of the principal human rights legislations recognized internationally. It is an amalgamation of all human rights which

[42] African Union Convention on Cyber Security and Personal Data Protection, 2014

also applies to the cyber space. Human rights must be adhered to on the cyber space as such, the UDHR also applies to the cyber space, however indirectly it may apply. This is because the UDHR is a global standard for human rights which is not limited to the physical space alone. The key rights which are particularly relevant in the context of cyberlaw include:

- Right to Privacy: personal devices and online services collect vast amounts of personal data from a wide array of data subjects, making the protection of the right to privacy very crucial in the cyberspace. This right is provided for under article 12 of the UDHR.
- Freedom of expression: the development of information technologies has bridged physical the gap between individuals and has become essential for the free flow of information. Provided for under article 19 of the UDHR, the right to freedom of expression must be safeguarded to protect users such as activists and journalists to publish unprejudiced information on the cyberspace.
- Right to own property: the right to own property extends to both physical property and property owned virtually. This could include, but not limited to; cryptocurrency, valuable virtual items (Skins, game items, etc.), domain names, etc... this right also extends to intellectual property, wherein there are numerous cases of stolen designs and ideas. It is enshrined in article 17 of the UDHR

General Data Protection Regulation

The general data protection regulation (GDPR), established by the European Union, regulates the collection and processing of personal data of individuals withing that

union. It affords data subjects greater control over their personal data and set rules for organizations collecting and using the data. The GDPR, particularly article 5, serves as a guiding framework in the protection of the privacy of individuals on and offline.

3.2 DOMESTIC LEGAL FRAMEWORK

Much as the penal code is the key punitory legislation in most African states, the novelty of cybercrime within the African cyberspace has necessitated the creation of specialized regulations to police the different aspects of cybercrime as a supplementary to the penal code. These legislations not only provide for the offences and punishments, but also preventive measures that should be put in place in particular organizations and institutions to address cyber-attacks. Some of these legislations include, but are not limited to:

Computer Misuse Act Cap. 96

The computer misuse act is the primary cybercrime legislation in Uganda. the purpose of this act, as stated in its long title is to provide for the safety and security of electronic transaction and information systems, to prevent unlawful access, abuse or misuse of information systems including computers and any related matters therein. To this effect, it defines what amount to the offence in question and sets out rules to ensure that this purpose is achieved. In the Ugandan case of Hesse Brian v Senyonga & ors[43], court relied on section 11 of the computer misuse act to reiterate the illegality of

[43] Hesse Brian v Senyonga & Ors, Civil Suit No. 612 of [2014] (2015) UGCommC 90.

hacking in declaring judgement against the defendant who were accused of hacking the email of an employee of the plaintiff.

The act also provides for methods of investigation and obtaining evidence for any of the offences provided therein. Case in point, section 31 of provides for the procedure to be followed during search and seizure.

Electronic Transactions Act Cap. 99

Complementing the Computer Misuse Act, the Electronic Transactions Act provides legal recognition to electronic transactions and facilitates e-commerce in Uganda. The electronic transactions act provides a legal framework for electronic communications and transaction, aiming to facilitate e-commerce and e-government. It ensures that electronic transactions and paper transactions are treated with equal scrutiny, establishing rules for contract formation, document validity and the admissibility of electronic evidence in court.

Electronic Signatures Act Cap. 98

The electronic signatures act provides a legal framework for the use of electronic signatures, recognizing them as being legally equivalent to handwritten signatures. It ensures the authenticity and security of electronic transactions by recognizing signature creating technologies. It is important to note that the electronic transactions act and the electronic signatures act often work hand in hand to ensure the effectiveness of a regulatory framework for the use, security, facilitation and regulation of electronic communications and transactions as well as the use of electronic signatures.

Data Protection and Privacy Act Cap. 97

The Data Protection and Privacy Act (DPPA) is an essential piece of legislation that underscores the importance of personal data protection. It outlines the rights of individuals concerning their personal information and mandates that data controllers and processors implement adequate security measures to safeguard this data. It protects this right by regulating the collection and processing the personal information off the data subjects. The DPPA finds it’s roots in the General Data Protection Regulation.

Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015

The cybercrimes act is a comprehensive and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. Similar to the Computer misuse act of Uganda, it is the primary cyber legislation in Nigeria. Unlike the Ugandan legal framework, the contents of the electronic transactions act and electronic signatures act and comprised in the cybercrimes act, making it a somewhat conclusive cybercrime legislation.

3.3 CONCLUSION

The above, being the extant domestic laws in Nigeria and Uganda, provide a solid legal framework in the aversion of cybercrime, though subject to change and amendment following the evolution of cybercrimes in the country/continent. The effectiveness of these laws however, would be discussed elaborately in the following chapter.

CHAPTER 4

4.1 FINDINGS AND RECOMMENDATIONS

Cybercrime poses significant threats to national security and economic stability. Having perused the discussed legal frameworks and literatures, various finding and recommendations has been observed and extracted as to the effectiveness of these laws in the aversion of cybercrimes

4.2 SUMMARY OF FINDINGS

Cybercrime is a perpetually escalating issue that affects all nations regardless of their level of development, impacting both businesses and consumers. The dynamic nature of cyber threats and the accompanying skills shortages pose significant challenges for law enforcement and judicial systems, especially concerning cross-border enforcement.

In her work, Caroline Ncube presents a detailed analysis of the multifaceted challenges that Africa face in combatting the threats of cybercrime. She examines the escalating challenges of cybercrime across the African continent with a particular focus on legal, economic and human rights implications. Some of the key insights from her work include:

- **Lack of comprehensive legal frameworks and policies:** According the United Nations Conference on Trade and Development (UNCTAD)[44], only 85% of countries in Africa has enacted legislations in cybercrime, leaving countries like Central

[44] 'Cybercrime Legislation Worldwide' | United Nations Conference on Trade and Development' Accessed on 10th May, 2025: https://unctad.org/page/cybercrime-legislation-worldwide

African Republic (CAR), Somalia and Eritrea without cybercrime legislations. The lack of legislations leaves these countries vulnerable to various forms of cybercrimes.

- **Balancing Security and Privacy:** the tension between ensuring cybersecurity and protecting the right to privacy of individuals is one of the critical challenges raised in her work. She highlights the regulation of interception of communications act, which raised concerns regarding potential infringement of privacy in a bid to protect national security. This leads to an abuse of power wherein journalists, activists, or opposition groups have their privacy over-policed by government agencies acting on the provisions of the legislations.

In their work, Emmanuel Obidimma and Richard Onyekachi outline amongst other things, a variety of challenges facing the effective investigation of cybercrime in Nigeria which to a larger extent similarly applies to a vast majority of African countries. Some of the challenges which the outlined includes:

- **Inadequacy of Legal Framework:** 85% of countries in Africa has enacted cybercrime laws, however, those legislations have proven to either be ineffective or inadequate in the combating of cybercrimes. For instance, in the Ugandan context, the law is silent in regard to cybersquatting and typo squatting. This is the act of reserving a domain name on the internet which would ordinarily be associated with a company's trademark and seeking to profit be selling or licensing the name to a company that has an interest in being identified with

it.[45] This creates an avenue for extortion of business owners who have not registered their trademark on a domain network.

- **Extradition challenge:** A core principle under extradition law is the principle of dual criminality. It requires that a suspect can only be extradited from one country to another id the crime they are accused of in the requesting country is also a crime under the law of the country from which extradition is sought. This poses a challenge because not all countries in Africa have cybercrime legislations, hence creating a lacuna whereby perpetrators can reside in these countries without cybercrime legislations to evade prosecution for their offence. This can also exist in cases wherein the requesting country has a more advanced cyber legislation than the country from which extradition is sought. In that, the crime which the perpetrator is being accused of might not yet be an offence in the country from which extradition is being sought.

4.3 RECOMMENDATIONS

Much as the rapid growth of information technologies has contributed to the growth of cybercrimes, it has also opened up new avenues for growth in Africa, which, if applied correctly, could greatly contribute to the development of legal and institutional frameworks in the eradication of cybercrimes.

[45] Bryan A. Garner and Henry Campbell Black, 'The Black's law dictionary' 8th edition, pg. 1169.

To build a sturdy digital resilience, it is crucial to promote an effective legal framework across the continent. This chapter outlines the key recommendations aimed at strengthening the cyber legal landscape in Africa.

Promoting an effective legal framework in the aversion of cybercrime in Africa involves addressing current gaps in legislation and enforcement. The key recommendations include, but are not limited to:

- **Harmonization of Cyberlaws across borders:** cybercrime is transnational in nature. Meaning that a single cybercrime case can affect victims from different countries. When laws are inconsistent with each other, it hinders prosecution and cooperation. Harmonizing legislations entails creating common legal definitions, procedures, and penalties related to the different types of cybercrimes. This can be facilitated through regional organizations like the African Union, Economic Community of West African States, and the East African Community.

  The African Union already provides a comprehensive legal framework for cybersecurity and data protection through its convention on cyber security ad personal data protection. However, countries like Uganda and a few others have yet to ratify this convention. Ratification and implementation of this convention can significantly contribute to the harmonization of cyberlaws in Africa.
- **Regular Revision of Extant cyber laws:** as cyber threats continue to evolve rapidly with advancements in technology, it is crucial that cyber laws remain current and adaptive to evolution. Revision of Cyber legislation is an essential factor in ensuring the long-term effectiveness of Africa's cyber legal framework. This revision helps to identify and address lacunas and ambiguities in the law

which can potentially be exploited by criminals, or hinder enforcement. This can be achieved by the establishment of a review committee for cyber legislations, which acts as a permanent body of legal experts, cybersecurity professionals and other necessary parties, to monitor cyber trends and recommend legal updates to the extant legislations.

- **Creation of a balance between Privacy and security:** As states work towards building a stronger legal framework for cybersecurity, a major challenge arises in the balancing of individuals' privacy and protection of national security. While it is essential to prevent cybercrimes, overreach in surveillance and data collection can infringe on the fundamental right to privacy of the data subject(s). Hence, it is important for legislators to ensure strong safeguards for the fundamental right to privacy of individuals in the creation of cyber laws.
- **Leverage international cooperation:** Africa is a continent that is comprised mostly of underdeveloped states. Cybercrime often involves actors outside national jurisdictions, sometimes from developed states. By cooperating and engaging internationally and with international organizations like the International Criminal Police Organization, International Telecommunication Union, and Europol's European Cybercrime Centre, African countries can exchange information and good practices, gain access to technical support and funding, or join global treaties which offers practical transnational cooperation.

4.4 CONCLUSION

Rather than being just a policy priority, it is necessary that as African continues its digital transformation, an effective and forward-looking legal framework is established in the aversion of cybercrimes. From harmonizing laws to ratifying necessary conventions, by embracing the above recommendations, African nations can, not only defend against he current and emerging cyber threats but also unlock the full potential of the digital economy, and promote sustainable development across the continent.

Bibliography

BOOKS AND ARTICLES

Adomi, E. E. (2005). Internet development and connectivity in Nigeria. *electronic library and information systems, Vol. 39 No. 3*.

Baryamureeba, F. T. (2007). Cybercrime in Uganda: Myth or reality? . *World academy of science, engineering and technology international journal of computer science and systems engineering, Vol. 1 No. 8*, 377 – 381.

Brenner, M. G. (2002). The emerging consensus on the criminal conduct in cyberspace,.

Bryan A. Garner, H. C. (2004). *The Black's law dictionary, 8th edition.*

Clough, J. (2010). *Principles of Cybercrime.*

Ishiguzo, E. O. (2023). Legal and institutional framework for cybercrime investigation and prosecution in Nigeria. *International Journal of Comparative Law and Legal Philosophy Vol. 2 No. 1.*

Lim, Y. F. (2002). *Cyberspace Law: commentaries and materials.*

Ncube, C. B. (2004). Africa Confronts Cybercrime.

Okike, M. C. (2009). Fighting Cybercrime: issues for the future. *African journal of crime and criminal justice. Vol. 1 No.1*, 114 – 140.

Verteş-Olteanu, D. A. (2014). Evolution of the criminal legal frameworks for preventing and combating cybercrime. *Journal of eastern-European criminal law No. 1*, 84 – 96.

Winfield, P. H. (1955). *Law of Tort, 5th edition.*

INTERNATIONAL INSTRUMENTS

1. African Union Convention on Cyber Security and Personal Data Protection, 2014
2. General Data Protection Regulation, European Union Regulation No. 679, 2016.
3. The council of Europe's Convention on Cybercrime Council of Europe Treaty Series – No. 185
4. United Nations Convention Against Cybercrime A/RES/79/243
5. Universal Declaration of Human Rights

STATUTES REFERRED TO

1. Cybercrimes (prohibition, Prevention, Etc.) Act. 2015.
2. Data Protection and Privacy Act Cap. 97
3. Electronic Signatures Act Cap. 98
4. Electronic Transactions Act Cap. 99
5. The Computer Misuse Act Cap.96

6. The constitution of the Federal Republic of Nigeria, 1999.
7. The constitution of the Republic of Uganda, 1995 Cap. 1

CASE LAW

1. Hesse Brian v Senyonga & Ors, Civil Suit No. 612 of [2014] (2015) UGCommC 90.
2. Privacy International and Others v the United Kingdom, Application No. 46259/16 ECHR (2020)

WEB LINKS

1. “Internet.” Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/Internet. Accessed 17 Dec. 2024.
2. https://www.sabre.com/
3. https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,to%20communicate%20with%20each%20other. Accessed 17 Dec. 2024.
4. “Cyberspace.” Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyberspace Accessed 17 Dec. 2024.
5. “Cybercriminal, N.” Oxford English Dictionary, Oxford UP: Accessed, March 2025, https://doi.org/10.1093/OED/1195961306.
6. “Cyberspace.” Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyberspace. Accessed 24 Apr. 2025.
7. “Cyberlaw, N.” Oxford English Dictionary, Oxford UP, https://doi.org/10.1093/OED/8944188690. Accessed 24th April, 2025.
8. ‘A Brief history of cybercrime’ | RedTeam Labs’ accessed 24th April, 2025: https://theredteamlabs.com/a-brief-history-of-cybercrime/
9. ‘Cybercrime to cost the world $9.5 trillion USD Annually in 2024 | Cybercrime Magazine accessed 3 April, 2025: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
10. ‘A Byte out of History: $10 million Hack’ | FBI’ Accessed 25th April, 2025: https://www.fbi.gov/investigate/cyber/major-cases
11. ‘Cybercrime Legislation Worldwide’ | United Nations Conference on Trade and Development’ Accessed on 10th May, 2025: https://unctad.org/page/cybercrime-legislation-worldwide