A Criminological Investigation into the Lived Experiences of Cybercrime Perpetrators in Southwest Nigeria

By

TOLULOPE LEMBOLA OJOLO

Submitted in fulfillment of the requirements for the degree

Doctor of Philosophy

In

Criminology and Forensic Studies

School of Applied Human Sciences, University of KwaZulu-Natal, Durban, South Africa

Supervisor: Dr Sazelo Mkhize

Co-supervisor: Dr Sogo Angel Olofinbiyi

2020

DECLARATION

I declare that the work contained in this thesis has not been previously submitted for a degree or diploma at any other higher institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person, except where due reference is made.

Signed: ----------

Date: ----------

DEDICATION

I dedicate this study to my beloved mother, Mrs Bosede Yetunde Oluwatayo. Mummy, you have been a source of motivation and joy. You will surely partake of the rewards of your labour of love, in Jesus' Name!

ACKNOWLEDGMENTS

Thanks, and praise to God almighty for His mercy in helping me to accomplish this work.

I would like to express my heartfelt gratitude to the people who helped and encouraged me on this incredible journey. I need to recognise a number of people. To begin with, I believe the first to be appreciated are those who participated in this research, the participants themselves. I want to thank you all for taking the time to participate in this study. Special thanks must go to my supervisors, Dr Sazelo Mkhize and Dr Sogo Olofinbiyi for their guidance, patience, and support, indeed they were of good value in my journey to completing this work.

I would like to acknowledge the untiring support I received from my friends and colleagues during this laborious journey. I would like to express my thanks particularly to Oluwatobi Alabi, for your unending support throughout this academic journey. I also express my gratitude to Dr Paul Bello and Dr Buhari, who was instrumental to the success of this study. Without a doubt my colleagues at the University of KwaZulu-Natal were instrumental throughout this academic journey; among them are Ojako Samson, Smith Philip, Ajimakin Ifedayo, Pelumi Adegbero, Akpan James, Bindela Khanyile, and Dr Adewumi Samson. I further wish to appreciate the spiritual support of Pastor and Dr Wilfred Akinola, for your endless prayers, I thank you. Also, I would like to thank Miss Ayanda Ntuli, my college administrator, for her selfless assistance and support. Further thanks to James Orieneme, Ogene Kewe, Ojolo Temitope, Adigun Ajibola, Agbedun Stella, Akinnola Oluwagbenga, Paul Oluyede, Rene Seaworyeh, Obanijesu Olajide, Agbajeola Omotola Ayomio Fasonranti, Adeyemo Adewumi, Damilola olobaniyi and Mrs Lola Kuton. I want to say a big thank you to you all. Finally, a sincere thanks go to my mother, Bosede Yetunde Oluwatayo and Prof Oluwatayo, Mom and Dad I cannot thank you enough for everything.

T.L Ojolo.

Abstract

Internet fraud, also known as 'yahoo-yahoo', has become very popular in Nigeria, especially among the youth. Adopting a qualitative research design through a phenomenological lens, this study investigates the experiences of cybercrime perpetrators, otherwise known as 'yahoo-boys', in Nigeria. It seeks to understand the factors influencing and sustaining youth involvement in cyber criminality in Nigeria. Painstaking in-depth interviews were conducted with 29 yahoo-boys across three cities in Nigeria namely, Lagos, Ibadan and Ado-Ekiti. The study adopts the arguments of Robert Merton's Strain Theory and Rational Choice Theory as a theoretical framework.

Findings suggest that poverty, unemployment, corrupt political leadership and law enforcement, failure of vital social institutions to meet the needs of most of the population, as well as the proliferation of internet service providers have all merged to create a booming business of cybercrime in Nigeria. Narratives of yahoo-yahoo among the yahoo-boys vary from some admitting that it is a criminal act to others seeing it as an opportunity to escape the harsh socio-economic realities of Nigeria. Some also see it as an avenue for retribution and the redistribution of wealth. Some of these yahoo-boys believe that because most of their victims are based in rich western countries, they are taking revenge for the years of exploitation and oppression Africa has suffered through slavery and colonialism.

Yahoo-yahoo is maintained and sustained through a highly sophisticated network of inter-continental groups of individuals and interests pooling resources together and sharing information and skills with the intent to defraud harmless individuals, business organisations and government parastatals across the globe. They pass on their skills and knowledge to recruits who, most times, consider themselves lucky to be joining the bandwagon through a structured system of apprenticeship and mentorship. The entire network of yahoo-yahoo is built on reliance and collaboration, and more recently has begun exploring elements of the supernatural-spiritualism, to boost the trade. It was brought to the fore that the efforts of the government to curb this illicit trade have been marred by corruption.

Therefore, the study concludes that yahoo-yahoo is an endemic problem in Nigeria that requires a broad, systemic, and multi-level intervention. The proliferation of yahoo-yahoo in the country does not just bring to the fore the consequences of the harsh socio-economic reality Nigerians endure, but its normalisation as an inescapable reality for some young people among various groups of people show the decadence that has pervades in the country's moral norms and

ethical codes. To address the problem there is the need for an attitudinal change. Yahoo-yahoo must be labelled as a crime and not an avenue to escape poverty or get retribution. The government must address unemployment, invest in poverty reduction initiatives, and provide better remuneration across the board. There will be a further need to purge the Nigerian law enforcement agencies of corruption and constantly (re)train its officers on how to handle cybercrime. If initiatives such as sport development programmes and skills acquisition programmes are part of the education curriculum, young people will have the opportunity to develop capacity in other conforming areas of life that could yield a better remuneration in their adult life.

Keywords: Cybercrime, cyber criminality, yahoo-yahoo, yahoo-boys, internet fraud

List of Acronyms

Association of Chief Police Officers (ACPO)

Australian Bankers Association (ABA)

Automated Teller Machine (ATM)

Council of Europe (COE)

Consumer Awareness and Financial Enlightenment Initiative (CAFEi)

Denial of Service Attack (DDoS)

Economic and Financial Crime Commission (EFCC)

Federal Bureau Investigation (FBI)

Federal Trade Commission (FCT)

Information and Communications Technology (ICT)

Information Technology (IT)

International Business Machine (IBM)

Internet Crime Complaints Centre (ICCC)

Nigerian Communications Commission (NCC),

Social Security Number (SSN)

The Centre for Strategic and International Studies (CSIS)

The Department of Defence (DoD)

The Department of Justice in the United States (DOJ)

United States of America (USA)

Very Small Aperture (VSA)

Worldwide Web (www)

Public-Private Partnership (PPP)

Contents

CHAPTER ONE
GENERAL ORIENTATION

1.1 Research Background

Modern technology has pushed the globe to the brink of a new internet era through the help of sophisticated technologies. The combination of connectivity and the accessibility of data presents vast opportunities to advance humanity (Schmidt and Cohen, 2013). However, this revolution has led to the breakdown of conventional borders which have enabled the cyberspace to become a haven for different cybercrimes in the world (Hill and Marion, 2016). Cybercrime has traditionally been described as crimes that occur directly over the internet, but it has increasingly become a synonym for online and computer-based crimes. In Nigeria, for example, the survey communication commission (NCC) survey reveals that broadband extensivity has attained a new height, with 99.05 million internet users in the country (Clement, 2019). This figure is projected to grow to 131.7 million internet users in 2023. Based on this survey, the country is considered a growing digital market where infrastructure and online usage development are growing extensively (Clement, 2019).

The more advanced technology has become, the more cybercrime has grown into a sophisticated art. Cyber-criminal, through computers and other technological devices, illicitly perpetrate crimes against individuals, institutions, or organisations to amass wealth (Wall, 2007). Cybercrime is an overarching issue which has transcended geographical precincts, its development, and modes of operation have evolved overtime (Britz, 2009). While the term cybercrime does not have clear definition, Cassim (2010) regards cybercrimes mainly as, "crimes committed on the internet through the use of computer, the computer can as well represent an object or subject of the crime". Cassim claims a realistic perspective by describing a "computer being the object for the crime to be carried out when there is theft of software and hardware. The subjective perspective is that computers are been used for conventional crimes such hacking, financial fraud and extortion". The menace of cybercrime is an intractable global

epidemic, with an annual increase of up to 30 per cent since the 1990s (World Youth Survey, cited in Sherlyn, 2013).

In Nigeria, 'yahoo-yahoo' has been used to describe cybercrime. Over the years this phenomenon has developed into a popular culture among the youth. Cybercrime in Nigeria has been regarded as a significant social issue, causing a threat to many countries across the world. As reported, Nigeria is ranked as the country with the third highest rate of cybercrime (Tade and Aliyu, 2013; Adesina, 2013; Lazarus, 2019). The repercussions are not only tarnishing the reputation of the country but have also deprived many innocent Nigerians opportunities in the international community. This is accompanied by the negative impacts on the economy as investors are wary of the fallen victims of the atrocities committed by cybercriminals.

From the above, the social conditions instrumental to the enormous involvement of the youth in 'yahoo-yahoo' should be prioritised. It is important to examine the reason behind this dysfunctional innovation if there is to be a lasting solution to curb the phenomenon. In fact, it has always been difficult to determine the root cause of cybercrime, because perpetrators are motivated by different reasons. However, literature suggests that non-functioning systems and a lack of social economic opportunities have led to high unemployment and poverty, which are factors that contribute to the wide spread of 'yahoo-yahoo' in Nigeria. (Ibrahim, 2019, Monsurat, 2020). Conversely, Chaba (2012) affirms that the youth often get involved in cybercrime as a means of survival. Equally, Yosi (2015) criticises the federal government for the prevalence of 'yahoo-yahoo' among the youth because of rampant unemployment, unequal dissemination of national resources, and dilapidated social structures. With this background, this study seeks to explore the lived experiences of cybercrime perpetrators, in an attempt to understand the key narratives in the 'yahoo-yahoo' enterprise, the predisposing factors, and to

examine the link between their experiences and the ineffectiveness of strategies put in place by the government to combat cybercrime in Nigeria.

1.2 Statement of the Problem

Cybercrime continues to be a major global threat. The advent of a graphical interface, World Wide Web (www), in the 1990's contributed to the tremendous growth in the number of internet users, and with this invention came embryonic challenges in the cyber community (Adomi, 2005). The fact is, as computer-based technology, particularly the internet, created more advanced functions, the number of cybercrime perpetrators and victims has increased (Vandebosch and Van Cleemput, 2009). The majority of the youth are involved in 'yahoo-yahoo' because of the technological development and social pathology in the country. To the extent that the practice of 'yahoo-yahoo' has become a popular youth culture. The phenomenon has metamorphosed from a highly reprehensible act into a subliminally welcomed practice. 'Yahoo-yahoo' (cybercrime) no longer attracts serious condemnation, instead it is being encouraged. Surprisingly, some parents subtly encourage their children to engage in these fraudulent activities (Tade and Aliyu, 2011; Ojedokun, 2012). Cybercrime is a cancer in Nigeria's social fabric which has metastasised to different age groups. According to Olaide and Adewole (2004), a large number of 'yahoo-yahoo' boys in Nigeria fall within the age bracket of 18 to 30 years of age and this population of cybercrime perpetrators continues to increase as technology advances and the prospect of such fraud increases.

The issue of cyber-related crime has raised series of fundamental questions among stakeholders in Nigeria, but despite the recognition of cybercrime as a proven youth crime, curbing it has been a difficult task. It is conceived that today urban youths want to live comfortable lives without necessarily engaging in physical work. Defrauding others through the internet has become a paramount means of survival (Ojedokun and Eraye, 2012). As success has become predicated on wealth acquisition in the Nigerian society, the entire populace is constantly

reminded of a need to be financially buoyant to be regarded as a successful, responsible, and impactful member of the society. However, society has failed to compensate diligent hard work. So, the majority are confronted with little or no opportunity to achieve success through a legal means, thus, they innovate (Tade and Aliyu, 2011; Okeshola and Adeta, 2013).

With an increased understanding of cybercriminals' perspectives, stakeholders in society can incorporate the knowledge gleaned from this study into social policies to serve as proactive measures that can help address the cybercrime problem at its budding stage rather than wait for youth to be involved in cybercrime, by which time reactionary measures would be less than useless. A key step to unravelling this criminological puzzle of cybercrime is to explore the lived experiences of the perpetrators to find out the circumstances that got them involved in this dysfunctional behaviour for lessons to be deduced. In light of the nauseating problems of cybercrime in Nigeria, which are most prominent among the youth, scholars and concerned citizens have attributed the menace to various factors, such as peer pressure, family instability, and greed, to name a few (Nwankwo *et al*., 2010). While recognising these causes, this study seeks to focus on the effect of poverty and unemployment on the prevalence of cybercrime among the Nigerian youth.

Also, this study explores the lived experiences of cybercrime perpetrators in Nigeria; it unveils information from the participants' perspectives and sources in-depth information about the circumstances that have driven them into cybercrime. Also, the study unpacks the socio-economic attributes responsible for cybercrime, the foundational factors responsible for participation in cybercrime, and the various techniques, strategies, and measures adopted by cyber perpetrators to sustain their network. This, in the researcher's opinion, is useful in the policy direction of the country regarding cybercrime, and it will consequently serve as a way of updating literature on the phenomenon in Nigeria.

1.3 Aim and Objectives of the Study

The study aims to explore cybercrime, the social and economic impact of the phenomenon in Nigeria, and the instrumentation of socio-economic factors to the involvement in cybercrime through the lived experiences of cyber criminals. The study adopts the use of a qualitative method of data analysis. The major focus is to generate secondary data from a qualitative stance. The study is mainly focused on youths, as the youth are the most susceptible to this form of crime. In light of this, the following research aims were constructed:

i. To examine the perceived circumstances which led some Nigerian youths to be involved in cybercrime.
ii. To explore the key narrative of cybercrime perpetrators and their activities in relation to cybercrime in Nigeria.
iii. To examine links between the lived experiences of cybercrime perpetrators and the ineffective strategies developed by the government to combat cybercrime.

Based on the above objectives, the following research questions were advanced to provide answers to the study's research problem.

i. What are the perceived circumstances which led some Nigerian youth to become involved in cybercrime?
ii. What are the key narratives among cybercrime perpetrators and their activities in relation to cybercrime in Nigeria?
iii. What are the links between the lived experiences of cybercrime perpetrators and the ineffective strategies developed by the government to combat cybercrime?

1.4 Significance of the Study

The aim of this study is to provide useful insight into the discourse of cybercrime in Nigeria. The prevalence of cybercrime activities in Nigeria among other things have been sustained by the anonymity of the internet and a booming socio-economic condition of unemployment

(youth specifically) and poverty in Nigeria. Over the last decade, the activities of cybercriminals have bloomed in Nigeria with several reports of international cybercrime syndicates activities traced to the country. The remedies deployed top curb cybercriminality in Nigeria has not been able to curb the spread of the activity in the country. Though, many studies have been conducted on cybercrime in its varying forms especially the various ways it adapts to technological innovation; the motivation of cybercrime; and the various ways in which poverty, unemployment and weakening socio-cultural bonds intersect to predispose young people to cybercrime in Nigeria (Tade and Aliyu, 2011; Ojedokun and Eraye, 2012; Tade, 2013), not very many studies have explored the lived experiences of cybercriminals- yahoo-yahoo. As a study designed to explore the lived experiences of cybercrime perpetrators, this study brings to the fore a narrative of cybercrime that is foregrounded in the experiences of perpetuators in Nigeria. It leverages on these narratives to present a nuanced understanding of the factors promulgating youth involvement cybercrime in Nigeria. As the scourge of cybercrime continue to increase in Nigeria and the usual idea that it is only targeted at individuals and business in the global north continue to fade as a result of the incessant attacks on financial institutions, corporations, government agencies, and private individuals in Nigeria, it has become more crucial to explore the narratives of perpetuators. It is reported that commercial banks in Nigeria suffered (US$39 million) as a result of electronic fraud and cybercrime, a percentage of these victims are residents in Nigeria (Ogbonnaya, 2019). The Consumer Awareness and Financial Enlightenment Initiative (CAFEi) of Nigeria estimates that cybercrime will cause a $6 trillion damage by 2030, both within and beyond the country. Another fundamental gap in the debate of cybercrime is that it does not take into consideration gender differences. Part of the objectives of this study examined the gender dynamics in the perpetration of cybercrime in Nigeria; it specifically brings into focus the activities of women in yahoo-yahoo.

While efforts are channelled at understanding the socio-economic influences shaping the nature, spate, and dynamics of cybercrime in Nigeria, this study will provide useful insights into the debate. The study benefitted from the multiplicity of subjective narratives shared by participants to explain the motivations and sustaining influences of cybercrime in Nigeria.

1.5 Conceptual explanations

The concepts discussed below are operationalised to provide a succinct description of how they are deployed in this study to explore cybercrime. This will undoubtedly assist the reader in developing a clearer picture of the concepts and how they are used in this study.

1.5.1 Socio-economic context

The term 'socio economic context', also widely referred to as 'socio-economic status'(SES) is a construct that combines multiple aspects, that is broadly characterised by family and the number of economic resources and hierarchy power they have. The American Psychological Association (APA) defines socioeconomic status as "the social standing or class of an individual or group" (APA 2018). In essence, the usage of this term brings into context various socio-economic factors that are peculiar to a group. Socio-economic factors are "the sectors of an individual's activities and understandings that shape an individual as an economically active person" (ILO, 1990:44).

This study understands socio-economic factors as indispensable catalyst responsible for the dynamism of cybercrime (yahoo-yahoo) and its sophisticated activities in Nigeria. In this context, the study refers to poverty, inflation, unemployment, bad governance as a result of leadership deficit and failure, non-fulfilment of social contract as regards the provision of basic amenities to the citizenry by the political state, corruption, greed, political deceit, and injustice as sprout of cybercrime and other related crimes in Nigeria.

Understanding relevant socio-economic factors provides a unique lens through which the issue of cybercrime (yahoo-yahoo) can be examined and comprehended to its fullest extent in this dissertation. There is a close relationship between people's relative standard of living or wealth and their social status or social position relative to other members of society, which is determined by their income, employment status, education, religion, and cultural practices.

1.5.2 Globalisation

There have been a number of competing arguments raised in the social science literature regarding the precise definition of globalisation. The term "globalisation" has a wide range of connotations, and as a result, there does not appear to be a single, globally agreed definition of the concept currently. For example, the concept is broad, and its understanding and meanings differs across disciplines. Inherently, arriving at a common and universally accepted definition appears impossible; however, the various meanings and definitions that have been ascribed to the concept needs more nuance, particularly in explaining how the numerous changes that the world has witnessed in terms of technological, social, political, cultural, and economic advancements shapes human life and experiences in a micro level.

Consequently, globalisation is a conceptual approximation of a description of technological, economic, political, and cultural processes that have accomplished the goal of making the global community of humanity more compact, intimately interrelated, and interdependent. Accordingly, the concept of globalisation has piqued the interest of researchers from a wide range of disciplines who are attempting to explain its form, character, and impact on the world.

In the same way that crime is a general term used to describe a range of various forms of offenses ranging from innocuous offences, such as littering, to the relatively serious offence, such as armed robbery and murder, globalisation is a term used to describe a variety of distinct processes. As defined by Das (2010), globalisation is the pooling together of a network of links

spanning several geographical distances, bringing them together in terms of economics, social interactions, cultural exchanges, and technical advancement. This concept outlines the dismantling of obstacles between countries and continents in order to facilitate the free flow of economic transactions across borders. Thus, with the introduction of globalisation, the constraints that formerly existed between individuals and corporate organizations are now being alleviated in order to facilitate effective economic transactions. According to Fazlul, Mohammed, and Faud (2010), globalisation is defined as the general outlook of connection among countries as a result of the increased flow of products and services; the spread and openness of political boundaries; and the unfettered mobility of labor. For Nayef and Gerard (2006), globalisation encompasses a wide range of challenges, including the integration of economies, the transfer of policies and expertise, and the growth of a flexible economy across the globe. In order to capture the implications of globalisation in a way that is appropriate for this study, this study operationalises globalisation as interconnectedness and interrelatedness of resources, skills and skillset across countries and continent for unlimited opportunities and profit. Globalisation has created a new market for illicit operations, allowing cybercriminals to establish a strong network and open the door to new opportunities for more transnational crimes (see Chapter Two for a discussion on this discourse).

1.5.3 Cybercrime

Cybercrime is colloquially defined as crimes committed on the internet using the computer as either a tool or a targeted victim. The phrases "computer crime" and "cybercrime" are used to describe cybercrime in literatures and publications. It is necessary to establish the relationship between cybercrime and other cyber-related crimes before other conceptual explanations. When compared to other computer-related crimes, “cybercrime" has a more specific connotation because it requires the use of computer network. Computer-related crimes, on the other hand, are crimes that have no connection to a network and simply have an impact on

stand-alone computers. During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed; “Computer crime” is defined as any illicit action directed by means of electronic operations that is directed against the security of computer systems and the data processed by them (Kaur, 2016). Conversely, cybercrime is defined as any criminal acts committed by means of, or in relation to, a computer system or network, which includes such crimes as illegal possession, offering or distributing information through the use of a computer system or network. There is also a widely accepted definition of cybercrime, which classifies it as any action in which computers or networks are used as a tool, a target, or a location for illegal behaviour (Donalds and Osei-Bryson, 2019).

The following are examples of other definitions that attempt to take objectives or intentions into consideration and define cybercrime more precisely, such as computer-related activities that are either illegal or considered illicit by certain parties and that can be conducted through global electronic networks (Friis, and Ringsmose, 2016). This definition thus excludes cases in which physical hardware is used to commit regular crime, but it runs the risk of excluding crimes that are classified as cybercrime under international treaties such as the Commonwealth Model Law on Computer and Computer-Related Crime or the Council of Europe Convention on Cyber Crime (Cybercrime Convention). As a result, the large variety of ways demonstrates that it is extremely difficult to define terms such as "computer crime" and "cybercrime." Because computer crimes can manifest themselves in a variety of ways, there is no single criterion that could encompass all of the behaviours outlined in the many legal methods to addressing the issue. One of the biggest issues in cybercrime research is the lack of common definition across law enforcement agencies who are involved in combatting it. For the Federal Bureau of investigation (FBI), cybercrime covers varieties of scenario including crimes against children (generally involved in child pornography or child rape), the theft of intellectual properties and/or publications, phishing, and intentional malware or spam sent to both domestic

and international networks for monetary gain. When it comes to defining cybercrime, Casey opined that every crime that includes computers and networks is seen to be a crime that uses the internet, which includes offenses that do not primarily rely on the internet (Casey, 2014).

For Thomas and Loader (2013, p.3) cyber-crime as "any computer-mediated activity that is illegal or illegitimate according to certain parties and that can be done across worldwide electronic networks". Nevertheless, the classification of cybercrimes is rather a tough proposition, as they defy attempts to be placed into different categories. Cybercrime can take on many different forms, and it can occur at any time or location. Cybercrime perpetrators have numerous tools at their disposal, dependent on their abilities and objectives. Regardless of whether one's objectives are honourable or malicious, every type of cybercrime involves a set of specialized skills, knowledge, resources, and access to various kinds of data or information systems. Cybercrime has traditionally been described as crimes that occur directly over the internet, but it has increasingly become a synonym for online and computer-based crimes. In Nigeria context, much has been published about cybercrime and around the world and the emergence of the phenomenon in Nigeria over the last two decades through the electronic gullet of academic scholars. In the local sense of Nigeria, this phenomenon is generally called 'yahoo-yahoo'. Nigeria is recognised as one of the world's largest cybercrime spots, owing to the widespread threat of the menace (Ibrahim, 2019).

1.5.4 History of the term yahoo-yahoo in Nigeria

Much has been published about cybercrime around the world and the emergence of the phenomenon in Nigeria over the last two decades through the electronic gullet of academic scholars (Tade and Aliyu, 2011; Okeshola and Adeta, 2013). In the local sense of Nigeria, this phenomenon is generally called 'yahoo-yahoo'. Nigeria is recognised as one of the world's largest cybercrime spots, owing to the widespread threat of the menace (Ibrahim, 2019). At the dawn of Nigeria's democratisation in 1999, internet access through mobile phones dominated

a large part of society, with approximately 350,000 subscribers, which, by 2013, grew to about 120 million subscribers (Doppelmayr, 2013). At this time the global market leader was an internet corporation called Yahoo, which offered different services such as an email address as well as functioning as a search engine. Yahoo held its dominant position in Nigeria as a service provider for years, leading to the name being used as slang to describe internet fraud (Doppelmayr, 2013).

However, the advent of this invention has advanced the technological landscape in Nigeria, has brought about social vices, and given rise to an enormous plague of cybercrime, popularly known as 'yahoo-yahoo'. Due to the internet being popularly named 'yahoo' when it was launched Nigeria, the youth were immediately labelled 'yahoo-yahoo boys', since boys were involved in various internet-based activities at that time (Tade and Aliyu, 2011; Tade, 2013; Doppelmayr, 2013). Sadly, current social and economic trends have left young people with a sour taste, particularly those with poor social and economic backgrounds. This societal lacuna has contributed to the immense growth of 'yahoo-yahoo', as this phenomenon is rooted into all levels of society.

1.5.6 Youth

Young people serve as a bellwether for the future of any nation. Therefore, it is imperative that youth are actively participating in the development of the country by fulfilling contributory obligations for the establishment of sustainable and resilient communities. The phrase "youth" can relate to someone young, or the quality of being young. A youth, according to the National Youth Policy of 2009, refers to any person between the ages of 18 and 35 who lives within the constraints of Nigerian society (te Lintelo, 2012). In this regard, Oputeh (2015), opines that any nation that denies its youth the required enabling environment to participate in nation building processes is doing so at their own peril. This is because youth serve as the foundation

of any society. Their energies, resources, character, and orientation determine the rate at which a nation develops and maintains its security. A nation's economic development and socio-political advancement are propelled forward by the collective efforts of its citizens' creative abilities and labor (Onyekpe, 2007). Indeed, a nation finds inspiration and power in the dreams, hopes, and energies of its young people.

To capture the role of youth in the fitting sense of this study, Nigerian youths have been described as been imaginative, diligent, and resourceful among many other positive characteristics. However, it is regrettable that, in the current Nigeria economic state one cannot make same argument without running the risk of being accused of making sweeping generalisation. The insatiable desire for survival has led in a massive increase in the engagement of Nigerian youth in cybercrime, which growing tremendously. Young individuals between the ages of 18 and 30 are anticipated to make up most of the population in Nigeria who are involved in cybercrime, which is a growing problem (Tade and Aliyu, 2011). This is not to indicate that other age groups are not participating, but most of the perpetuators fall into this age range. Because of this high level of fraud, Nigeria has risen to the position of being the most internet fraudulent country in Africa, while also occupying the third largest control in the world, after China and the United States of America, where the world records the highest number of cybercrimes, according to the United Nations (Tade and Aliyu, 201; Sulieman, 2019).

1.6 Overview of the Chapters

An overview of the structure of this thesis is as follows. This chapter consists of seven chapters. Each chapter discusses different issues, although they are not completely different from each other as all of them are related towards addressing the research problems. This chapter presents the key concept of the study by introducing the research topic, the research problems, and the research objectives, as well as the rationale for the study which is accurately discussed by

explicitly stating its importance to the research. Equally, this chapter contributes to existing knowledge in the broad field of criminology and, especially, towards a tenacious global issue like cybercrime and other related disciplines. Further, this chapter outlines the research questions, significance of the study, and how it progresses in achieving the objectives.

Chapter Two: This chapters focuses on introducing the purpose of this study for which relevant literature was sourced and discussed. First, the chapter critically reviews existing studies and the conceptual framework used in explaining the subject matter.

Chapter Three: This chapter explains the relevant theoretical framework adopted in the study. This chapter also offers a theoretical framework for the study by highlighting appropriate theoretical models which serve as a blueprint for a better investigation, explanation, and understanding of the phenomenon. These theoretical insights contribute to examining why the youth participate in criminal activities online. Strain and rational choice theories see delinquency as a consequence of a mechanism of deliberate reasoning and decision-making by individual entities. Therefore, these theories provide rich arguments to further understand cybercrime perpetrators and the predisposing factors to deviance in society.

Chapter Four: This chapter's aim is to explain the methodological strategy employed in the conducting of this study. This chapter describes different strands of research philosophies, the research design, and the choice of the study's location is justified. Further, this chapter discusses the various steps that were taken in generating and analysing the qualitative data. The following approach systematically addresses the research objective. This chapter also involves a detailed discussion about the ethical consequences of the study, in particular the identity of participants, privacy, and informed consent, which was dealt with during the selection process, data collection, and the data analysis process. The chapter ends with a summary of the youth in the social world.

Chapter Five: This chapter centres on the presentation, analysis, and interpretation of the data that were generated during the fieldwork phase of this research.

Chapter Six: This chapter addresses the findings that emerged from the identified themes for comparative and reflective purposes.

Chapter Seven: This chapter concludes the journey of this thesis. This chapter presents the summary of findings, conclusion, and recommendations. In addition, specific recommendations were suggested for the sake of policymakers for intervention programs that will empower the youth based on the research findings that were formulated. Lastly, future suggestions for further studies are presented in this chapter.

CHAPTER TWO
LITERATURE REVIEW

2.1. Introduction

Given the relevance of the internet in our daily lives and the impact it has on the practices that define contemporary ways of life, connectivity has become a commonplace. In contrast, the same characteristics that have helped to ensure that the internet has been successful are also criminogenic, leading to the emergence of new crimes that are facilitated or intensified by technological advances, which are referred to as cybercrime in this context. Cybercrimes have become more understood as a result of several studies conducted over the last two decades. As a result, the need to unearth, summarize, and synthesize scholarly debates on the discourse of cybercrime from a global perspective and within the framework of developing countries, which includes Sub-Saharan Africa, where cyber threat is a major concern, is fundamental to this chapter. There is no doubt that conducting a literature review exercise is a crucial component of the research process, one that makes important contributions to the complete research procedure (Kumar, 2012). As a matter of fact, it provides the researcher with critical information regarding the issues under consideration (Welman, Kruger, and Mitchell, 2005), and it also acts as a road map to the discovery of new knowledge by identifying current gaps in the corpus of existing knowledge on a topic under investigation (Collins and Hussey, 2013).

The impact of Information and Communication Technology (ICT) on human development is well documented and apparent. ICT has been integrated into the different economies of the world through the aid of electronics and internet connectivity (Hameed, 2007). Many corporate organisations, including banks, now depend on ICT and computer networks to perform basic as well as complex tasks (Hameed, 2007). Cybercrime is no doubt a deep-rooted phenomenon with a long history. However, the proliferation of the internet has indeed come with an unintended consequence, as a haven for criminals. A plethora of studies have investigated the phenomenon and concluded it is a serious global phenomenon affecting many societies

(Brenner, 2008:19; Adeniran, 2008; Shinder, 2002; Broadhurst *et al*., 2013; Tade and Aliyu, 2011).

Examining the cybercrime phenomenon, observable facts are abundant on the coverage of this crime, with a vast number of reports retaining the phenomenon's image as a global occurrence (Broadhurst *et al*., 2013). Although these reports differ across countries, regions, and continents, a majority of them tend to have similar views, especially regarding their root causes and motivations, for what seems to be an endless phenomenon. The issue of cybercriminal activities has been a global threat for decades. As a result, many issues related to these problems were raised and addressed by the published works of eminent scholars. In this context, international studies on cybercriminal research revealed many reasons why this trend continues to persist across the world, especially in Nigeria, despite many attempts to put an end to the menace (Hopkins and Dehghantanha, 2015; Broadhurst, 2006). In a quest to shed light on the findings of the different studies on the topic, the findings from previous research studies are subdivided into the following sections. This chapter begins by exploring the global perspective and definitions of cybercrime; the stages and development of cybercrime; the global statistics on cybercrime and their implications; the common typologies of cybercrime; perspectives on cybercrime in Africa; the self-crusading financial reparation agenda for prolonged slavery and colonialism of Africa; cybercrime being rife in West Africa, using Nigeria and Ghana as case studies; the extent of cybercrime in Nigeria; understanding how cybercrime has morphed from computer-based fraud to include fetish-based spiritual sacrifices: The tale of Yahoo plus in Nigeria; legislation on cybercrime in Nigeria; the challenges that cybercrime presents for criminal justice systems and criminological explanations; the challenges faced by criminal justice systems and the police in combating cyber-crime in Nigeria; legal, policing, and political challenges to tackling cybercrime in Nigeria; approaches for policing and combating internet fraud in Nigeria.

2.1.1 Perspectives and Definitions of Cybercrime

A definition for cybercrime is essential to describe the significance of the subject of the study and to discern it from other forms of crime. A definition for cybercrime will help to identify the most suitable terminology to be used in explaining the phenomenon; for example, computer-related crimes, computer abuse, digital crimes, cybercrime itself, and other related terms. Recognising a particular term for criminal activities in the cyberspace will empower the differences and, by extension, the identification of cybercrimes. According to Maghaireh (2009), diversified global issues impede on a consensus definition of contentious phenomena such as cultural, economic, political, and religious issues, all of which conspire to obstruct approved definitions. In the early periods of the new millennium, it was difficult to develop approved definitions for certain social phenomena. A typical example during this period is terrorism, even though scholarly definitions were presented and put forward, the international community could not reach an approved definition for this social nuisance. In the same vein, cybercrime during this era was considered a new phenomenon compared to other global crimes, with no conclusive or uniform definition. Although, cybercrime has been referred to as network crime for some time, especially due to the internet, but this term has become largely synonymous with computer crimes (Maghaireh, 2009).

Cybercrime has been defined and viewed from different perspectives by scholars and experts. As an example, Don Parker, the first national expert on computer security in the United States, described any, “illegal activity perpetrated using the cyberspace as computer abuse, instead of the generic terminology computer crime”. Parker simply defines computer abuse as, “any intentional act in which one or more victims suffered or could have suffered a loss, and one or more perpetrators made or could have made a profit” (Parker, 1976:59). Also, the United Nations Office on Drugs and Crime (2005) defines cybercrime as an activity involving the use of digital technologies in the commission of the offence; it is aimed at computing and

communications systems and includes the accidental use of computers within other crimes committed. Also, the United Kingdom Association of Chief Police Officers (ACPO) depicts e-crime as the "use of networked computer, telephony or internet technology to commit or facilitate the commission of a crime", which is in line with the original, network-specific, origin of the term cybercrime. Cybercrime can be considered as a computer-mediated practice that some parties find illegal or unlawful and can be carried out through international digital networks (Thomas and Loader, 2000). As such, cybercrime is a crime committed through the use of computer systems. Similarly, the Australian Bankers Association (ABA) delineates cybercrime as, "any crime effected or progressed using a public or private telecommunications service". The Department of Justice in the United States (DOJ, 1989) identifies computer crime as any, "criminal law offences involving computer technology expertise for their perpetration, investigation, or prosecution". From a sociological point of view, Cohen and Felson (1979) argue that, under unprotected circumstances, "Cybercrime is a crime of opportunity committed against a potential victim by a motivated perpetrator". Cybercrime is different from other types of crime (Emanuelsson-Korsell and Soderman, 2001).

Further, the Symantec Corporation evaluates cybercrime from a broader perspective. Accordingly, cybercrime is, "any crime that is committed using a computer or network or hard device". This definition is broad because it does not only include crimes that use or threaten computer systems and networks but also crimes that occur on a stand-alone unit. Recently, cybercrime has been classified as a transnational crime because of the new dimension that has to encompass illegal activities; hence, cybercrime has been defined differently by numerous constitutions across the world. For instance, under the cybercrime Act 2001 of Australia, cybercrime is referred to, "as crimes that target computer data and system" (Katyal, 2001:1007). While, the USA Department of Justice, Computer Crime, and Intellectual Property Section, submits that it is irrelevant if cybercrime is identified as 'new' crime or 'old' as it

creates a unique problem for law enforcement and a concomitant threat to the welfare of the public. Equally, the council of Europe's (COE) Convention on cybercrime describes the act as, "an offence against integrity, confidentiality and availability of computer systems and data, computer-related offences, content-related offences, and offences related to violation of copyrights and related rights". The Nigerian criminal code Act states that,

> "any person who by means of any fraudulent trick or device obtains from any person anything capable of being stolen, or to pay or deliver to any person any money or goods or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour and is liable to imprisonment for two years. This offence is also known as an offence of cheating".

Flowing from above, it is obvious that there are different approaches through which cybercrime has been conceptualised by different countries and organisation. This research sheds lights on the different forms of computer-related crimes and utilitarian crimes applicable to the study, which are characteristically related to economic gain, such as online fraud. As found in pieces of literature, cybercrime suggests personal gain as a major catalyst for continuous perpetration of the crime. As the phenomenon has evolved, different perspectives and new definitions were generated by different scholars to describe the long-standing menace. Although, the centre of the inventive definition on the knowledge of computer technologies is that to commit computer-related crimes is the only prerequisite. The motivation for committing cybercrime offences vary, as motivation is multifaceted and can include factors such as social influences, unemployment, or poverty. Based on existing findings in literature, this study assumes that financial gain, or more generally, personal achievement is a major justification for the persistent activities of cybercrime across the globe, and in Nigeria in particular, although other motivating factors are not exempt (Parker, 1976:59; Olugbodi, 2010; Okeshola and Adeta, 2013).

2.1.2 Stages in the Development of Cybercrime

It is important to examine the stages and growth in the development of cybercrime before this epidemic became a silent digital phenomenon. According to McLaughlin and Aidoo (1978) submit that the early reports of cybercrime first surfaced in the early 1960s in which the advent of transistor-based computer systems prompted expansion in the utilisation of computer technology. During this period misuse was first reported. At that time cybercrime focused on the physical destruction of computer system parts and stored data, with the first occurrence reportedly happening in Canada in 1969. Further, in the mid-1960s, cybercrime perpetrators in the United States concentrated more on databases and the related risks to privacy. Similarly, Gercke (2012:13) notes that the usage of computers in the 1970s was on the rise and predicted that an estimated number of 100 000 computers were functioning in the United States. Computer technology became important and accessible to the public and corporate organisations. The emergence of cybercrime in the 1970s could be considered as a paradigm shift from the usual ways of committing crime, which includes the physical obliteration of stored data and computer systems that was predominate in the 1960s, to a modernised way of crime. Although physical obliteration was still a pertinent type of crime against computer systems as new types of computer crime were still developing, this includes the manipulation of electronic information. The fundamental change in approach from manual to electronic or computer-related crime provoked a new form of crime that could be classified as computer-related crimes.

Interestingly, in the 1980s the utilisation of personal computers became increasingly common. This advancement in technology and computer systems increased the number of potential targets and victims for cybercriminals (Gercke, 2012). Bolstering this position, Yee (2000) notes that one of the facet effects in the increase of personal computers becoming popular is the development and introduction of software which technically enabled the evolution of the

first forms of software piracy and crime associated with copyright law. Also, this presented cybercriminals with opportunities to distribute computer viruses and malicious software through viable networks without necessarily being at the crime scene. Fast-forward to the 1990s, the graphical interface of the worldwide web (www) was introduced. This initiative aimed to provide universal access to a large universe of documents, compared to the difficult way information had been accessed and shared beforehand. This new initiative encouraged an enormous increase in the number of internet users. This, however, contributed to the challenges and difficulties in the digital world, increasing the numbers of victims and perpetrators.

2.1.3 Globalisation and Cybercrime

Globalisation has risen as a key trend of the new millennium, and in today's society it has become an inevitable reality. No society can be quarantined from the positive and negative impacts of globalisation. Globalisation is a phase of social change that crosses geographical and cultural barriers. Globalisation cannot be separated from the waves of advancement in information and communication technology. The major benefit of this development is the growing access of people to the internet and cyberspace. The internet is one of the most essential features of globalised society and it has helped tremendously in the development of the world. The internet has become a crucial tool for governments, enterprises, associations, and individuals (Nugroho, 2008). More interestingly, the development of the internet has transformed society and reshaped interpersonal processes. However, the unfathomable possibilities inherent in the growth of the internet and the breaking of the world's spatial border is not without limitations and challenges. Regardless of the benefits that come with globalisation, it has also created some cynicism. The main purpose of globalisation is to bring the world together and to make the gathering of information more accessible. The internet has created unlimited access for both legitimate and illegitimate transactions, although some groups of individuals harness the positive use of the internet to perpetrate criminal activities.

This brought forth the introduction of the phenomenon of cybercrime, which has become a significant area of interest as victims, perpetrators, and intentions differ in cybercriminal activities.

The dynamic of cybercrime in the 21st century introduces new drift to the menace; cybercriminals are currently more advanced and organised than ever before. The collection of threats in the cyberspace are changing with the growing interconnection of people and devices, and this trend will continue as the century progresses. In the view of people, this innovation aims to bring suitability and make the world a more captivating place, with new technologies offering numerous opportunities. Concomitantly, in the dark web, cybercriminals have used these technologies to their advantage, equally empowering themselves. The dark web is a world without limitations, a digital wilderness where the rules of law are disregarded. Buttressing this position, Gercke *et al.*, (2012:13;2014) opine that advancement in technology makes it difficult for law enforcement agencies to investigate computer-related crimes. The author, however, emphasises that the method alone did not change but has also had the negative impact of encouraging cybercriminals to launch automated attacks with new strategies, which has resulted in an increase in cybercrime perpetrators around the world. Conversely, countries around the world, including international organisations, have reacted significantly to the growing challenges caused by cybercrime, and have given it extreme priority. This action can be subject to both civil and criminal action depending on the target (Mamandi and Yari, 2014).

Considering the intricacy of cybercrime, it is apparent that many underlying assumptions are flawed, unrealistic, and implausible in explaining the modes of operation of cybercriminals who are fuelled by different motivations. The accelerating waves of change have undoubtedly increased the speed and the precision of cybercrime, as it has grown into a global epidemic affecting both developed and developing countries. For instance, some of the most plausible alternatives to decisively curbing this menace may equally counter some positive outcomes of

the cyber world. For example, shutting down the cyber system will mean those using it for all types of positive things will be locked out. Also, improvement in technology has introduced new dynamics, hence, cybercrime activities have birthed new problems, such as the different types of cyber-criminality (Olugbodi, 2010). With the digitisation of society, crimes have also been digitalised and have made some criminal activities, like cybercrime a global concern (Bassmann, 2015). Buttressing this position, Bernik *et al.*, (2013) notes that cybercrime perpetrators have gained great access to a new world of unlimited possibilities and opportunities. From the days of email romance scams, internet fraud has metamorphosised into new forms, such as hacking databases, taking down websites or networks, creating botnets, infecting computers with malware, crippling information technology (IT) systems using Denial of Service Attack (DDoS), internet fraud, threats, and cyberstalking, among other things (Leukfeldt, 2017). Information technology plays an increasingly important role in the realisation of cyber-enabled crimes. Digitisation has great consequences for a large chunk of crimes and raises all sorts of questions. Perpetrators of cybercrime are unmatched and untainted by state apparatus, with no geographical limitations because of the advent of the internet and globalisation, which gives them global access from the comfort of their homes, just like any other person (Bernik *et al*., 2013).

In this light, it is important to also state that cybercrime has become a criminal activity that has emerged from an individual level to being perpetrated by groups and geographically boundless networks. Von Lampe (2007) affirms that perpetrators no longer act individually but frequently work in cooperation and with varying teams. Equally, Anderson *et al*., (2012) submits that, overtime, cybercrime has gradually evolved from a relatively low volume crime committed by an individual to a mainstream organised crime. Cybercriminals build associations and crime corners in an advanced way. Internet evolution has boosted development in other areas of information and communication technology. In the same vein, mobile devices and cloud

computing are among the biggest technological breakthroughs because of its fast, revealing, simple, and fast internet connectivity (Chicone, 2009; Riedy *et al.*, 2011). The constant improvement in technology and globalisation has broadened the scope of communication across the nations of the world, aided primarily by the internet.

2.1.4 Global Statistics of Cybercrime and the Implications

Cybercrime has serious implications, the extent of which can be far-reaching. These implications can be examined from different perspectives such as exploring the economic, social, and political implications. From an economic point of view, several people have lost fortunes to the incidence of cybercrime. Lewis and Baker (2013:5) submit that the annual damage caused by cybercrime, globally, is estimated to be anywhere between 300 billion and 1 trillion USD, affecting 556 million people worldwide. Norton's cybercrime report (2014) submits that most internet users around the world have fallen victim and feel, "powerless against the faceless", cybercrime perpetrators. The statistical report shows that 65 per cent of adults in the world have been victims of cybercrime. The report reveals that malware attacks and computer viruses are the most distinctive types of cybercrime experienced by people while online romance scams, the cloning of social media profiles, credit card fraud, and phishing are on the increase as well.

A ground-breaking study conducted by Norton in 2011 revealed that in 2010, more than 74 million people were victims of cybercrime in the United States. These criminal activities led to direct economic losses of 32 billion USD. More assessment of this underlying issue discloses that 69 per cent of internet users, especially adults, have been victims of cybercrime, increasing the number of victims to one million a day (Coleman, 2011). There is a clear indication that cybercrime has impacted the global economy negatively, as the economy continues to depend on the internet more for success it is endangered to the peril of cybercriminals. Also, the annual revenue accumulation of cybercrime varies depending on the source. According to Gregory

Webb, the CEO of Bromium, a private computer software company which has overwhelming research finding on a blog posted in April 2018. The study states that, "cybercriminals generate revenues of $1.5trillion annually from illicit activities". However, cybercrime, which has developed into a professional economy similar to other legitimate industries with tremendous revenue, reports on the waves of cybercrime from a global perspective, discloses the extent at which cybercrime activities such as data breaches, thefts of intellectual property, ransomware have generated more revenue than cooperate organisations such as Facebook, Netflix, Apple, and Google in recent years (Brain O'Connor, 2018).

Similarly, Gercke (2012:14) argues that statistics only reveal crime that has been identified and reported, there are concerns that the number of cases not reported are significant. For instance, companies and cooperate organisations might be sceptical to publicly disclose that their server has been assessed by cybercriminals (hackers) as this might affect their reputation, hence, it detaches the trust and faith of their customers. The consequences could be more prominent than the misfortune that could be caused by cybercrime attack. Affirming this position, McGuire (2018) contends that the 1.5 trillion USD annual estimate revealed by other studies is most likely low due to difficulties in the acquisition of global data. The study further argues that the estimated figure is based only on five conspicuous types of cybercrime. Meanwhile, McGuire reports that malicious software designed specifically to automate cybercrime, popularly called crime-ware, generates 1.6 billion USD through Trojan-related malware sales and DDoS attacks in the cybercrime industry, these tools are mostly used by hackers. However, the estimate completely overlooks other forms of cybercrime, such as romance scams, advance fee scams, and credit card scams, which generated approximately 29 billion USD in the United States, Australia, and the United Kingdom in 2015 (McGuire, 2018). Despite these precarious statistics, the United States has frequently provided and lead the race in estimated global crimes. Like every other street crime, cyber-attacks are the fastest emerging crime in the United

States, and they are growing by large magnitude, cost, and complexity. Also, the cyber security venture report (2019) maintains that cybercrime is causing global damage, hence, security demands are promptly growing, suggesting that cybercrime has become an extraordinary threat affecting both public and private sectors. The report further predicts that by 2021 cybercrime will cost the world six trillion USD. Although addressing these issues, the major challenges in regulating cybercrime are the expensive technology and human resources required for this problem. Since cybercrime is based on technology, the treatment should also be based on technology, and as a result, it will incur higher costs than other methods of crime prevention.

The deleterious social impact of cybercrime can be sensed across the social spectrum, like every other crime has its divergent impact on society and the world at large. Many scholarly studies reveal that it has influenced people's social life as a whole, like other crimes. In understanding the impacts of cybercrime, it is important to see the effects of computer technology and the internet on people since cybercrime is certainly a consequence of computer technology and is also closely linked to the internet. Cybercrimes mainly affect developed and developing countries in social terms. As discussed before, the prosecution and investigation of cybercrime is not an easy process and developing and underdeveloped countries have to fund this area by sacrificing other important social programs for the benefit of society (Khadam, 2012). Individuals and businesses also have an increasing sense of fear and anxiety about the activities of cybercriminals. IBM's study, which released in 2006 and was cited by kshetri (2010), found that United States companies are more concerned with cybercrime than physical crime. The report shows that Americans believed they were three times more likely to be victims of cybercrime than physical crime. Buttressing this position, Khadam (2012) submits that the social impacts of cybercrime are due to the threat and vulnerability perceived by the public, and at some point, the need to be involved in the use of modern technology might reduce, this is in a bid to be protected from criminal actions occurring in the cyberspace. This

could influence people's social networking and, thus, close many people's doors to fortunes in such a globalised age. Another social impact relative to this research can be adopted from Elgie McFayden Jr.'s *Implications of White-Collar Crimes*, which emphasises that in some parts of the world, for example Nigeria, the youth see white-collar crime as a lifestyle and a good way of life which has diminished their mentality to understand the consequences of such actions. Therefore, cybercrime, which is also considered a white-collar crime, affects the young people of nations and, more specifically, the intelligent and knowledgeable, since cybercrime involves a high level of intelligence (McFayden, 2010).

Lastly, since the 1980s, politically motivated computer crimes have increasingly progressed. According to the US Department of Homeland Security, cyber-attacks against US federal agencies rose by 152 per cent in 2007 compared to the previous year (United press international, 2009, Cited by Shank, 2011). The Department of Defence (DoD) also reported in 2008 that it has witnessed more than 3 million attacks annually on its network (Hess, 2008). In 2009, the FBI ranked cybercrime as the third largest threat to US national security following nuclear war and weapons of mass destruction (Sloane, 2009, citied by Kshetri, 2010). All cyber-attacks and threats come from the political agendas of both nation-states and individuals or groups. Governments, businesses, and individuals can all be affected by state-sponsored web attacks which can cause major disruptions to public services such as banking, as shown in the 2007 cyber-attacks on Estonia[1]. The negative implication of this is that it limits the opportunities for multinational organisations to invest resources in underdeveloped countries. Mcfayden (2010) opines that a swift increase in white-collar crimes can result in increased funding for warlords and anti-government regimes. It allows better protection for criminal organisations from the police and government services. Hacking into government organisations

[1] http://www.computerweekly.com/opinion/How-do-we-tackle-political-cyber-crime accessed on 20 October 2019.

and the website of political parties is not a new phenomenon across the world; for example, Russia tried hacking the 2016 US presidential elections which certainly adversely affected the country's political scenario (CNN, 2016).

2.1.5 Typologies of Cybercrime

Cybercrime is comprised of a broad range of atrocities. Therefore, it becomes problematic to classify cybercrime as a single entity (McCusker, 2006). Correspondingly, Koops (2011) suggests that the internet has been instrumental in the perpetuation and sustenance of cybercrime. The internet has, therefore, completely transformed how cybercrime is being perpetrated. Cybercrime advances into new forms with different dynamics every year. In recent years cybercrime has become more organised and the growth is winding up tremendously. According to Taylor *et al.* (2014), cybercrime can be classified into two categories, the first category deals with the infections of computers with malware and viruses, while the second engages with cyber tools as a medium for deceit and fraud, such as identity theft, cyber stalking, and information warfare phishing scams. Therefore, to understand the dynamics of cybercrime it is essential to distinguish it appropriately, since the modus operandi by perpetrators differs completely depending on the form of cybercrime. Koop (2011) maintains that cybercrime has become a contemporary phenomenon affecting the world on a global scale. Koop (2011) emphasises the fact that computer inventions and advancements in technologies have empowered individuals, hence, the digital world has become a vehicle for cybercriminals to commit fraud, all of which raises new questions in regard to criminal law and policy. Shinder (2002) defines cybercrime and its related activities as any form of criminal act or offence committed with the use of the internet or components of networks as part of the crime, whether there is legal or illegal motive.

These crimes are committed against individuals, groups, or institutions with the criminal intention of harming potential victims, in many instances this could cause psychological

damage either directly or indirectly, using the medium of telecommunication networks such as the internet and mobile phones. Drawing on insight from technologies and how they have pervaded society, Broadhurst *et al*., (2013) debate that technology improves the effectiveness of our customary daily activities, as well the proficiency of criminal activities; for instance, in promoting criminal conspiracies where cybercriminals and terrorists use the internet as a means of communication. In the case of reputable citizens, however, the internet has been adopted for positive uses, such as storing data, sharing information, and completing financial transactions, whilst financial transaction in the case of cybercriminals could refer to money laundering (Ulbricht, 2013). Gercke (2012) acknowledges three main cybercrime offences: Offences against the confidentiality, integrity, and availability of computer data and systems (hacking, viruses, and possessing hacker software); Computer-related offences such as offences of forgery and fraud; and Content-related offences such as copyright and patent offences. The aforementioned prominent forms of cybercrime are discussed below.

2.1.6 Software piracy

According to Kin-Wai Lau (2006), software piracy is the unauthorised copying and lifting of someone's works or software. By design, most software is meant to serve one user without hitch. It is clear that when an individual purchases software, he or she is using it as a licensed user and not otherwise. As a licensed user, he or she is charged with the responsibility of not selling or using the software for nefarious acts (Morgan, 2017). The distribution of such software is a violation of copyright laws across the world. Due to the way and manner in which software engineers have designed their software, it is impossible to entirely stop piracy.

Hence, software companies now launch legal suits against bandits and criminals violating their software rights under software copyright law. Years ago, software companies attempted to prevent software piracy by copy-protecting software, but this strategy was neither fool proof nor convenient for users (Shinder, 2011). Software companies sincerely advocate for

software registration when launching the software for the first time, this comes in many forms, such as a mechanism to check on piracy and the illegal usage and distribution of the software. This entails the illegal copying of software for distribution and resale. On countless occasions numerous software companies have incurred losses of whopping sums of money annually, thereby killing the software companies financially and people also losses their jobs and livelihoods as a result (Tade and Aliyu, 2011; Ajayi, 2015; Leukfeldt, 2017). Software piracy is a major issue around the world, most especially in the United States and European countries. It has become a tradition to use people's software without their knowledge and without any legal repercussion. Such criminal acts are also very rampant in Africa.

The Symantec Corporation (2009) have discussed forms of software piracy. One of which is counterfeiting, which is the illegal selection, copying or duplication, distribution, and sale of materials that are copyrighted with the sole aim of imitation. It is purely an adaptation of the original for local use at a very cheap rate. In the case of packaged software, it is common to find counterfeit copies of the compact discs incorporating the software programs, as well as the related packaging, manuals, license agreements, labels, registration cards, and security features. The second form of software piracy is related to the internet. Internet gurus, especially hackers, go on to the internet to download any software with the sole aim of either using it privately or producing it in commercial quantity. Another is internet piracy, which occurs when the software is downloaded from the internet. In most cases, online software needs to be purchased in the same way physical compact disc versions of the software do. Here listed are some of the common internet piracy techniques and adaptations of websites that make software available for free download or in exchange for other copies of different software; internet auction sites that offer counterfeit or out of channel software; peer-to-peer networks that enable the unauthorised transfer of copyrighted programs; there is also user piracy which occurs when an individual reproduces copies of software without authorisation,

for example, using one licensed copy to install a program on multiple computers; copying disc for multiple installations or distribution; taking advantage of upgrade offers without having a legal copy of the version to be upgraded; acquiring academic, other restricted, or non-retail versions of software without the proper license; and swapping discs in or outside of the online space (Yar and Jewkes, 2010; Adaramola, 2018).

There is also client-server overuse as a type of software piracy. This type of piracy occurs when too many users on a network are using a central copy of a program at the same time. The availability of local area networks does not make the software free for all users. Using the server to install programs for several people to use shows criminal intent. Some will go ahead to abuse this by giving others access- criminals-in-partnership.

2.1.7 Online Romance Scams

With numerous types of cybercrime being perpetrated globally, romance scam is one of the common typologies of cybercrime. Whitty (2018) describes online romance scams as a type of advance fee fraud, usually perpetrated by international criminal groups, particularly from West African countries, through dating websites and social network sites to trick potential victims out of money. The study conducted by Whitty (2018) reveals that criminals inaugurate a relationship to defraud their victims of a massive amount of money. These criminals create a fake profile on dating websites with the use of fake identities and develop a relationship with their victims by proclaiming their love until they are convinced the victim is ready to part with their money.

Cybercriminals, however, leverage the relationship gained and built on the dating website then show interest in meeting their victim but claim that they need money for travel and other miscellaneous expenses ranging from hotel accommodation to restaurants among other things. They often then lie, claiming to have been trapped in a foreign land, needing emergency exit before they are jailed, or they claim that they have to pay medical bills abroad. There are other

countless numbers of frivolous requisitions and mundane things that scammers request from their victims. Scammers may use the confidence gained to introduce a variant of the original Nigeria letter scheme (Balancing Act, 2014; Ajayi, 2015), such as saying that they need to get money or valuables out of the country and offer to share the wealth, requesting help in leaving the country, which is even more attractive to the victim.

Flowing from the above, Whitty and Buchanan (2012) opine that this heinous activity perpetrated by cybercriminals has a twofold hit on the victim, this is in the form of financial misfortune and the loss of the relationship. However, their study submits that for certain victims the loss of the relationship was more irritating than their financial misfortune, with some victims portraying their misfortune as something that could be compared to incurring the loss of a friend or family member. Also, Titus and Gover (2001) highlight that the characteristics of the victims of romance scams include greed, gullibility, being a risk-taker, generosity, being a good citizen, and showing high displays of trust. However, contrary to the public notion that stupid people are the most gullible and account for most of the victims of romance scams, Fischer *et al*. (2012) argue that educated people are also likely to be victims of romance scams because they are massive users of online dating websites. They further argue that being educated does not necessarily rescue you from being scammed.

2.1.8 Website Hacking

Website hacking is unquestionably on the increase. Kothari (2018) believes that website hacking, and penetrative criminal activities are carried out for two core reasons, which are to control the extent of damage or destroy, access, use, or jailbreak a protocol without the knowledge of an institution. It is any activity that changes the behaviour of things on a website from their original status. However, scammers and hackers are becoming more advanced by the day, ranging from small units of networkers to massive syndicates of high wired intrigues. To make it explicitly clear, hacking means gaining access to a website's details without proper

notice or attention. It is as simple as badging into people's accounts without prior notice and without being given a password. This is a criminal act according to the law. Over time, there are countless numbers of sites that are being hacked daily such as Facebook and Yahoo among others (Fafinski and Minassian, 2009; Chawki *et al.*, 2015a).

After such atrocities, hackers are sometimes susceptible to change the password, which will make the account difficult for webmasters to access. Hackers usually insert harmful programs by inserting malicious code into the website. This will also cause the website server to be slow (Spitzber and Hoobler, 2002). Many notable companies and organisations have been hacked, like Amazon and Yahoo (Council of Europe, 2001; Chawki *et al.*, 2015a). Hacking a website means taking control of the website owner. Suppose an individual owns the username and password to control the website for the sake of mopping up web pages, adding and deleting contents, maintaining tables, or controlling membership, should a hacker gain access to said username and password control will be lost from the owner and the hacker would gain control of the aforementioned processes and directions of the website.

The hacker gets the username and password and then begins to use them to carry out their nefarious acts as well as destroy valuable information databases. Hackers try as much as possible to use various permutations and combinations to gain access to websites and wreak havoc without minding the implications thereof (FBI, 2014; Bernik *et al.*, 2013).

2.1.9 Identity Theft

One of the most fascinating yet most overlooked forms of cybercrime is identity theft. Identity theft is the deliberate use of someone else's identity to perpetrate a crime. Identity theft is ranked among one of the fastest-growing crimes in the western world. Koops and Leenes (2006) argue that there is no precise definition of identity theft because it is difficult to understand the threat posited by this phenomenon. This crime encompasses adopting the identifying information of an individual in order to pseudo-represent the original person. It is

purely an assumption of a person's data and credentials so as to complete transactions of any kind between the victim and organisations for the sole purpose of wrong use, in most cases financial gain. To succinctly conceptualise this act, identity theft perpetrators do not steal identities, rather they adopt an identity as a mechanism to steal money without the victim realising they have been scammed for a long period of time. A lot of things can be achieved with identities, not only can someone else's identity be used but people can likewise swap identities or destroy identities; such things can, in cases, occur coincidentally. However, in the context of 'yahoo-yahoo', it occurs when an individual or group of people steal one person's details to commit a crime, for example, open new bank accounts, file fake tax returns, and other criminal activities.

Erika Harrell (2016) reveals that an estimate of 26 million American citizens, 16 or older, have reportedly been a victim of identity theft. The author mentions that five per cent of residents in America, 16 and older, had encountered at least one incident that involves the misappropriation of an existing credit card, and five per cent of American residents had encountered the misuse of an existing bank account. Erika Harrell (2016) also highlights that one per cent of US occupants, age 16 and above, had encountered the misuse use of their personal information to commit a crime such as fraudulent claims for government benefits or medical care. However, this odious crime rarely harms the victim. An evaluation revealed that 12 per cent of identity theft victims had experienced an impecunious loss of $1 or more, while 88 per cent of the victims had no impecunious loss. Erika's statistical argument mentioned that over 10 per cent of identity theft victims had experienced serious emotional pain because of the illegal activities perpetrated by criminals. Also, Hoofnagle (2007) discusses the degree of financial impairment identity theft has caused to co-operate organisations, individuals, consumers of retail establishments, and the economy. The author further probes that the Federal Trade Commission (FCT) has described this mischievous act perpetrated by criminals

as the fastest growing white-collar crime, which makes it difficult to highlight its prevalence and how much damage it has caused on the economy despite efforts and laws enacted by the federal and state government to curb this menace.

As discussed above, the rapid growth of identity theft is becoming problematic globally, especially in western countries. Hoofnagle (2012) identifies the two distinct categories of identity theft as new account fraud and account takeover. New account fraud requires an impersonator creating a new credit card account, mortgage, or requesting other commercial services with information of another person. However, this type of crime entails that the impersonator has access to the prospective victim's social security number (SSN) to successfully perpetrate the crime. However, the author emphasises that new account fraud can become problematic for potential victims because the fraudulent account may appear in their credit history, making it difficult for them to obtain credit if necessary and could also stand as an obstacle for employment. Inquisitively, there is a significant aspect of new account fraud called synthetic identity theft, this is different from the popular new account fraud that involves the utilisation of the potential victim's real name. In the occurrence of synthetic identity theft, the criminal acquires the victims' social security number (SSN) with a fictitious name that allows the criminal to create a new synthetic identity which is used to create a fraudulent account and make fraudulent purchases. In other cases, the criminal can generate a fraudulent identity from scratch with entirely fictitious information, at this point no victim is targeted by the perpetrators of this illicit crime.

Synthetic identity theft has more negative impacts than new account fraud as it creates massive havoc, and its growth has become rapid. Although, no dependable statistics are revealing impecunious losses from synthetic identity theft, however, some profound experts argue and estimate that synthetic theft activities contribute nothing less than 20 per cent of credit charge offs and 80 per cent of casualties from credit fraud. This statistic indicates the

tremendous growth of this type of crime (Cook, 2005). On the other hand, account takeover, which is another form of identity theft, has been perpetrated differently. In this circumstance, the impersonator adopts a victim's valid financial account information and uses it for credit card fraud, which is normally achieved through phishing. Phishing is the act of deceiving prospective victims into revealing passwords to their personal information, thus, permitting the perpetrator to gain access to their financial accounts (Hong, 2012). Probing further, Hoofnagle (2007) opines that there is a targeted account for this crime, the author mentions that traditional checking accounts, saving accounts, and auction services such as eBay and PayPal are the main targets for phishers. In the nefarious acts of adopting people's personal information, criminals represent their victim to defraud, withdraw, relate, and even pretend to be another person in order to avoid summons, dodge the discovery of a check, or avoid a warrant document bearing their real name and details. It is also used to avoid an arrest or conviction record. In health-related theft, some bandits bear someone else's details to enjoin free health care, while in the finance world identity theft uses people private details to make money through illegal means. In child identity theft, someone uses a child's name and social security details for various forms of personal gain. This is also extremely common as children typically do not have information associated with them that could pose as obstacles for the perpetrator, who may use the child's name and social security number to obtain a residence, find employment, obtains loans, or avoid arrest for outstanding warrants. Often, the victim is a family member or someone close *(*Jøsang, 2007).

Hoofnagle, (2007) discusses high-tech identity theft as another form of identity theft. It increasingly thrives with the use of modern technologies to obtain people details for fraudulent activities and criminalities. To indulge in such, they search hard drives of stolen computers and other accessories that could have leading information that may help them hack into websites, computers, or computer networks, access computer-based public records, use

information-gathering malware to infect computers, browse social networking sites, or generate deceptive emails or text messages. Irrespective of how people view it, identity theft can be prevented.

According to Tade and Aliyu (2011) and Shinder (2002), one of the most crucial means of averting such acts is to constantly check and monitor personal documents, bank cards, computer systems, and other valuable information, so that when any form of illegal activity comes up, it can be quickly reported without much damage being done. Nowadays, lots of businesses provide products that help people avoid and mitigate the effects of identity theft. It helps people to safeguard their private information and monitor the public domain and personal records with immediate effect to alert their respective clients and instruct them to terminate or stall any further transactions. Also, some government agencies and non-profit organisations provide similar assistance, typically with websites that have information and tools to help people avoid, remedy, and report incidents of identity theft.

In their study, Nhan *et al*. (2009) examine, "Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Solicitation". It was discovered that the amount of internet spam has grown exponentially over the last decade. While much of these unsolicited emails are harmless advertising, a growing proportion of them are insidious in nature and fraudulent in intent. Two email accounts were used to capture a total of 476 unsolicited emails identified as coming from a single suspect over the course of three months. The researchers analysed the nature of the solicitation, the nature of the solicitor, and the information asked for from the target. The findings show that relationship-building social engineering methods are preferred over the direct inquiry of sensitive information.

2.1.10 Phishing

This is an ICT term which depicts imitative sites set up with the broad aim of deceiving users and making them give out private details, particularly information relating to their banks or

network agencies (Ramzan, 2010). It also takes the shape of unnecessary spammed emails that look like ones sent from one's banks or network agencies. It is the scandalous means of obtaining sensitive information, such as application and websites names, passwords, pins, or log-on links, by disguising a site or email as a clean entity or one created by a trusted institution in electronic communication (Tan, 2006).

They usually use email spoofing or instant messenger which usually redirect users to enter their personal information and private details into non-existing websites. Phishing is one of the criminal means and social mechanisms being used to deceive most people, especially greedy internet users who are often lured through a nefarious means or perhaps a trap purported from a clean source or trusted party, such as social web sites, auction sites, banks, online payment processors, or IT administrators (Jøsang, 2007). Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures, because phishing attacks also often exploit weaknesses in current web security.

2.1.11 Advance Fee Fraud

The Federal Bureau of Investigation (FBI, 2016) defines advance fee fraud an illegal scheme which occurs when the victim pays money to someone in anticipation of receiving something of greater value in return such as a loan, contract, investment, or gift and then they receive little or nothing in return. It is a very common type of fraud and one of the types that are predominant among the youth in nearly all countries of the world, especially West African countries. This cybercrime intends to promise the victim a lion's share in the sum of money involved in the deal in exchange for a short, small payment which the criminal asks for in order to obtain the large sum. When such payment is made, the cyber fraudster may likely demand more cash or disappear into thin air. There are many variations of this type of scam, including the 419 scams (also known as the Nigeria prince scam), the Spanish prisoner scam, the black money scam, Fifo's fraud, and the Detroit-Buffalo scam. The scam has been used with fax

and traditional mail and is now prevalent in online communications (Etter, 2002).

According to Ajayi (2015; 2016) and Okochu (2017), advanced fee fraud is labelled after criminal code 419 in the Nigerian constitution, which is completely outlawed. The criminal act is always perfected in a near clean way that victims believe they are engaging in a 100 per cent honest dealing which later will turn out to be false. This occurs after the victims would have suffered massively in terms of emotions, investment, finance, time wastage, material losses, and psychological depravity. Whittaker and Button (2020) noted that several people have been victims of this type of scam. Balancing the equations, most of the victims are not faithful to themselves. They crave free things, money, and materials but end up losing lots of all of these things without prior notice or signals. They easily fall victim because of a thirst for gifts and lunches. In any case, fraudsters of this caliber, have different strategies they use to hook their victims, with the sole aim of achieving high returns within a short space of time. Internet scams and their related fraudulent practices are the commonest ways of duping people out of their hard-earned valuables and material resources (Jude, 2011; Kaplan, 2010). For instance, an internet scammer or fraudster sends an email to an identified victim informing him or her of a huge sum of money in foreign currency that has just been won, giving excellent but imaginary details of the award. The scammer then goes ahead to demand the personal details of his victim, including their bank account number where the imaginary money can be lodged or transferred. This is especially common these days.

2.1.12 Electronic Fraud

There has been a steady increase in the number of internet users around the world and the development has given way to unlimited possibilities for global e-commerce. Literature has established that the internet and e-commerce are significant aspects of developmental progress (Hoffman, 2000). Thus, contemporary society is dependent on information communication technology to function as the swing towards digitalisation is growing rapidly. The

advancement in the utilisation of technologies in developed and developing countries is the path that has led to an increase in electronic fraud. In developing countries, e-commerce was anticipated to bring a new dimension into financial development (Humphrey *et al*., 2003). The possibilities provided by information communication technology (ICT) are a paramount requirement for e-commerce which has persuaded people to think that e-commerce will enable developing countries to grow and put them on the global economic map. Unfortunately, the same opportunities that come with the advancement in technology are being explored by cybercriminals to perpetrate fraud. Conversely, Kanu and Okorafor (2013) opine that banking and financial institutions are important because they determine the economic growth of any country and, therefore, it becomes essential to protect these financial institutions from the activities of cybercriminals. These criminal activities are identified as electronic fraud, which includes automated teller machine (ATM) fraud and credit card fraud. While trying to capitalise on the advantages and possibilities of modern technologies, most people have ended up being victims, cybercriminals purposefully configure or design similar websites that look legitimate where unfortunate victims enter their personal information such as usernames and passwords of their credit cards. In other cases, emails are sent to the recipient by fraudsters requesting sensitive information, upon disclosure of this information the cybercriminals gain access into accounts and damage is executed (Dzomira, 2014:18)

Electronic fraud is a type of fraud carried out on the internet under a heavy presence, fraudsters provide incorrect information for the sole aim of duping people out of their valuables, money, time, and properties. Internet or electronic fraud is not seen as the only crime perpetrated online; it is unique but has a hegemonic power with arrays of associated criminal acts. It covers a range of illegal and illicit actions that are committed in the cyberspace. It is, however, differentiated from theft since, in this case, victims voluntarily provide personal information to perpetrators. It is also distinguished by the way it involves temporally and spatially

separated offenders (ICCC, 2013; 2014). According to the FBI internet crime report (2017), the internet crime complaints center received about 300,000 complaints from victims who lost over 14 billion USD to online fraud. According to a study conducted by the Centre for Strategic and International Studies (CSIS) and McAfee, cybercrime costs the global economy as much as 600 billion USD, which translates into 0.8 per cent of the global GDP. It is crystal clear that cyber fraud appears in many forms with different styles, ranging from email spoofing, spam box messages, and false links, among other things.

2.1.13 Ransomware and Cryptocrime

The tremendous growth in the number of internet users and private computer users all over the world has amplified numerous opportunities for cybercrime perpetrators to explore. Cybercriminals, through a cyber-phenomenon called ransomware, have established a platform for targeting data stored on computers. The United States Computer Emergency Readiness Team (US-CERT, 2016) defines ransomware as a "form of malicious software (malware) that infects a device and restricts access to it until a ransom is paid to unlock it". The process involves the contamination of computers, making them unusable for users except for smalls parts of operation. Ransomware is essentially 'digital extortion*' and* is a form of cybercriminal activity gaining recognition in the cybercrime industry. The mode of operations includes the use of malware and malicious codes that infect computers. This cybercrime activity varies from email attachments, freeware apps, and advertisements that offer money and incentives to attract potential victims (O'Gorman and McDonald, 2012; Bhardwaj *et al*., 2016). Ransomware attacks have, therefore, materialised into a prevalent and aggressive cyber threat that frustrates individuals as well as companies, hospitals, and cooperate organisations (Popli and Girdhar, 2019). Similarly, Czuck (2017) reported that Kaspersky Lab solutions detected and stopped 479,528,279 malicious cyber-attacks around the world and revealed that mobile ransomware attacks were amplified by more than 13 times from the previous quarter, in the

first quarter, as reported in 2017.

Despite the fact that ransomware has been present for more than a decade, the rise of cryptocurrencies has allowed this particular sort of malware to become more prevalent. Ransomware is believed to have cost businesses between £1.9 million and £3.8 million in the first three quarters of 2012 (O'Gorman and McDonald 2012). Prepaid money cards such as Paysafecard, Ukash, and Moneypak were used to make these payments. Due to malware developers using cryptocurrencies, their income increased by an order of magnitude. Crypto Locker, a specific type of Bitcoin-based ransomware, was studied for a span of five months from 2013 to 2014 and the researchers discovered that $300,000 to $1,000,000 was lost due to this infection (Anderson et al., 2019) . Over a two-year period from 2015 to 2017, Huang et al (2018) discovered $16 million in illegal money generated by ransomware via cryptocurrencies. In an independent investigation conducted by Paquet-Clouston et al (2019), these findings were corroborated. Without a doubt, direct damages as a result of ransomware (for example, lost data and systems, and recovery time) may be one to two orders of magnitude higher than other forms of cybercrime.

There have been other types of crimes associated with digital currency as well, including scams perpetrated by bitcoin exchanges and underground drug marketplaces against their customers, as well as attacks on these exchanges and markets by hackers. The bankruptcy of Mt. Gox in 2014, when an exchange declared that a large portion of its bitcoin stock had been stolen and there were various allegations of internal malfeasance, was the beginning of an unprecedented series of exchanges and other cryptocurrency traders going out of business, often citing hacks as the reason for their failure. Consumer bitcoin wallets are increasingly being "hosted" by exchanges, which means that they hold the bitcoins rather than the customer, and act more like a bank than a safe-custody service.

Thus, it is apparent that these attacks on devices or computers are financially motivated for

cybercriminals, this mere act affects many countries economy most especially the United States economy, individuals, and companies across the world, making them lose billions of dollars. Also, the impact of malware and ransom has become a global threat to computer users in terms of stealing and gaining access to the personal and private information of unfortunate victims, such as locking and disabling personal computers. In 2017 the global statistics of ransomware skyrocketed to 5 billion USD in total damages, whilst it was expected to cost the world 11.5 billion USD in 2019 and 20 billion USD in 2021 (cyber security, 2019). According to Cyence, a cyber-risk firm estimated that the WannaCry ransomware that surfaced in 2017 could result in a global economic loss of four billion USD (Tapsoba, 2018).

This emerging form of crime has become a new phenomenon and business enterprise skyrocketing in the cyberspace (United States Department of Justice, 2018). The method adopted by cybercriminals to perpetuate this criminal act often used by cybercriminals is to have computer users download payload malware that contains viruses and codes which hack into their devices. It is installed as an application with the purpose of been able to perform all kinds of operations on the computer, thus, it is concealed on the device of the owner in a hidden place. This code or virus takes over the computer or device of the users when it been launched, hence, it prevents users from obtaining access to personal information and computer system encryption that would have been accessible ordinarily. Other possible function could be stopping applications from running on the computer, disabling physical input devices, and obstructing the operating system (Bhardwaj *et al*., 2016).

There has been some scholarly work on understanding the methods extortionists have adopted in asking victims to make payments. Extortionist, in this context, are referred to as hackers, it has been noted that the proliferation of ransomware could be partially fueled by the spread of crypto currencies. Before cryptocurrencies became a massive digital asset, extortionists usually asked victims to send money directly to bank accounts through money transfers and

bank deposits, and such transactions were traceable if law enforcement agencies got involved. Crypto currencies aid the easy perpetration of ransomware because identifying perpetrators based on bitcoin addresses is almost impossible. (Kshetri and Voas, 2017:11; Tapsoba, 2018). Similarly, the cybersecurity (2019) report reveals that law enforcement agencies advised individuals and organisations to ignore extortionists seeking ransom through any form of cryptocurrency, this has reduced the percentage of ransom victims who pay bitcoins to hackers or extortionists hoping to claim their personal information.

Tapsoba (2018) argues that extorting victims is often based on the request of hackers for money as soon as possible before victims can regain access to their information or resources. However, three notable factors instigate the process of paying the ransom. The first factor is educated users; it is believed that well-educated users will not be threatened by the antics of the hackers due to a good back up policy and excellent system restore options that can prevent malware attacks. These policies are believed to interrupt all kinds of transactions because, in this situation, the hacker does not have control. Secondly, the complexity level of the malware; this examines the extent to which malware has caused damage to the computer or the device of the victim and also determines if the victim can recover or repair the damaged information. Depending on the complexity of the virus imposed on the device, the victim might find it difficult to retrieve information without contacting the hacker. Occasionally, the computer or device now depends on the malware to function effectively. Lastly, the urgency of recovery; ransomware might not be successful if recovering the data seized by the hacker is not particularly important to the victim. A victim may as well disregard the antics of the hacker when the information or resources are less important.

To recap, the steady rise of this threat in recent years is a burgeoning problem which has rapidly become an extremely lucrative criminal enterprise. Embattled organisations often think that the most cost-effective way to get their data back is to pay the ransom and,

unfortunately, this may be the reality as well. Companies that pay to recover their files are directly financing the development of the next generation of ransomware. As a result, ransomware is growing at an alarming rate, with more complex development making it more important than ever to protect data from ransomware.

2.2 Understanding the Swiftness of Cybercrime from an African Perspective

Cybercrime is without a doubt a global issue and no country is exempt from the vulnerability it causes. In appraising the degree of the phenomenon, it is important to examine some pressing issues, such as political instability and poverty pre-occupying some Africa countries. As such, these factors contribute to the meteoric increase of cybercrime on the continent. The modern age of digital technology creates a new environment for criminal behaviour, so criminality is also burgeoning massively without restriction. As a consequence, cyber security analysts are advocating for more effective ways and measures to educate users on security awareness, develop regulations, and build a better information infrastructure to help at all fronts in the quest to decisively deal with cybercrime. Through a critical review of existing literature, Tade and Aliyu (2011) reveal that the extent of cybercrime in Sub-Saharan Africa is far-reaching, cyber criminality in the region has become increasingly pervasive.

Socio-economic problems, like unemployment issues, which have gone overboard in most Africa countries and have led abject poverty and redundancy, have predisposed the citizenry, especially the youth, to partake in fraudulent activities, both online and offline, as a means to survive, irrespective of the weight of such atrocities. The growth of cybercrime is complementary to the prevalent poverty and employment coupled with a dire need to survive on the continent. Symantec's (2016) ground-breaking research on cybercrime in Africa reports that 24 million incidents of malware activities were recorded on the continent. Equally, in another study, it was observed that cybercrime was on the increase in Africa more than any other continent in the world. Another statistical report submits that more than 400,000 incidents

were linked to malware and malicious crimes in Africa, while 44 million spam emails and 280,000 botnet crimes existed in Africa (Ghana financial institutions, 2016). The literature on the prevalence of cybercrime in Africa has ranked the most fraudulent countries in the world; there is generally an assumption that it is becoming a giant illegal organisation in Africa (Ojedokun, 2005; Olowu, 2009; Ibrahim, 2016). Of course, at the mention of Africa-based criminal organisations, the stereotyped country that come to minds is Nigeria and Ghana, which are indeed host the most sophisticated cyber criminals in the world and the various financial scams known as '419' frauds (Oriola, 2005; Olowu 2009; Warner, 2011). Therefore, this subsection examines the narratives around cybercrime in some Africa countries, since they are globally recognised as safe havens for cybercriminals.

2.3 Cybercrime - Rife in West Africa

Computing and internet developments have brought about incredible technological advances to human society and these developments support contemporary society in many respects. Because these developments are followed by unlimited opportunities, they have also created unlimited opportunities for criminal activity around the globe and raised concerns about internet usage protection (Nkanga, 2008; Aransiola and Asindemade, 2017). However, these unlimited opportunities explored by cybercriminals have caused a great deal of concern over the range of cyber-enabled and cyber-dependent crimes emerging from West Africa or perpetrated by West Africans across the world. The most popular forms of these illicit activities come in the form of spamming, financial fraud, hacking, terrorism, drugs, and human trafficking (Quarshie and Martin-Odoom, 2012; Witty and Ng, 2017). Scientific research has shown that Nigeria leads in these malevolent internet activities that continue to persist in West Africa (Longe and Chiemeke, 2008; Aransiola and Asindemade, 2011; Quarshie and Martin-Odoom, 2012; Witty 2017). Correspondingly, Anderson *et al.,* (2013) opine that this never-ending criminal activity that has emanated from West Africa has become

a global issue that affects individuals, organisations, and countries, particularly in Western societies as they are the main target for cybercrime perpetrators.

Equally, like every other part of the African continent, internet facilities and advanced technological gadgets are accessible everywhere, making them an integral part of the government, cooperate institutions, and individual's lives; but the benefits that have amassed from the growing access to technology is being undermined by cyber criminals who are exploiting its capabilities to the detriment of others. For instance, in Ghana the use of the internet has been become significant and has grown tremendously since the liberation of the telecommunication industry in the 1990s (ITU, 2008). All this in spite of the economic quagmire the country has plunged in to and regardless of its status as a developing society. Smartphones provide automatic access to social media platforms where cyber criminals can dupe people. Others who may not be able to afford smartphones venture into attending cybercafés to carry out their nefarious act. All of these provide the leverage for scamming in Ghana, which was code-named 'Sakawa'. According to Ezebuiro (2018), it is a renowned practice in Ghana which depicts, "modern internet-based fraud practices with traditional Akan religious rituals". 'Sakawa' is the preferred name for locals compared to the nomenclature 'cybercrime'. It is well known in the country, to a degree that even kids can quickly decipher that it simply means cybercrime. It is a scheme which was code-named to mean online scamming, phishing, hacking, and engaging in an illicit relationships and illegitimate business forums. There are several pages on Facebook and other social media platforms helping cybercrime thrive with fake identities, the trading of fake skills, and another criminal acts. A bank account is employed, traded, and sold out to the fast-track criminal community. Scamming in Ghana and many other African countries has been linked to the alarming rate of unemployment and economic hardship.

Cybercrime in Ghana has grown in leaps and bounds, it has metamorphosised into a higher degree of criminality. This is not limited to Ghana, it has also increased in Nigeria, South Africa, and other parts of the world, including some developed countries of the west. The 'Sakawa' boys of Ghana do not succeed only with their combination of wits, persuasion, subtlety, expertise, and intelligence, which are the normal characteristics of internet scammers; they also use some kind of 'abracadabra', 'juju', or 'voodoo' (Ezebuiro, 2018). It has degenerated to the extent that everyone sings about them, and they live a life of affluence and ostentation. Brenner (2007) opines that Ghana has the highest rate of cybercrime in Africa. As part of an effort to curb internet crime, Kirk (2018) opines that Microsoft's Internet Safety Security and Privacy Initiative for Nigeria came with a song in conjunction, with the song starring Banky Wellington. He submits that Microsoft and Nigeria have released a song and video as part of a campaign to dissuade people from getting involved in cybercrime with the caption 'Maga need no pay', which means victim do not need to be parting away with their hard-earned money to jobless ones, but rather hard work pays.

People, stakeholders, government agencies, parastatal, and ministries are investing heavily in information and communication technology at an extremely high pace based on the sophistication of various countries. Worthy of note is that there is more to network infrastructure security than the initial implementation of the system, upgrades and ongoing maintenance must be taken into account. The financial institutions and banking organisations in Africa believe they are committed to cybersecurity and having mechanisms put in place to prevent fraudulent activities and guarantee great security and protection of customers' investments, savings, and transactions. Lately, with the increasing wave of cybercrime, financial experts are discovering that their institutions are losing billions of dollars to organised cybercrime syndicates across the globe (Okochu, 2017).

Forbes (2010) and the New York Times (2015) created a related documentary on business

security in Africa and submit that online businesses in Africa are vulnerable to cyber-crimes or online attacks. The great continent of Africa is in dire need of repositioning of her online cyber security in terms of awareness, training, retraining of users, workers, law agencies, and other stakeholders in order to fight cybercrime head-on. It is argued that Africa is becoming a breeding ground for such social vices, for instance, Nigeria is ranked as the leading State in the region as a target and source of malicious internet activities, and this is spreading across the West African sub-region (Ribadu, 2007; Mazzitelli, 2007). Egypt is also reputed to be one of the most phished countries in the world, with about 2000 phishing incidents, followed closely by other countries such as South Africa (Ojedokun, 2005), and more recently, Ghana.

In the same vein, the growth and development of international banking, as well as money-laundering, has made Africa as a continent a source of money and is much-flaunted as a target for criminal acts. The rapid progression of transferring and ferrying cash electronically in a nascent banking system, which is mostly anonymous through a tangled means, has propelled cybercriminals in their ability to see areas of attack and loopholes as well as strategise how to cut their shares (Viljoen, 2007). Online banking has provided a clear ground to wire illegitimate cash without concern of getting caught in the web of criminalities. There abound are renowned cases of money laundering in Africa. According to Ojedokun (2005), there are many well-known online money-laundering cases involving victims in Africa who were tricked, having their identities stolen or transferred out of their accounts through phishing and fraud.

Also, the reservoir of information online allows criminals to thrive. People learn about the 'job' of cyber criminality. Hence, hackers have all they need at their beck and call, this allows them to be able to launch attacks easily (Ribadu, 2007; Paganini, 2013; Olugbodi, 2010). Africa is also suffering from a lack of great internet-specific laws. There are little to no regulations for the use of internet facilities. Everyone is just thronging on the net to get

information, data, and knowledge, as well as organise crises. Policing without legislations is a shared waste of time (Olugbodi, 2010). A few countries on the continent are trying to shape new legislation and legal definitions for cyber-crime, such as Botswana, Egypt, Lesotho, Mauritius, and South Africa, but there is still a need for more specific laws for cybercrime activities. Over ten years ago, a bill was sponsored on the floor of the House of Representatives in Nigeria titled the Nigerian Computer Security and Critical Information Infrastructure Protection Bill. In 2005, the Bill was submitted to the joint body of the National Assembly but has not been passed to law. In the same vein, countries with some relatively strong rules and regulations have created a framework for internet-related issues but lack the power to tackle international internet crimes head-on. It has no locus standing to combat the cybercrime phenomenon. Even in Nigeria, limitations are compelling on the search, arrest, prosecution, and punishment within the territorial integrity of the country without interfering with others (Olugbodi, 2010).

The South African Electronic Communications and Transactions Act of 2002 hardly holds water as cyber inspectors are weak in their ability to search, arrest, detain, and interrogate cybercriminal masterminds within their territorial and geographical jurisdiction (Okochu, 2017). Due to the style of criminal justice and law enforcement techniques across most countries in Africa, mainly Burkina-Faso, Gambia, Ghana, Kenya, Senegal, and Zimbabwe, using emergency laws and ad hoc approaches instead of establishing ascertainable cyber-crime laws and policies against the phenomenon are cumbersome. Many other African countries embark on the journey of minimal internet monitoring and the blocking of internet violators. Many of the laws enacted, whether regular or emergency ones are not designed to completely deal with cyber-criminal activities because there is no boundary set for them. The parameters are very weak and are declining by the day. Nigeria comes into view as the manifestation with one of the most extra-legal approaches to cyber criminality. Nigerian law

enforcement agencies can sometimes be very irrational, crude, wicked, non-calculative, and shallow in their approach to dealing with civic issues (Ogwezzy, 2012). They are good at fighting symptoms rather than curing the cankerworm that is bedeviling the entire continent. Ogwezzy (2012) opines that a State whose law enforcement and security agencies are yet to fully shed the military culture of repression creates and environment where it becomes routine for police officers and other security agents to swoop on cyber-cafés and arrest all users of the internet without considering that there may be honest and innocent patrons. This is apparently the state of backward and primitive problem-solving that Nigerian and the rest of the continent practices.

Nigeria, as a country, bellies the criminality of some citizen and brutality of some law enforcement agents (Transparency International, 2014; Jude, 2011). A suspect is brutalised and is never afforded the opportunity of fair hearing, or the safeguards of criminal procedures. In a country where an accused person is hardly afforded the safeguards of criminal procedures, the incessant practice of swooping on cyber-cafés has opened further doors for the corrupt enrichment of the police and security agents (Connell, 2000; Olaide and Adewole, 2004; Morgan, 2017). It is crystal clear that both the actions and mechanisms of the police are ineffective and non-sustainable, they may even put innocent ones in jail without a reasonable offence committed. Clear regulations are invariably absent tantamount to weak law enforcement agencies and due to poor training and substandard tools as well as archaic policing techniques. Most countries in Africa do not have specific laws for the protection of cyber-based intellectual property. According to an empirical study, several African States rank high in virus infection (Internet Crime Forum, 2001; Koops and Leenes, 2006). It is a well-known fact that viruses can be spread rapidly, infested files can be downloaded or distributed between internet peer to peer chats or through pirated software. This indicates that the African States also ranks high in cyber-based intellectual property violations and software

piracy. There is an exceptionally low landscape of laws and policies against cybercrime in Nigeria as well as some other African states. The array of inadequacies is clearly shown with the rising cases of criminality and brutality both online and in real-life situations. Apart from isolated pockets of diplomatic interaction at sub-regional levels, such as the one-day meeting of the Ministers of Telecommunications in the Economic Community of West African States (ECOWAS) sub-region in October 2008 (Debora, 2012; Okeshola and Adeta, 2013). There has been an absence of agreed African continental agenda for pooling resources together to tackle cybercrime cooperatively and collaboratively with a pro-active action guide, intervention strategies, and related initiatives. It behooves each African country to fight cyber criminality by themselves and with their weaponry alone, but the era of lone rangers is over. There is a need for a multi-dimensional approach to fighting the nefarious act through collaborative initiatives and support systems.

It is an affirmative fact that able young people in any society are a blessing in disguise, they are of paramount importance and are needed to proffer plausible solutions to personal and societal problems. They are seen as the leaders of tomorrow who are still innocent and without prejudice. However, Olaide and Adewale (2004) observe that a sizeable number of cyber bandits in Nigeria are young and lack the necessary experiences of life. The present-day is rooted and grounded in criminality and rife with fraud that uses the internet as a mechanism in engaging in criminal activities. The great country of Nigeria in current times is referred to as a nation of criminality and absurdity due to the advance free frauds the youth are engaging in. Criminal activities are not particular to Nigeria alone within Africa, or even the world at large. In 2006, 61 per cent of internet criminals were traced to locations in the United States, while 16 per cent were traced to the United Kingdom and 6 per cent to Nigeria (Aransiola, and Asindemade, 2011). Other nations known to have a high incidence of advance fee fraud include the Ivory Coast, Togo, South Africa, Netherlands, Spain, and Jamaica (Cook, 1997;

Internet Crime Forum IRC Subgroup, 2001; Zero Tolerance, 2006; Internet World Stats, 2014).

The number of 419 refers to the section of the Nigerian Criminal Code dealing with fraud, its charges, and its penalties for offenders (Balancing Act, 2014). However, Nigeria is not the only nation where cybercrimes are being perpetrated. The incident can rightly be said to be on the increase in the country due to a lack of infrastructural facilities, economic opportunities, and bad leadership. Nigeria is a renowned hotspot for internet scams. At times, it is termed as an internet scam hotbed. Conversations with career 'yahoo-yahoo boys' reveals that this hustle is in no way slowing down. The Crowd-Strike report said it was commonplace for the fraudsters to have officers of some crime-fighting outfits on their payroll. Here is how another 'yahoo-yahoo boy', who also requested anonymity, described it;

> "You receive the money using accounts. To receive money from overseas, you need accounts to move it around and there are middlemen whose only contribution to a scam operation is providing accounts. Many are in China so when they receive money, they buy goods and export to Nigeria" (Tade, and Aliyu, 2011).

In fact, it is blue-chip companies' international organisations and institutions that are being attacked alone. As a civil society leader who is high and mighty in society, a mover and shaker of nations, and a private business mogul, a high-flying corporation like Nigeria National Petroleum Corporation are new targets of cyber-attacks. Some various strategies and techniques are now being used to infiltrate and cause commotion in government, wreak havoc on institutions, fight surveillance, bully people and organisations online, partake in data and identity theft, and create fake news. Citizen lab (2018) carried out a study and reports tainted leaks showing how civil society groups and journalists critical of the Russian government were obstructed, where cyber-attacks were used to steal or alter information they work with. Another report, by Reckless Exploit (2016), reveals how Mexican journalists and human

rights defenders were attacked with advanced spying software for working on a range of issues that included corruption allegations against the Mexican President and human rights abuses by the government. It is a well-known fact that digital attacks will keep rising in Africa, more money will be lost, and more data will be breached as a result of insufficient internet regulations and security measures. Some governments may decide to stifle social media, freedom of speech, activism, pressure groups, and other heinous actions, through laws, digital surveillance, or spying. However, to curb people's excesses, such as hacking, critical awareness and orientation need to take center stage.

2.4 Cybercrime in Nigeria

At the turn of the 21st century, the widespread use of the internet took a running jump. Whereas the number used to be less than 5 per cent from 2002 to 2003, it stood at over 40 per cent by the end of 2015, and the growth is only poised to accelerate (Radwan and Pellegrini, 2010). According to Adaramola (2018), the introduction of mobile telephones and networks in the Nigerian market has played a major role in the improvement of the nation's economy and opened it up to the 21st century's global life. The Very Small Aperture (VSA) terminal deployments that were once the only source of dependable internet connectivity have since been rendered quaint and antediluvian compared to the untapped capacity of the undersea broadband cable that has been brought to the coast of Nigeria since 2009 (Adeniran, 2008). Over time, various marketing competitions and market forces were playing out in the industry, building, and growing quality as well as running down average consumers to popularise the use and coverage of the internet in Nigeria (Adaramola, 2018). However, the rapid growth of the internet across Nigeria and the global world has had unintended and unimaginable consequences. The nation has achieved global notoriety as a New Haven for criminals in the cyberspace.

Internet fraud has been evolving at a rapid level in Nigerian society. It started from the days of 419, email, and romance scams and is currently in the more advanced form of internet fee fraud. Moreover, the advancement of the internet and high-speed connectivity has given a platform for more individuals to participate in cyber-criminality (Transparency International, 2014; Tade and Aliyu, 2011). The ubiquitous concept and construct of 419 has since been extended and submerged into the criminal world in Nigeria with the street name 'yahoo-yahoo' (Tade and Aliyu, 2011). It has become a household phenomenon that is used to address people who perpetrate scams online and most times live very luxurious lifestyles (Olaide and Adewole, 2004; Oyewole and Obeta, 2002, Olugbodi, 2010; Ribadu, 2007).

The widespread adoption of the internet has brought about two distinct and separate events across the world (Okeshola and Adeta, 2013). Firstly, it has helped in promoting e-business and integrating nations and national economies of the world; it has also increased the rate of ill behaviours or inappropriate social behaviours, particularly crime and especially among the youth (Okeshola and Adeta, 2013). Also, the usage of the internet has exposed many young people to activities related to cyber-crime (for example, 'yahoo-yahoo'), a modern form of internet theft in Nigeria. But the adverse effects of these technological orientations and innovations weigh enormously on peoples' lives, properties, companies' asset bases, and the country's image in the international community as a whole.

In the last decade, cyber-crime has been more pronounced among university undergraduates in Nigeria (Muriana and Muriana, 2015; Tade and Aliyu, 2011). In 2010, a famous centre, the National White Cybercrime centre, in conjunction with the Federal Bureau of Investigation (FBI), reported that Nigeria was ranked as having the 3rd highest rate of cybercrime in the entire world, a phenomenon that is locally known as 'yahoo-yahoo' (Tade and Aliyu, 2013). In a study carried out by Okeshola and Adeta (2013) on the nature, causes, and consequences of cybercrime in tertiary institutions in Zaria, Kaduna Nigeria, it was discovered that a countless

number of crimes are committed daily without apprehension and conviction. These criminal acts include the falsification of documents, identity theft, cyber harassment, killing, bullying, romance scams, automated teller machine fraud, pornography, spoofing, piracy, hacking, phishing, and spamming, among other things. They are usually committed in the form of sending fraudulent and bogus financial details, sending a nefarious email, or helping people at ATM posts. This has become a strong threat to the economy, commerce, and the overall development of the country (Okeshola and Adeta, 2013). Nigeria, as a nation, has been battered, defamed, and demeaned in the international community because of all of these criminal acts (Ade and Aliyu, 2013).

McConnel (2000) submits that cybercrime differs from the most common local crime in different ways. He itemised four major differences as, those being that it is easy to learn, requires few resources to start, it can be undertaken in an area where the culprit need not be, and above all, it is illegal. As such, it has become one of the greatest issues facing law enforcement agencies and the world at large. According to Ribadu (2007), culprits in Nigeria have some forms of cybercrimes they perpetrate that are common among them. These are the cloning of websites, creating fake identity, false internet purchases, and other forms of e-commerce fraud. To this degree, Olugbodi (2010) supports the submission of the Ribadu (2007), he states that the most prevalent forms of cybercrime are website cloning, financial fraud, credit card theft and use, cyber theft, cyber harassment, fraudulent electronic emails, cyber laundering, creating, and distributing viruses, false software and corporate websites, and identity theft, and among other things.

2.5 Understanding Cybercrime's Morph from Computer-based Fraud to Fetish-based Spiritual Sacrifices: The Tale of Yahoo Plus in Nigeria.

In the African context, spiritual things are an important aspect of social reality. Therefore, it is important to enhance our understanding of this social phenomenon. Although spirituality is debated scientifically, the fact that people hold it up as a basis for interpreting social events

makes it a necessary component in African societies (Tade, 2013; Lazarus, 2018). As indicated in literature, most Nigerians, like their ancestors, believe that supernatural powers could be a mechanism to fast track success and wealth. The perception of many Nigerians is that there is a need to receive divine blessings from supernatural beings to be successful in any career path, whether legitimate or illegal. (Akanle and Adejare, 2018). Lazarus (2019) highlights the arguments of distinguished scholars that reflect the general opinion that physical strength and hard work alone do not guarantee success in life, so it is important to understand and possess spiritual powers to achieve maximum success.

Interestingly, the narrative of cybercrime in Nigeria took another swing, some of the perpetrators adopted a new approach of combining spiritual elements with their criminal activities to improve their chances of success in defrauding their victims. These new strategies employed by perpetrators are being referred to as 'yahoo plus' (Tade and Lazarus, 2013:689; 2018). The authors focused on exploring the underlying factors fuelling the spiritual dimension and the techniques used to proliferate internet fraud. In this context, it is understood that cybercrime perpetrators, who are within the local parlance called 'yahoo boys' in Nigeria, have embraced this medium to manifest supernatural powers to defraud their potential victims around the world (Ayotunde and Melvin, 2010; Ibrahim, 2016; Lazarus, 2018).

Conversely, Arasiola and Asindemade, (2011) observe the spiritual dimension of cybercrime in Nigeria; their research explains the use and importance of voodoo (traditional power) to achieve the anticipated goals of the perpetrators. Their research reveals that 'yahoo boys' in Nigeria believe in the popular perception that spiritual power is needed for success in all ramifications of life, hence, they believe there is a need to use voodoo and mystical powers for spiritual protection and to cast spells on their victims, which they describe as 'yahoo plus'. The activities of the 'yahoo plus' enterprise was discussed in detail in their study, which reflects

that ‘yahoo plus’ entails the use of human parts, incisions on their bodies, spiritual finger rings, and sleeping in a cemetery, the purpose of this is to fast-track success.

Following from the above, scholars have argued that cyber spirituality is not a new phenomenon, it has been in existence before the introduction of technology, and hence, there is a historical narrative to this. According to Igwe (2007), in the 1940s before the integration of technology into everyday life, colonial leaders described the money doubling activities of a group of Nigerian youth that were vicious manipulators. Their primary agenda was to trick and defraud victims from western society with scam letters. This heinous activity was successful due to their deep collaboration with native doctors (*Babalawo).* Equally, Nkoh (1963) opines that the money doubling phenomenon has always been connected with diabolical powers. Also, some of the studies conducted by Aransiola and Asindemade (2011), Ajirola Ibrahim (2016b), and Lazarus and Okolorie (2019) completely reflect the spiritual extent of cybercrime in Nigeria. Other scholars whose studies reflect and expatiate on this phenomenon include Tade (2013) and Ayotunde (2010).

In the same way, Lazarus (2019; 2018) avers that, in recent years, most of the victims of romance scams are typically defrauded because of their desperation to find love, therefore, it becomes easier for ‘yahoo boys’ to cast a love spell on them. Equally, (Whitty *et al*., 2017) opines that people who are liable to be victims of romance scams are those who attempt to seek true love and perfect partners. However, this speculation does not appraise the effectiveness of charms *(Oogun*) and other supernatural powers in romance scam victimisation. In the case of cybercrime perpetrators, ‘yahoo boys’, they manipulate their clients (victims) with distinct types of spiritual powers, indigenously known as ‘African Jazz’ (Lazarus, 2019; Information Nigeria, 2017; Ajirola, 2015). These supernatural powers include placing a spell on the victims' photographs or names with the assistance of a spiritual personality (*rogues babalawo,* pastors, *Alfa* etc.*),* depending on their beliefs and religions, while they continue to communicate with

their victims (client) via emails, phone calls, and other mediums of communication that have been established between them through 'words of power', traditionally addressed as *ma ye hun'* (Do as I say). These spells incorporate the use of verbal axioms that enormously open forces that can enable the spirit to manifest itself in the physical realm (Peavy, 2016). This is an indication that victims do not fall in love naturally; rather it is considered as an affection that is being facilitated by fetish means because they do not have a choice and cannot consider what the proposed love is, which innocently leads them to be commanded and they do as their lordship pleases.

Spells can, therefore, be invoked by words of power or rhetoric prepositions, depending on what the invokers aim to achieve. For instance, *ma ye hun* (words of power) can be invoked to intensify economic benefits if the client (victim) proves to be adamant. Tade (2013) identifies important factors that have promulgated the rapid involvement of charms in cybercrime in Nigeria, especially in the aspect of romance scam victimisation. Firstly, there is massive media awareness on all social media platforms to educate people about the strategies and mechanisms of the activities of scammers online, as a result, these people's engagements online are reduced and there is a delay in success. Following these challenges, a new approach emerged within the local parlance of Nigeria popularly called 'yahoo plus', the purpose of this is to fast-track economic success through spiritual means. However, this experience is the amalgamation of the use of charms or 'juju' while surfing the internet, particularly online dating websites, in the hope of meeting unfortunate victims. This may be related to the popular *Yoruba* adage: *"e ni ke ni to ba maa je oyin inun apata ko ni wo enu ake" (*whoever what wants the honey inside the rock will not be bothered with the mouth of the axe*).*

Nigerian cybercriminals ('yahoo boys'), who are usually youths, have pushed aimlessly to combine spirituality with cybercrime for success. Tade (2103) describes these activities as cyber-spiritualism. Though, the narrative that surrounds cyber-spiritualism has

metamorphosised into money rituals, which has become bloodcurdling because most youths in Nigeria are believed to be involved with money rituals while hiding under the charade of ‘yahoo-yahoo’. Damilola Ismail reported in Laila news (2019) that so many ‘yahoo boys’ have made the change from scamming people online with their intellectual capacity to involving rituals and killing individuals. The article reveals the extent to which ‘yahoo boys’ are involved in money rituals to maintain social status. Nigeria is currently overwhelmed by many insecurity challenges because of the Boko Haram crises in the Northern part of the country over the years, which is only perpetuated by the new wave of ‘yahoo plus’ rituals and undertakings, which has all pushed the social life of the country to the brink of meltdown. Nearly every day a new facet of ‘yahoo plus’ activities make headlines in the news. To Illustrate, a suspected ‘yahoo boy’ ran mad, confessing to having used his father for money rituals because he wanted to live a flamboyant lifestyle by driving in the latest Mercedes Benz (Pulse, 2018).

Unfortunately, money ritual killings are quickly turning into a prevailing trend in Nigeria. Many have ascribed to the disintegration of the value system of the country, which unexpectedly appears to have given rise to money becoming a god-like entity the youth adore. Therefore, money rituals are becoming the new antics ‘yahoo boys’ have adopted to get rich quickly. The modus operandi for these activities includes the killing of human beings, stealing of ladies' underwear, and sleeping with corpses. Some of the alleged suspects apprehended by the police confessed to the aforementioned activities (BBC Africa, 2019). In the same vein Lawani and Osagie-Obazee (2019) reported some of the headlines on ‘yahoo plus’ activities in Nigeria; “Yahoo Ritualist Caught with 12 Soaked Sanitary Pads” and “Female Underwear; Fear of Ritualists in Delta: We Anoint Our Pants to Escape” (Okogba, 2018; Amaize, 2018; Lawal, 2018; Ewubare, 2018; Egobiambu, 2018; Young, 2017). This deleterious act is an indication that the Nigerian youth do not appreciate hard work and institutionalised means of

achieving success, rather they are involved in cybercrime and see money rituals as a way to become millionaires overnight.

Propping the above exposition, cyber spiritualism has become a paradigm shift from the well-known ‘yahoo-yahoo’, through which most activities depend exclusively on the use of the internet to victimise innocent people. Nevertheless, the amalgamation of spirituality and cybercrime has proven that intellectual capacity alone cannot produce results, as is the case in numerous campaigns, and people are becoming more educated about the modus operandi of ‘yahoo-yahoo’, which has hence thwarted cybercriminals. This has caused cybercriminals to embrace the innovated spiritual rudiments into cybercrime, leading to the materialisation of ‘yahoo plus’ in Nigeria.

2.6 Fundamental Factors and Motivations Behind Cybercrime Perpetrators in Nigeria

The motive behind criminal activities is astonishing. According to Yar and Jwekes (2010) and Aransiola and Asindemade (2011), the fundamental reasons why some youths are persistently engaged in cybercrime and nefarious the infiltration, destruction, and gaining unauthorised access to networks and computer systems are traceable to the massive amount of monetary gain and increases in societal status. Also, the use of telecommunications via the cyberspace continues to thwart global efforts targeted at tracking criminals and bringing them to book; the likelihood of not been able to identify cyber criminals when they have perpetrated their illegal activities continues to be a motivation for them to persist in their criminal activities.

Also, Wall (2013) advocates seven motivational factors for youths engaging in cybercrime, these include self-satisfaction, earning peer respect, commercial gains, criminal advantage, revenge, and distance from the victim, as well as political motivation. These motivational factors depict that cybercrime is vast and cybercriminals employ dynamic approaches. Of great importance is the fact that cybercrime is revealed by their titles and nomenclature. The value of this grouping is most evident in the criminal gain or commercial advantage and politically

motivated categories. For example, whilst some types of cybercrime, such as cyber extortion, cyber fraud, and cyber embezzlement, fit squarely under the canopy of the former, cyber espionage, cyber terrorism, and cyber rebellion, can be located smoothly in the sphere of the latter.

Ibrahim (2016) deeply researched the social and contextual taxonomy of cybercrime and the socio-economic theory of Nigerian cybercriminals. His study aimed to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. The study relies upon a basic principle of categorisation alongside motivational theories to offer a tripartite conceptual framework for grouping the cybercrime nexus. It argues that cybercrime is motivated by three possible factors, those being socioeconomic, psychosocial, and geopolitical. Whilst this contribution challenges the statistics relied on to inform the prevalence of cybercrime perpetrators across nations, it provides new ways of making sense of the voluminous variances of cybercrime. Concomitantly, it enables a clearer conceptualisation of cybercrime in Nigeria and elsewhere because jurisdictional cultures and nuances apply online in the same way they do offline.

Kerstens and Stol, (2012) claim that young people make use of neutralisation techniques when they talk about cybercrime as a fundamental assumption and the motivating factors in engaging in crime. Such language includes phrase like, “everybody does it” or, “it's normal to do so” when referring to virtual theft, or “to bring malpractices to the forefront” as a reason for hacking. Secondly, young people downplay the criminal aspects of cybercrime as they think or do not know that something is punishable or think that there is no police investigation taking place into this form of crime (low probability of detection). And above all, they found evidence for the role of disinhibition among young people regarding their reactions of others on the internet which are often delayed and asynchronous, which makes young people think that their criminal actions online do not have any harmful effects. Besides this, the interviews

revealed that young people often take on another name online, which sets the stage for experiencing dissociation; they do not ascribe the criminal actions to themselves anymore, they perceive it as a game.

In the same vein, competitors provide a boost to cyber criminality either by sponsoring attacks on one another or through spying and espionage to steal critical information relating to trade secrets or the paralysis of competitor's services through Distributed Denial of Service (DDoS) attacks. Some schools of thought submit that cybercrimes are not solely committed for the sake of money or pecuniary advantage but are driven purely by satisfaction through intrinsic motivation. Criminals derive pleasure in gaining unauthorised access to people's computers, data, and networks. The mere fact that cybercriminals gain porous and unhindered access to an individual's, government's, or institution's computer system is like adding a feather to their cap, they see that what the owners claimed to have maximum security on has been jail broken by a so-called expert, revealing their vulnerability serves as intrinsic motivation for them. Jwekes, (2010) simply believes that they are antagonists to the use of computer systems, this led to the outward manifestation of a registration of disagreement or disapproval against owners or operators. This form of motivation is also often aimed at getting profit out cybercriminal activities.

There is a countless number of cybercrime consequences; these include a loss of intellectual property and sensitive data, opportunity costs including services and employment disruptions, damage to a brand's image and company's reputation, penalties and compensatory payments to customers (for inconvenience or consequential loss), or contractual compensation (for delays, etc.), costs of countermeasures and insurance, costs of mitigation strategies and recovery from cyber-attacks, the loss of trade and competitiveness, distortion of trade, and job loss (Paganini, 2013). Cybercrime continues to thrive because of a failure to increase awareness among individuals so that they can protect themselves and avoid being victims.

Worthy of note is that most people are gullible and are ignorant of how to prevent being a victim of Self-Crusading Financial Reparation Agenda for Prolonged Slavery and Colonialism in Africa

Colonialism is a fact of history, it implied the exploitation of peoples and raw materials (Rodney, 1973). It was the imposition of the powerful. It is a tantalising idol, charming the needy nations for salvation in the guise of a savior. Surely, colonialism is bad for a colony. Different social, political, and economic institutions were controlled and morphed into systems that would suit the colonising agencies and were mostly to the dismay of the natives. It makes the colony a resource field and whatever production is carried out in a colony is geared towards the benefit of the colonial masters, even at the cost of starvation in the colony. Colonialism in any shape and form is not and should not be tolerated, rather it should be cursed because of its deterrent and dividing nature (Omoruyi, 2012). The first principle of all colonising forces is ‘divide and rule’. There are so many unanswered questions regarding the rise against the catastrophic nature of colonialism. History is a good eyewitness and there is no need to lengthen the debate. Colonialism lies behind degraded and exploited natural resources and the loss of self-governance capabilities, national identity, languages, and cultural values. It brings about a divided society, a double standard of treatment, dumping ground for surplus and inferior goods, diseases, and unwanted prisoners, as well as the abduction of some local people to become slaves in the coloniser's countries, etc.

Occupants create a class of privileged peoples who govern the country after liberation. When the occupant leaves the country, they have already made various unsolvable regional issues. The West (colonial) has been hegemonic to all its colonies and there has been no denying this fact. However, the hegemony extended to the realms of language, skill, knowledge, faith, polity, education, social customs, law, medicine, and the arts, among other things. The 19th Century Western colonial forces were convinced of their universalistic models in each of these

above categories, and they were to be imposed on the local and lesser native models in order to create a tendency to see the others as lesser, evil, foreign, or uncivil. This gets worse when one further accepts colonial systems and institutionalises them. Colonisation needs to be checked as an aberrant code that has the potential to disrupt the varied worldviews of different people. To ask for justification of colonial excesses could be penny wise but pound foolish. However, there is a notion, which lacks empirical evidence, that scamming the Europeans was a way to get back at them.

Criminality and colonialism may be separable concepts, but many youths in west Africa, particularly Nigeria have termed it as an avenue to get back at their colonist. The evil perpetrated by colonist is seen as needless and unwarranted (Ayitey, 2010), where African resources, both human and material, are carted away unjustly and the resultant effect is where many African countries found themselves today. The economic pillars of development have been dented and the psyche and structure of African traditional settings has been deeply and negatively affected. Colonialism has presented several impediments and constraints that have been ingrained on the feeble minds of the colonised countries in Africa. Riding on this gives some African youth the illegal and uncivilised license to fire back.

Emeka Okonkwo (n.d) opines that, in June 2019, four teenagers were arrested and interrogated for engaging in internet crime where they were swindling European nationals. They submitted that it was a mechanism set in motion to gain revenge for defrauding their forefathers during the colonial era. While some eighteen suspects aged between 18 and 27 years of age were ambushed and arrested by the operatives of the EFCC, Endurance Ahunwan, the chief suspect and the oldest, submits that they were getting back at the colonial whites who cashed and carted away their countries resources even before they were born. The EFCC spokesperson opined that, "Upon arrest, the prime suspect confessed that he recruited the team, saying they were paying back Europeans for stealing from their forefathers". Hence, the nature of

colonialism served to unleash crime into society which has negatively affected the needs, yearnings, and aspirations of the African society (Robbins and Judge, 2009). It has slowed the progress of development in Nigeria as youth are giving in to get-rich-quick-syndrome (Okeshola and Adeta, 2013).

2.7 Societal Embracement of Cybercrime (yahoo-yahoo) in Nigeria and the Prevalence of the Menace

Cybercrime is known as one of the most popular criminal acts in the 21st century. It is seen as the world's social problem that is evolving and napping the feeble minds of the present generation of youths. It has become massive and burgeoning. Government agencies, ministries, and parastatals and corporations and individuals keep on losing large sums of money, valuable data, and information daily to cyber-attacks like phishing, spoofing, social media hacks, ransomware, and data theft. Zakariyya (2018) opines that though greed, desire for money, and sexual innuendoes give many Nigerians away to cybercriminals, internet scammers have their antics with which they catch their victims. Studies have shown that cyber criminalities are massive in the western world, forgetting the fact that the world is now a global village, wired and interconnected together to share resources, information, and data as well share in the liability and pains thereof.

Hence, cybercrime perpetrators are not particular to the western world alone but the entire interconnected web of geographical and political zones in their entirety. Cybercrime is global as long as there are internet facilities in the regions or countries and jobless youths. A person who has access to a computer and is connected to the internet might be participating, attempting, or planning a criminal act anywhere in the world (Kumar, 2003). Awe (2009) confirmed that computer attacks can be generated by criminals from anywhere in the world, and executed in other areas, irrespective of geographical location. And often these criminal activities can be faster, easier, and more damaging with the use of the internet. With the above

assertions, cyber criminalities are a global phenomenon. However, in Nigeria it has become a nightmare, thereby both the government and its citizens are sitting on a metaphorical keg of gun powder. The remote and immediate causes, as identified above, must be statistically and qualitatively traced, and examined, thereby leading to the acquisition of a plausible solution to the cankerworm.

In Nigeria, cybercriminals are popularly referred to as 'yahoo boys. They are taking advantage of e-commerce systems available on the internet to defraud, bully, spy, and steal vital information and documents, thousands of dollars are taken from their victims which are mostly foreigners. Cybercrime perpetrators dupe victims with the fake identity of either a businessman, government official, or person high and mighty in society to scheme and dupe them out of their possessions. Their mode of operation sometimes suggests they have loan scheme or financial institution where money can be given out with little or no collateral. In this regard, so many persons have been duped or fallen victim. However, there are countless other methods employed by cybercriminals in duping innocent minds. Every trick and measure put in place by Government to curb excesses have not been met with great success as the identities of cybercriminals remain silent, hidden, and inadequate. A study by Zero Tolerance (2006) indicates that cybercriminals are usually within the ages of 18 and 30 years and they indulge in the crime to survive and have a taste of the good life. With these revelations, there is a need to fashion out more characteristics that are particular to cybercriminals. The core rationale for engaging in cybercrime must be known, assessed, and combated. The motivating factors for engaging in cyber criminalities must be killed. Nigeria's Economic and Financial Crime Commission (EFCC) has recorded great success in the quest to ending cybercrime in Nigeria. The commission has dissipated energy and increased efforts to stop internet scams, but perpetrators are numerous and highly organised. Zakariyya (2018) made an assertive statement on cybercrime and the root causes which are linked to societal

acceptance and embracement of internet scams through body language, culture, songs, street slang, belief systems, and a poverty mentality of getting quick money without respect for labour. In his words, "419 scams have taken root in Nigeria's popular culture, Scammers enjoy a rebellious, 'cool' mystique, even producing songs and music videos that celebrate their audacity". Based on this, there is a need for a paradigm shift in the thinking style and pattern of living in the society which has been enmeshed with criminality.

According to Emmanuel (2019), entertainment has become a new investment that is trendy and causing waves. A countless number of teenagers and adolescents are aiming to become the next superstars, without due regards for diligence, education, reverence to God on their career, and destiny. They want to live big without looking inward to think big. They are fantasising of being young, famous, and successful without due respect for the dignity of labour. They cannot get enough of the fantasies of being young, famous, and successful, like living luxuriously as flaunted by popular musical artists. However, some of these celebrities are being followed and mentored through the acts, lifestyles, and posts on social media platforms. Adolescents and teenagers are technically being directed and guided by some celebrities with no track record.

Over four decades ago, legendary Afro beat Musician, Fela Anikulapo-kuti, employed his music to curb citizens' nefarious acts but the reverse is the case with current crops of musical artists whose works indirectly encourage criminality at best. Just very recent is the Naira Marley saga, with his hit track "am I a yahoo boy", and not quite long is that of Olu maintain "*yahoozee na* music". All of these and many more are indirect ways of celebrating cybercrime and illegality in society. Entertainment is an avenue to practice, exhibit, explore, and express talents in various ways but this should not be at the detriment of an already rotten society. Only very recent are celebrities like Falz, MI, Simi, Ruggedman, Soundsultan, and Banky W are rising to the occasion of combating crimes of many forms through their music, videos, skits,

social media posts, and utterances. The campaign burgeoning and aims to label ‘yahoo-yahoo’ and other fraudulent activities as things that should be condemned in society. Olupohunda (2019) opines that the Nigerian street sensation, Naira Marley, submits in its totality that internet fraud is not as bad as is being preached. He proceeds by saying that the activities of ‘yahoo boys’ are retributive actions targeted at paying back western people for colonising Africa. This simply implies that the ace singer considers cybercrime and other related internet activities as the nemesis of the western world and an acclaimed way of getting back at the white colonial masters.

By every standard and measure, fellow musicians Ali Baba, Ruggedman and Falz Simi Gold have refuted such claims by claiming that there is no justification for cybercrime. Ruggedman particularly opines that the entire black race should not be dragged into the gory scenario internet crime. In fact, the activities of cybercriminals have cost many young Nigerians their freedom, jobs, and peace of mind. Ruggedman submits that, if they wanted to scam anyone in the first place, it should be Nigerian leaders. From his perspective, most Nigerian leaders were looting trillions of Naira, and that duping them of this money and giving it back to the poor masses would mean going the way of Robin-hood, and this would be embraced more (Olupohunda, 2019).

2.8 Financial Impingement of Internet Fraud in Nigeria

According to ICAR, and Clab (2016), Action Fraud UK (2014), and Forbes Today (2018) the massive prevalence of fraudulent activities in the financial world is shocking, demeaning, violent, and unwarranted. Whenever issues regarding financial fraud and improprieties are raised, what comes to mind is direct financial loss and porous security measures. On a yearly basis, millions of dollars are being lost in the financial-cum-economic sector, e-commerce, and telecommunication sectors due to fraudulent practices. These acts are not only particular to the United States of America alone, where online payments are the order of the day. In the

European market, according to data from July 2016 in Great Britain, one out of ten people fall victim to online theft or crime. In other words, an individual is 20 times more likely to be stolen from in the comfort of their home in front of a computer than they are walking down the street. Also, the increase in the use of mobile phones for financial transactions and online purchases has not gone unnoticed. In the last Clab, held in Peru in September 2016, the most recent data regarding mobile fraud was reported; it has increased 170 per cent from the previous year and now represents 62 per cent of all online fraud. Of this, identity theft represents 95 per cent of attacks and is one of the most common cybercrimes, along with phishing and hacking.

Loss of reputation is part of the security issue that directly affect a company's brand and reputation. When a company's security is distorted, it may decline a client's partnership and patronage. Investors and business partners may want to decline to do business with such organisations.

Following suit is a loss of client trust. Security is of paramount importance and extremely critical for customers of financial institutions. When there is online fraud which affects a financial institution, and if it is in the public domain, the perception of clients who are solely depending on such institutions to provide them with the maximum guarantee of security regarding properties and documents declines significantly when there is evidence of financial fraud. Even when clients have not completely lost faith in such financial houses, there is evidence of crash sales and relationship to the wider world because the trust would have been battered and wounded, thereby leading to low patronage. In the same vein, when fraud arises in the form of online payments to a third party, studies indicate that a high percentage of the clients consider the financial institution to be responsible.

To curb some of these issues, security audits are required for all companies that store classified data. For financial institutions, data and information is a charitable asset that requires a high

level of security. Hence, there need for audit work every two years to assess and block loopholes because any attempt to avoid audit may spell doom for such institutions as data might have been stolen or there may be unauthorised losses, alterations, access, or the mishandling of personal data and other valuables.

Considering the challenges discussed above, there is a likelihood of a loss of income, which is inimical to the profit of such an institution. For blue-chip financial institutions, the loss may be somehow absorbed while in some small companies it may lead to their total breakdown. It may serve as the end of the journey. Cybercrime and other fraudulent activities have greatly impacted the financial sector far beyond the immediate loss of income.

2.9 Nigerian Legislative Framework Response on Cybercrime

More can be said in support of stressing the necessity to integrate ethics and law in controlling the activities that occur in the cyberspace. This is essential to combat the growing threat of cybercrime, which has seeped deep into the fabric of society and must be addressed. Information technology revolution has transformed the world into a global village, benefiting every field and sector of society, including the economy, trade, social services, and education. Nonetheless, despite the benefits, the society is under jeopardy from the growing tendency of cybercrime. Arguably, cybercrime thrives due to a lack of a universal legal framework and jurisdictional constraints that make bringing cybercriminals to justice difficult. In a scenario someone commit a fraudulent activity in Nigeria against their victim in another country, even though the perpetrator is in Nigeria, will the perpetrator face punishment under the international law; this raises the question of which jurisdiction deal with cases in this kind of scenario. This difficulty has intensified the illegal activities of cybercrime around the world, particularly in Nigeria, where they have increased because of many factors. In the light of this, this section will delve into the legislative framework response on cybercrime and the challenges faced by the criminal justice system in combatting the menace.

2.9.1 *Nigerian Criminal Code Act*

The Criminal Code Act is a British legacy that predates the internet era and understandably does not specifically address cybercrime. The Criminal Code Act criminalises any type of stealing of funds in whatever form, an offence punishable under the Act. The most renowned provisions of the Act regarding cybercrime are Section 419 and 421. Section 419 provides as follows:

> "Any person who by any false pretense, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and it liable to imprisonment for three years."

However, Section 418 defines pretense as any representation made by words, writing, or conduct of a matter of fact, either past or present, in which representation is false in fact and which the person making it knows to be false or does not believe to be true. Section 421 of the criminal code states that,

> "Any person who utilising any fraudulent trick or device obtains from any person anything capable of being stolen, or to pay or deliver to any person any money or goods or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanor and is liable to imprisonment for two years. This offence is also known as the offence of cheating."

The practice of online scammers fits snugly between the elements of the offence under section 419 of the Criminal Code Act, cited above, which has been used for years by the Nigerian law enforcement agencies for the prosecuting of the alleged acquisition of property by pretense. While the offence is specified in the Criminal code Act as a misdemeanor that is punishable with three years of imprisonment, it is utterly untidy for the prosecution to continue to file charges on acts relating to cybercrime offences with municipal laws which have no nexus to

cybercrime offences as it is ill-suited for cyberspace criminal governance. The offence of internet fraud is different from municipal and basic fraud offences (Justin, 2012). The crimes related to internet fraud consist of the basic ingredients of municipal fraud offences and also contains input manipulations, where incorrect data is fed into the computer or by program with manipulates data and causes other interferences with the course of data processing, with financial and personal benefits as an underlying motivation (llievski and Bernik, 2013). This is however different from basic fraud offences as can be seen from the definitions proffered above in section 419 of the Criminal Code Act 1990 (Mohamed *et al.*, 2015).

2.9.2 *The Economic and Financial Crime Commission Act*

The Economic and Financial Crimes Commission (EFCC) Act 2002 established the Economic and Financial Crimes Commission (EFCC) to halt all economic and financial related crimes in Nigeria. The Economic and Financial Crimes Commission (EFCC) Act 2002 was repealed by the Economic and Financial Crime Commission (Establishment) Act and was adopted in June 2004. The EFCC has been mandated by its establishment Act with special powers to investigate any person, corporate body, or organisation who has committed any Act relating to Economic and Financial Crimes. Section 7(2) of the EFCC Commission (Establishment) Act 2004 equips the Commission with the responsibility of enforcing the provision of:

(a) The Money Laundering Act 2004; 2003 No. 7 1995 No. 13 (as amended)
(b) The Advance Fee Fraud and Other Related Offences Act 2006
(c) The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended.
(d) The Banks and Other Financial Institution Act 1991, as amended
(e) Miscellaneous offences Act
(f) Any other law or regulations relating to economic and financial crimes including the criminal code or penal code.

Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

(a) The investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, and contract scams, among others.

(b) The coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority.

(c) The examination and investigation of all reported cases of economic and financial crimes to identify individuals, corporate bodies, or group involved.

(d) Undertaking research and similar works to determine the manifestation, extent, magnitude, and effects of economic and financial crimes and advising the government on appropriate intervention measures for combating them.

(e) Taking charge of supervising, controlling, and coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney General of the Federation.

(f) The coordination of all investigation units for existing economic and financial crimes, in Nigeria.

(g) The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995.

(h) The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended.

(i) The Banks and other Financial Institutions Act 1991, as amended, and Miscellaneous Offences Act.

The Act further gives a broad meaning for the phrase, “Economic and Financial Crimes”, in section 48, meaning that it includes:

> "The non-violent criminal and illicit activities committed with objectives of earning wealth illegally either individually or in a group or organised 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 practice, illegal arms dealing, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of the ceremony, theft of intellectual property and privacy, open market abuse, dumping of toxic waste and prohibited goods, etc."

This elucidation covers a few cybercrimes as manifestly seen in Nigeria. For example, internet hacking.

2.9.3 Advance Fee Fraud and Other Fraud Related Offences (AFF) Act

Another source of Law is the Advance Fee Fraud and Other Fraud Related Offences Act, 2006. This Act replaced the Advance Fee Fraud and Other Related Offences Decree No. 13 of 1995. The Act is the first law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybercafés, it does not deal with the broad spectrum of computer misuse and cybercrime.

The Act punishes "advance fee fraud"[2] (419).[3] The Act prohibits, amongst other things, cybercrime, and other related online frauds. The actions prohibited under the Act include obtaining property by pretence,[4] use of premises for fraudulent activities, fraudulent invitation

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

[3] 419 originates from section 419 of the Nigerian Criminal Code Act, cap.77 Laws of the Federation of Nigeria, 1990 and it is the first Nigerian criminal statute to punish the act of obtaining money by false pretence.

[4] Nigerian Advance Fee Fraud and other Related Offences Act, 2006, s.s 1 & 2.

to launder funds obtained through unlawful activity, conspiracy, aiding and abetting. Moreover, the Act also made certain provisions by imposing duties on electronic communications service providers such as telecommunications service providers, internet service providers, and owners of telephones and internet cafes to prevent or halt the use of the internet and telecommunications facilities in the perpetration of advance fee scams. For instance, the Act obliges any person or entity that is providing an electronic communication service or remote computing service, either by e-mail or any other form, to obtain the full names; residential address, in the case of an individual; and corporate address, in the case of corporate bodies, from customers or subscribers. It is an offence for a subscriber, customer, or service provider to not comply with the identifying information requirement. The Act also foists it upon any person or entity who engages in the business of providing internet services, the owner or person in the management of any premises being used as a telephone or internet café, or by whatever name called to register with the Economic and Financial Crimes Commission, to maintain a register of all fixed line customers which shall be liable for inspection by any authorised officer of the EFCC and also to submit returns to the EFCC on demand for the use of its facilities.

2.9.4Evidence Act of 2011

Mostly at play in cybercrime cases coming before courts are electronic and computer-generated documents of various kinds. It is a generic description for certain classes of evidence processed, stored, or derived from computers, computer-based devices, or electronic communication systems. A major characteristic of this class of documents is that, unless printed, they are paperless and contain visible but intangible objects. These include e-mails, telephone records, text messages, digital cameras, mobile phones, letters, or other documents processed in a computer or electronic device or stored in a computer-based storage device (Eboibi, 2011). Before the amendment of the Nigerian Evidence Act, the 2004 Act had no provision to accommodate computer-generated evidence. Undoubtedly the most significant innovation of

the new Act is the provisions on the admissibility and treatment of Electronically Generated Evidence which may provide a welcome solution to this hitherto unsettled aspect of Nigeria's law of evidence.

The Act provides in section 84 for the admissibility of documents produced by computers. Section 84(1) provides as follows:

> "In any proceedings a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question".

Specifically, section 84 of the Evidence Act 2011 is a positive to effective cybercrime prosecution in Nigeria because it recognises the admissibility of the aforementioned electronic or computer-generated evidence in trials and the enlargement of the definition of documents to include computer-generated ones by the Nigerian Evidence Act 2011.

However, the admissibility of the aforementioned electronic or computer-generated evidence in cybercrime trials is subject to the fulfilment of certain conditions. Section 84 of the Act states that, provided it can be established that the document sought to be tendered was produced by the computer from information supplied to it during a period over which the computer was used regularly and functioning properly to store and process information for the purpose for which that document was produced at that particular time, any statement contained in such document shall be admissible as evidence through any fact stated in it of which direct oral evidence would be admissible, in any proceeding.

2.9.5 The Cybercrimes (Prohibition and Prevention etc.) Act of 2015

The Nigeria Cybercrimes (Prohibition and Prevention) Act 2015 is the first Nigerian cybercrime legal and regulatory framework enacted to regulate the activities of persons in the

cyberspace, particularly relating to cybercrimes, in Nigeria (Eboibi, 2015). The explanatory memorandum and objective of the Act encapsulates the true and express intendment of the Act, demonstrating the deterrence theory of punishment. The Act is punitive, and this is a result of the prevailing threat of cybercrime in Nigeria. It provides a legal, regulatory, and institutional framework for the prohibition, prevention, detection, investigation and prosecution, and punishment of cybercrimes and other related matters (Cybercrime Prohibition Act, 2015). Precisely, the Act offers an avenue for cyber security and, consequently, fortifies the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights as well as securing the preservation and protection of critical national information.

2.10 Challenges Faced by the Criminal Justice System and Police in Combating Cyber-Crime in Nigeria

Cybercrimes and other nefarious activities are driven by technology and have shown a great negative effect on people, computer systems, and data networks. They have also evaded traditional local justice strategies put in place by countries of the world to curb its excesses. Jurisdictional challenges and legal hurdles have hampered and handcuffed the way and manner in which its amelioration is undertaken. Challenges have been identified from various stakeholders of criminal justice in responding to Cyber Economic Crimes. Technical, operational, legal, and human resources are the main four areas where challenges are faced whilst in terms of combatting cybercrime (Godara 2011). Based on the existing facts, corporations, blue-chip companies, organisations, nations, and private individuals have begun to play a key role in debarring the activities of evolving cybercrimes. There countless numbers of challenges faced by the criminal justice system in combating internet crimes and fraud. One of these challenges has to do with the enforcement of cyber laws and policies. Bearing in mind, various principles guiding each independent country, such as the separation of power, rule of law, sovereignty, territorial integrity, and lots more, every country of the world has the

democratic, legal right to make laws for their respective states without fear or favor. Based on this assertion, countries make different laws, enact rules, and pronounce regulations from various backgrounds and with diverse peculiarities, issues, and prejudices. Hence, there is a conflict of law as well as the segregation approach to global issues and problems like cybercrime and its nefarious acts. An inability to apply one law to try a cyber-criminal of international standard causes a problem.

Jurisdiction implies that a court of competence stature can only entertain any actions, petitions, and proceedings, as well try any criminals, within the ambit of the law in terms of its area and power adjudication. Furthermore, jurisdiction encompasses many facets. Hence, the biggest concern to stunting cybercrime is the geographical and power constraints of a justice system's jurisdiction (Miquelon-Weismann, 2005). It is geographical when it addresses fundamental issues in the context that a court has the power beyond the territory where it situates. It is jurisdictional in persona when a court is empowered to hear and determine a case of a cybercriminal outside of its jurisdiction. Seeing cybercrime at its best, one cannot rule out the fact that cybercrime is in a class of its own. It is technically different for other forms of local crimes; it is particularly different in quantum and its effect is felt by the victim. To make it expressly clear, cybercrime in its pace and magnitude is an international crime that goes beyond states and jurisdictions. Cybercrimes cross borders and is considered transitional crime as cybercriminals may sit in the comfort of his or her home, office, or cybercafé using their system, laptop, palmtop, modem, or other computer accessories which are connected to the internet to carry out their nefarious activities miles away without anybody knowing what has transpired. The ubiquitous nature of cybercrime and its pervasiveness has been aptly expressed in clear terms. Sierber (1997) opines that the availability of information and communication systems in the modern world has made it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for

face-to-face conversation before acts of illegality take place because any unlawful action, such as computer usage, technology adaption, and internet manipulation, is capable of having a long and immediate effect on people, data networks, and computers in other countries. In summary, a jurisdictional challenge to the proper enforcement of cybercrime laws is that if the hurdles of anonymity are removed and cyber activities are clearly defined, with criminals residing in the same country, then judicial laws and trials can be highly effective to deal decisively with such social miscreants. According to Miquelon-Weismann (2005), the court and judges may not be able to function effectively if cyber criminals are international as there should be respect for other's countries' laws and policies. Succinctly, extradition and repatriation are fraught with their own challenges due to double criminality requirements, especially where there is not an extradition treaty or mutual legal assistance treaty in existence between the requesting state and the state having custody of the criminal.

From a technical point of view, there are countless numbers of challenges debarring a strong judicial fight against cybercrime. According to Nicholas (2008), there is a lack of Information Technological Infrastructures and facilities. Nearly all stakeholders in the criminal justice system do not have adequate and advanced training in information technology hardware and software. Cyber forensic equipment for the sake of investigation and evidence analysis is lacking at police establishments and forensic laboratories. The quality of investigations is impacted adversely due to a lack of tools and technology. Also, Paganini (2013) opines that there is a challenge in the anonymity of the internet. Anonymity is the dominant feature of the internet, and this encourages criminal behaviour. This also creates a significant hurdle for the investigation agency in their bid to trace, locate, and identify the accused. It has been rightly noted that the internet has become a conduit for criminal activities due to its anonymity (Wall, 2010). There is also the issue of the dark web and illegal trade. Heinous crimes in the physical world have now been shifted to the cyber world due to fast-paced, encrypted communication,

anonymity, and its global reach. The dark web uses a browser like Tor, which makes the tracing nearly impossible for investigation agencies. Due to technical hurdles, it has become a challenge to stop the illegal activities on the fark web for law enforcement agencies. Kumar (2003) elucidated another challenge faced by the criminal justice system in the fight against internet fraud. There is encrypted and peer-to-peer communication. Internet applications like WhatsApp and Telegram provide fast and encrypted communication. Hence, to trace and recover such communication in crimes is particularly important but, due to technical problems, it not possible. This challenge has kept many crimes undetected. These applications have now become the primary tools of communication for criminals.

Succinctly, there are also legal challenges to the fight against cybercrime. There is a jurisdiction issue. Cybercrime is a borderless crime (McConnell, 2000; Ogbuoshi, 2006). The virtual world does not recognise physical boundaries. Anyone from anywhere can commit a crime anywhere, this is the unique characteristic of cybercrime. Due to this problem, deciding the jurisdiction of the crime is an overly complicated issue for the criminal justice system. In the virtual world, the victim may be in one state, the IT set up maybe in another state, and the criminal may be in the third state. In such a situation locating the correct jurisdiction for prosecution is challenging. The United Nations agency has also conducted a detailed study of cybercrime and identifies jurisdictional issues as a major challenge. It has suggested the development of model provisions for fixing the jurisdiction of cybercrime to provide a common base in all countries (United Nations Office on Drugs and Crime, 2013). The government of India has acknowledged the problem of jurisdiction and is creating a common portal as per the Supreme Court's direction for reporting cybercrime (Ministry of Home Affairs 2018). This should also be replicated in Nigeria.

There are also no legal provisions for the new forms of crime. The year 2000 Act on Information Technology is a special act to tackle cybercrime. The IT act was enacted in 2000

and amended in 2008. It is, however, especially important to note that the basic premise of the law is not the prevention of cybercrime but to foster e-commerce in the country. Due to this objective, there are many criminal acts which have not been covered under the law. The new evolving technology used for crime and criminal acts like cyber defamation, cyber-stalking, and trolling are not covered in this law. There is also the case of international information sharing and collaboration. In the information technology domain, with the introduction of the internet and cloud technology, all the information and data are stored in various parts of the world. There is no physical constraint to storing said information. It is also important to note that there is no specific legal arrangement for the localisation of data generated in India. Many times, servers are located in USA or European Countries for services such as email and social media applications. At an international level, information sharing takes place as per the Mutual Legal Assistance Treaty (MLAT) and other international agreements. Investigations remain pending while waiting for necessary information and evidence from service providing companies from foreign lands. Criminals have no constraints, as cyber economic crime is a borderless crime, but law enforcement agencies are facing a major problem in the collection of information from foreign countries. The United Nations office on drugs and crime studied the issues of cybercrime in 2013 and has concluded that over-reliance on traditions and formal international cooperation is not working in the case of cybercrime when attempting to get a timely response for obtaining evidence (United Nations Office on Drugs and Crime, 2013).

There are countless number of operational challenges facing the judicial quest to attack internet crimes head-on. One of such is the lack of prerogative for all police officers to investigate cybercrime. Bearing in mind the non-cooperation from service providers, there is the challenge of preventing cybercrime; the prevention of cyber economic offenses over the internet has become a big challenge. As regulators in one country blocks even the pages,

things are visible using the virtual private network. There is no state control over the internet, and no single agency controls the internet. Thus, the prevention of criminal activities over the internet has become a significant challenge, considering the nature of the internet.

There is also an excessive pendency of cases. This is due to the shortage of manpower and inadequate infrastructure, which is a big challenge for forensic laboratories and judiciaries. Cases take nearly a year or more to reach a logical conclusion. Pendency is a major challenge. The root cause of this challenge is a paucity of technical tools and a lack of skilled human resources.

There is also a lack of coordination by various stakeholders. The criminal justice system consists of many known and unknown contributions by various institutions and persons to bring one case to a logical conclusion and accord justice to the victims. However, the irony is that all the organisations work in a silo and have little harmonisation or synchronisation. A study conducted on the challenges of coordination in cybercrime and cyber security has also proved that there is a need for the harmonisation of the various stakeholders of the criminal justice system (Jang and Lim, 2013). Coordination with service providers and intermediaries is also a major challenge when attempting to get evidence at the right time. Most of the time, companies deny information for various reasons, creating hurdles in the investigation. It is crystal clear that there is a lack of skilled manpower. The criminal justice system is traditional and does not having adequate, skilled human resources for cyber economic crimes as it is a new phenomenon. There is a gap between the number of offenses registered and the number of officers available to deal with the issues of all the stakeholders. There is an immense workload in regard to existing cases of traditional crimes and officers are finding it difficult to deal with cyber economic crimes' due to the paucity of skilled human resources.

There is no adequate training or capacity building to fight internet crime. The present frequency and quantum of training is not adequate for meeting the needs of new technology.

Every day various new crime forms are evolving, and the changes to technology are so fast in the domain of information technology that every year new technology encroaches, which is creating challenges for the training of staff. The parliamentary committee of information technology has also identified the problem of the training of human resources for cybercrime and suggested a separate nodal agency for cybercrime (Secretariat, 2017). There are technological and knowledge gaps regarding new forms of crime and technology within the traditional criminal justice system. There are no settled techniques, laws, or standard operating procedures for dealing with emerging technologies, which is posing a big challenge. There are very few case laws, cases studies, forensic tools, and technologies within the criminal justice system in India, thus, there is a knowledge gap in the system, as the system is more accustomed to deal with traditional forms of crime

2.11 Legal, Policing, and Political Challenges in Tackling Cybercrime in Nigeria

In contemporary society, cybercrimes and security systems have turned out to be the focal points of the virtual governments of developed countries. It is significant as their countless actors and economic shakers and movers in the global economic field aim to tackle technologically driven crimes at a matched pace and magnitude. It has become an issue well-debated by every standard and measure as the sure bet to the survival of their economies lies in the hope and glory of information and communication technology. The role of ICT is that it has now been accepted as the common language of private individuals and business empires. It represents the centre of attractions and rules the new world, the new economy of the twenty-first century. It is against this main interest that there have been policies, interventions, and legislations drawn up by the various governments to drastically reduce the massive negative impacts that ICT has brought into the 21st-century world and economy. There were a number of interventions and policies promulgated by the United Nations, the Council of Europe (COE), and the Group of Eight Industrialised States (G-8) to fight cybercrime and its

implication to the economies of the world. It is noteworthy that all their initiatives to date were borne out of the stark realities of singularly fighting a phenomenon that cuts across multiple national frontiers (Pounder, 2001; Nykodym, and Taylor, 20040; Kshetri, 2005).

A number of both regional and international organisations have made frantic efforts to encourage cyber-security awareness at its fullest. With privileged records and literature assessed, there has been no regional initiative at the level of the Africa Union on cybercrime and its nefarious activities. Further, in pursuance of its mandate for the harmonisation of national legal frameworks against cybercrimes, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade African states to sign and ratify the Convention on Cybercrime, albeit with no tangible outcome to show for their efforts. Based on some efforts made, it becomes clear that Africa remains a non-dominant actor in the quest to rid the world of cybercrime regarding its legal approaches. Despite the reluctance of many African countries to critically engage with the cybercrime phenomenon concisely, one of the more important means undertaken is to formulate a comprehensive team of legal experts across the divide which should not be limited by jurisdiction to pursue cyber-criminals across borders.

Internet and its facilities pose a new fundamental challenge for victims, law enforcement, and lawmakers. The diverse technicalities and various natures of cybercrime often confuse victims in terms of who to help them out of the quagmire they find themselves in. The legislative arms of governments are franticly dissipating energies to draft laws that will hold up across geographical divide to cross multiple jurisdictions. Law enforcement must also deal with the difficulties associated with jurisdiction (Brenner and Koops, 2004; Burns, Whitworth, and Thompson, 2004), digital evidence (Scarborough *et al.*, 2006), and issues related with the culture and structure of law enforcement (Nhan and Huey, 2008). There is a need for numerous laws to confront internet crimes and fraudulent practices. Hence, legislation in the

area should be conscientious and consistently evolving as technologies advance because the revision and additional to legislations are of paramount importance in attacking the unpleasant side of cybercrimes in Africa. U.S. laws often do not distinguish internet fraud from traditional fraud. Brenner (2006) highlights the legislation surrounding identity theft, including Section 1028 of Title 18 of the U.S. Code which prohibits behaviour considered to be fraud in conjunction with identification documents and contains penalties of five to fifteen years of imprisonment, as well as fines and forfeitures. According to the FBI (2015) and the Internet Crime Centre (2012), under central laws, regulations, and policies it is,

> "Illegal to knowingly and without permission produce an authentication feature, an identification document, or a false identification document. Further, transferring these types of documents knowing that they were stolen or produced without authority is illegal".

Sometimes, offenders will unlawfully employ the patent, copyright, or trademark of an established organisation, institution, or reputable company in an attempt to persuade victims to submit personal details of private information. For instance, email spoofing is but a single form of phishing which is committed in violation of the Lanham Act (2000) and the Trademark Counterfeiting Act (2000), which addresses violations of trademark infringement. The Lanham Act addresses civil damages for trademark infringement and the Trademark Counterfeiting Act facilitates criminal penalties. In order to successfully superimpose criminal and fraudulent charges on culprits, prosecutors must demonstrate that the defendant intentionally and knowingly used the counterfeit trademark to traffic in, or attempt to traffic in, goods and services. These, and related actions, as detailed by Brenner and other legal scholars who elaborate on the nature of identity theft legislation, have become more feasible due to extensive technological advancements.

The interconnected networks of data and computers have not, in their entirety changed the

fundamental approach to the legal orientations and motivations for fraud. Phishing is a type of internet crime being carried out using electronic fraud. According to Brenner (2001:1), cybercrime is categorised into four core legal components; *Actus Reus* (the perpetrator communicates false information); *Mensrea* (communicating false statements to defraud the victim); Attendant circumstances (perpetrator's statements are false); and Harm (the victim was defrauded out of the property or something of value). Under this legal analysis, existing laws are adequate to indict internet fraudsters. Prosecutors can use traditional mail and wire fraud statutes, although not cybercrime-specific, to convict fraud committed via the internet (Brenner, 2006).

Cyber law acts, decrees, edits, rules, and regulations of countries in the whole wide world exist to curtail excesses, be they at federal/central, state, or international levels. They exist to fight head-on jurisdictional issues on the internet as well as other criminalities. The inter-jurisdictional nature of virtually all internet crime provides a unique characteristic of crime not found in conventional crimes associated with human behavioral disorders or defects. Virtually all states and countries in the world differ in their approach and response to criminalities, some with well-cut out laws and regulations, some with a fire brigade approach, and some with laxity and lackadaisical attitudes to burgeoning crimes like illegal cyber activities. In 2006, the United States became an official participant of the Convention on Cybercrime Treaty, established by the Council of Europe, to set minimum standards on international cyber laws. There are uncertainties, innuendoes, and peculiarities can be attributed to differences in law. According to the legal scholars and experts Brenner and Koops (2004), only two situations are associated with international jurisdictional issues, these are, "No one has the right to claim jurisdiction" and, "no country or state can claim more than the other. The scholar further explained at a more fundamental level… it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator,

the location of the effect, or the nationality of the owner of the computer that is under attack? Also, substantive differences in-laws, such as the age at which a society considers one a minor, and the age which distinguishes pornography from child pornography, can be problematic".

It is a fact, that legal and jurisdictional issues massively compound the technicalities and structural complications associated with monitoring and policing cybercrimes. The patchwork of the overlapping hierarchy of law enforcement agencies makes required collaborations cumbersome. Law enforcement agencies, most especially the police, tend to pitch their tents to their practices, entrenched in traditional notions of territory, and have had difficulty adapting to the abstract nature of the cyberspace (Huey, 2002). A countless number of scholars have proposed a paradigm shift from the conventional policing approach to more modern methods that are in line with global practices. There is a need to incorporate partnerships with non-state entities to adapt to the information age (Wall, 2007; Nhan and Huey, 2008). The police prioritise traditional crime and control activities associated with street crime as they must serve the needs of localised citizens and groups (Bayley, 2005). Consequently, the lack of adequate enforcement stemming from law enforcement's static nature in a dynamic environment creates a 'digital disorder' online, resulting in a 'broken windows' condition that is conducive to deviance (Correia and Bowling, 1999).

2.12 Approaches for Policing and Combating Internet Fraud in Nigeria

Combating cybercrime cannot be achieved through a quick fixed surgical hand but rather requires deliberate understanding that cybercrime emerged from certain socio-economic and technical nuances that are rooted within the milieu of a country. There are various root causes of cybercrime and, until that is identified, the approach to combating it may be an illusion because it will be multidimensional, weak, and hapless in ameliorating the nefarious acts. Some of these factors, according to Bakare (1994), are:

i. Causation resides in an individual, such as their cognitive skills, technical skills, peer influence, low self-esteem, exposure to the internet, innate tendencies of theft, and burglary.

ii. Causation resides in the family, such as in a broken home, poverty, indiscipline, or a lack of a role model. Causation resides in the family, such as one's cognitive stimulation, basic nutrition during the first two years of their life, types of discipline at home, a lack of a role model, and finances.

iii. Causation resides in schools, such as one's school environment and their interpersonal relationships with peers.

iv. Causation resides in society, such as a country's poor education policy, non-admission, job loss, unemployment, rustication, bad economy, and poor basic infrastructural facilities.

All of these causes are capable of propelling an individual to engage in online scams. Hence, when this has been identified, a holistic approach can be employed in correcting the abnormalities. There are various approaches employed by the community or society to enforce compliance and maintenance of law and order. However, there is a need for the best possible international practices and approaches to fighting crime. There are current standings of fighting cybercrime in various countries based upon legal, organisational, and scientific outcomes, and there is a strong need for government at all levels to recommend and control several programs, policies, executive order, intelligence reporting agencies, law enforcement agencies, public opinion, and writers and researchers to holistically fight the cankerworm of cybercrime.

Ogwezzy, (2012) submits that the role that officers of the Nigeria police force play in combating internet crime is still unmatched by every standard and measure. They have been able to degrade and ameliorate cybercrime rates in society. Nigeria has serious internet fraud

issues which cannot be solved only by regular arrests of these criminals. This type of approach will only be tantamount to merely treating the symptoms and not focusing on the illness. It will practically amount to a wasted effort. Over a hundred internet criminals could be arrested, but it would not stop cyber-criminality in its entirety. Ayomide (2018) opines that Nigeria needs to embark on a long-term approach to deal with internet fraud. Internet fraud is a nasty scar on the face of the county in the comity of nations. Hence, irrespective of the giant strides made in movies, music, medicine, sports, and others field, the 'Nigerian prince' email scam is still how many foreigners perceive the country. They believe Nigeria is a nation of scammers. Internet fraud, which birthed the famously advanced fee fraud (419), has given Nigeria a bad reputation as a country filled with thieves scheming on how to trick innocent people into giving away their hard-earned cash (Ribadu, 2007).

Not all victims of internet fraud are lucky to get their money back. This criminal act has ruined many lives and families, banishing them to a life of poverty. Through the Economic and Financial Crimes Commission (EFCC), the Federal Government has been doing its best to deal with internet fraud. In May 2018, operatives of the EFCC arrested suspected internet fraudsters, popularly known as 'yahoo boys', at a nightclub in Lagos. It was a sensational piece of news that grabbed several headlines even though it was not the first time that the EFCC had arrested suspected fraudsters. This incidence led to an online discussion on internet fraudsters and whether they should be branded as criminals or just victims and products of their environment. It was reported that between January and May 2019, EFCC operatives made rapid progress in tracking down yahoo-yahoo boys, with a countless number of arrests, prosecutions, and convictions being made (Punchng, 2019). However, they remain behind bars for the shortest time possible. This simply means the penalty meted at them is always very mild and as they may not be detrimental to others (Okeshola and Adeta, 2013; Jude, 2011; and Albanese, 2015). Without mincing words, 'yahoo boys' are criminals and should

face the law and be prosecuted and jailed for their crimes.

Community policing is a burgeoning strategy to focus on constructive engagement with citizens who are end-users of the police service and re-negotiate the contract between the people and the police, thereby making the community co-producers of justice and improving the quality of police services (Okeshola and Mudiare, 2013). Ikuteyijo (2009) opines that community policing depicts civic engagement and community partnership in creating an atmosphere that is serene, safe, and secured. It is policing for all whereby all hands are on deck to ensure that everyone safeguards his or her environment with a staunch commitment and reportage to law enforcement. Brogden and Nijhar, (2005) assert that community policing is a proactive measure employed to focus on identifying and analysing problems and developing solutions. Community policing is preventative and proactive, focusing on identifying and analysing problems and developing solutions (Brogden and Nijhar, 2005). Fighting crime and police-community relations are intimately related and it is stated that bringing police services closer to the community will strengthen the accountability of the police to the public. Although, a study conducted in Nigeria found that community policing created more opportunities for corrupt or unethical practices through police officers having closer ties with community members, and instances of preferential treatment arise (Olusegun, 2009).

Democratic policing respects the rights of all those who meet officers and ensures that officers behave in a procedurally fair manner. It is one of the many approaches to dealing with cybercrimes and other nefarious acts. Paganini (2013) and Radwan and Pellegrini (2010) submit that democratic policing has been used in many parts of the world with resounding successes. Its main objective is to combat criminality through the involvement of community members. According to Dickson (2007), there are various obstacles to the successful implementation of community policy in Nigeria, among which are the inadequate support

from members of the public, government, and law enforcement agents as well as little to no remuneration and an unhealthy rivalry between ethnic groups. Also, with so much poverty in a land where the minimum wage is N18, 000 ($50), it is not surprising that young men have turned to a life of crime. Where there is poverty, expect criminal acts from the financially disenfranchised. In a bid to live the Nigerian dream (which is to hammer by any means necessary), men and women become online bandits, robbing people of their hard-earned cash. Another long-term approach to dealing with internet fraud is reducing the poverty rate in the country. If more Nigerians are above the poverty level and the minimum wage increases to meet the financial demands of the present time, there will be a drastic decline in criminal activities, including internet fraud.

The National Bureau of Statistics (2018) affirmed that 16 million Nigerians were unemployed during the third quarter of 2017. Hence, unemployment has helped the growth of internet fraud. Young individuals who have no job and live below the poverty line most likely enter a life of crime, such as partaking in internet fraud. These factors of unemployment and poverty have led many young Nigerians to crime, including internet fraud. Nigeria's long-term approach to dealing with this menace will be to reduce the poverty and unemployment rates. If a sustainable approach is developed, the level of crime in the country will dwindle. There is a third factor that has eroded the moral fabric of Nigerian society; get rich-quick syndrome has turned average Nigerians into criminals and the devil’s work tools. Excessive materialism plays a huge factor in internet fraud and other nefarious activities engaged in by the Nigerian youth. Whether pandemic or endemic, corruption has also eaten too deep into the moral fabric of the country. Corrupt politicians and businessmen have been having a field day and hardly ever face the wrath of the law; most societies have done away with the value of hard work, diligence, and integrity. They have imbued themselves with the excessive quest for materialism, they do what they have to do to make money at all costs. People admire and hero-

worship individuals with questionable sources of wealth more than people who grind daily to earn an honest living. When a society promotes the thinking of getting rich by any means necessary, there will be people who will be willing to do anything to get rich. Many young Nigerians were born into this way of thinking and instead of working hard to make something out of themselves, they choose the fast life of quick money and crime. To properly deal with internet fraud, a national reorientation of our values must happen. There is a need to reinstate honesty and hard work to previous social pedestals and do away with the mindset of excessive materialism and get rich quick schemes. Nigeria must play the long game to deal with and defeat internet fraud. Poverty, unemployment, and excessive materialism must be dealt with to get rid of this national menace.

2.13 Explanation of Cybercrime Victimisation

Cybercrime victimisation can be defined as the process of bullying or stiffening people, companies, and entities through privileged information at one's disposal and with the help of technologies. It is also referred to as the resultant effect of victimisation from any forms using the internet and other technological applications. Cybercrime victims can be governments, organisations, or individuals. With the arrival and introduction of technologies into daily life, cybercrimes like online bullying have received a great deal of concern and attention from researchers, data analysts, schools, organisations, parents, children, and the public. Cyberbullying is a new form and extension of face-to-face bullying which occurs when bullies target victims via cyberspace (Smith et al., 2008). Bullies might target victims through emails, instant messaging, chat rooms, social networking sites, and text messages. It aims to achieve the maiming, tormenting, harassing, or threatening of victims internationally as well locally (Grigg, 2010). It occurs one-on-one, among groups, peer mates, and through mass audiences (Dooley *et al.*, 2009).

The prevalent rates of cyber victimisation vary from 6 per cent to 41 per cent, depending on

the definition of cyber victimisation, the measurement of cyber victimisation, and the time parameters used to assess this experience (Li, 2006; Nivers and Noret, 2010). Irrespective of it differences and variations, reportage of cyber criminalities is very important because dealing with such an event alone could lead to one contemplating suicide, depression, anxiety, loneliness, alcoholism, drug use, and abuse as well as lower academic performance (Bauman *et al.*, 2013; Campbell *et al.*, 2013; Huang and Choi, 2010; Kowalski and Limber, 2013; Mitchell *et al.*, 2007; Schenk *et al.*, 2013). Hence, due to the psycho-social adjustment difficulties associated with cyber victimisation, researchers have directed their attention to factors that might buffer or reduce the negative effects of experiencing cyber-bullying. One of the most dependable and frequent uses is the mediation of young one's technology usage by all the agents of socialisation, those being their parents, guardians, peers, teachers, or religious houses, among other things (Livingstone and Helsper, 2008; Van Den Eijnden *et al.*, 2010).

Cyber victimisation has the potentials for existing anonymously, while the perpetrators and their nefarious crime are capable of wreaking havoc of a high magnitude and pace on victims, which is significantly greater than face-to-face bullying or theft. It offers narrow routes of escape for innocent victims. Anyone can be bullied anywhere, for example in school, any social gathering, or online. The victim is frequently being attacked on a social level rather than a physical one. For the bully, computer prowess is more important than physical brawn. Being bullied is a significant risk factor for subsequent social anxiety, but bullying is changing. It is moving from the schoolyard to the internet, it is becoming relational rather than physical. Anyone with a smart phone can become a cyber-bully and the audience that can observe these acts of cyber-bullying are potentially unlimited and geographically far-reaching. Unless there is a way to find effective methods to manage cyber-bullying amongst school children, adolescents, and young adults in the area of physical and social anxiety, the

youth will continue to be stifled by cyberbullies.

Carin Bergh and Junger (2018), in their study on victims of cybercrime in Europe, employed a large perusing strategy of searching databases, online, agencies, offices, and departments for national statistical figures and raw facts in Europe. The selected surveys gave a valid expression and representation of cases of victimisation on individual bases which were capable of depicting the entire cybercrime issue. It was discovered that six types of cybercrime are well pronounced, these being online fraud through banking payment, online shopping, advance fee fraud, malware, hacking, and harassment. For every survey, the questions on cybercrime are presented and the crime prevalence estimates are compared. It was discovered that nine surveys were included. Annual crime prevalence rates ranged from one to three per cent for online shopping fraud and from less than one to two per cent for online banking/payment fraud. Less than 1 per cent of the population was a victim of other types of fraud and a maximum of three per cent of the population had experienced some sort of online bullying such as stalking (one per cent) or threatening (one per cent). One to six percent were victims of hacking. The estimates for being a victim of malware ranged from two to 15 percent. For all offences it cannot be estimated how much of the differences are due to variation in data collection methods and questioning methods between the studies, real differences between countries, or changes over time.

It was also discovered that in 2018 23 per cent of the households in the United States of America were victimised by cybercrime. Americans are more likely to talk or report one or more household members to have been scammed, defrauded, and humiliated online through the tampering of their personal details or having their credit cards and financial information stolen by computer hackers than report being victimised by any of the eight other forms of criminal activity. Nearly a quarter of Americans, 23 per cent, say that they or someone in their household fell victim to this type of cybercrime in 2018. Little changed this year as 25 per cent

reported being targeted similarly. Nearly a quarter of Americans were victims of cybercrime in 2018 (Zero tolerance, 2019: ICCC, 2019).

2.14 Conclusion

The world in general, and Africa in particular, have seen a rapid increase in the use of the internet as well as an increase in cybercrime, both in its occurrence and its variance. In the same vein, cybercrime proven that it is here to stay in Nigeria and beyond. It is a cankerworm that has eaten deeply into the social fabric of African society. Nigerian youth now adopt cybercrime as a convincing root to making easy cash, thereby abandoning the dignity of labour and respect for the fundamental human rights of others. A large chunk of youths and teenagers, across the divide, whether in developing or developed countries, are engaging in nefarious acts such as identity theft, hacking, phishing, electronic fraud, pornography, piracy, spamming, and ATM/ACR spoofing, among other things. Usually, these crimes are committed in the form of sending fraudulent or bogus financial proposals from the cybercriminals to innocent internet users. This has become a large threat to Nigeria's e-commerce growth and has led to a poor reputation intentionally and has consequently denied some innocent Nigerians certain opportunities abroad. Cybercrime constitutes a worldwide problem that requires a holistic approach to dealing with it.

Socially, there are countless factors which are responsible for the burgeoning rate of cybercrime in Nigeria, Africa, and beyond. They are enormous and re-occurring daily issues which includes unemployment, poor standards of living, poor economies, greed, infrastructural deficits, political instability, and the unconscious neglect of youths. There is a strong urge to assess these factors in tandem with the prevailing acts. Security apparatus put in place to combat this nefarious act is being side-track by bribes and conjuring by famous individuals and the dependent judiciary. There is outlandish growth in the use of internet facilities and the economy too is going online. This means that virtually all sectors of the

economy and of society are more and more dependent on the internet.

Technology has also influenced people into switching to internet banking and completing transactions online. The unique opportunities of a quickly developed financial infrastructure allows anyone to transfer monetary funds to any State anonymously and through tangled routes, and this has caught the attention of cyber criminals. Electronic transfers are an efficient tool for concealing sources of money intakes and laundering illegally earned money. Many have followed these illegal acts, and this has led to cries and hues in society. Thus, Nigerians and the rest of the worlds internet users should be security conscious with the intent of gearing up their knowledge and widening their horizon about the burgeoning world of information and communication technology as well as the massive industry of cybercrime in its different forms and styles.

CHAPTER THREE
THEORETICAL FRAMEWORK

3.1 Introduction

This chapter provides the theoretical framework for the study by describing the relevant theoretical approaches that served as a blueprint for the better investigation, explanation, and understanding of cybercrime. The section discusses Robert Merton's strain theory and the rational choice theory to account for the wide range of variables that have caused and sustained cybercrime activities in Nigeria despite efforts to reduce the social menace. Also, the study evaluated other theoretical frameworks that share a related but distinct opinion with the current study, the purpose of this is to compare and juxtapose the different theoretical approaches that previous scholars have adopted to explain the phenomenon of cybercrime in Nigeria.

Cybercrime posits one of the ultimate threats experienced by humanity through the use of modern technology, irrespective of the lens is viewed. The havoc and threat caused by this phenomenon remains a global controversial debate among citizens and stakeholders. Obviously, the tremendous growth in computer connectivity and its usage over the last four decades has presented a massive opportunity for cybercrime perpetrators to undertake their nefarious acts within the cyberspace at the expense of unfortunate victims. Some of their criminal activities include ransomware, hacking, phishing, and online romance scams. However, given the alarming increase in computer and internet-based crime, prospective criminals have at their disposal the necessary tools and means to hone their skills in their criminal acts and other related anti-social behaviours. The quest to engage in all forms of computer-related crimes bears the same notion of achieving socially acclaimed success of monetary value with illegitimate means provided for unconsciously by the society which is meant to protect and grow individuals into a full-fledged personality that can offer plausible solutions to both personal and community problems, but the reverse is the case. Cybercrime opportunities keep growing by the day.

Taylor *et al.*, (2006) bemoan few attempts at developing and applying criminological theories to the concept of cybercrime. Hence, this study will adopt Robert Merton's strain theory and the rational choice theory by George Homans (1961) to peruse the attitudinal patterns and behavioural manifestations of the lived experiences of cybercrime perpetrators in Nigeria. These theoretical perspectives will help assess why people engage in destructive activities online at the detriment of other people and the image of the country in the international community. Both Strain and Rational Choice theories view delinquency as a product of individual agency, following a process of conscious thoughts and decision. These theories, therefore, bring on board rich scholarly arguments to examine cybercrime perpetrators' attitudinal patterns and the predisposing factors to deviance within societies.

3.2 Merton's Strain Theory (Overview)

Strain theory has been advanced by prominent scholars and researchers like Robert King Merton (1938), Albert K. Cohen (1955), Richard Cloward, Lloyd Ohlin (1960), Neil Smelser (1963), Robert Agnew (1992), Steven Messner, and Richard Rosenfeld (1994), after the foundation laid by Emile Durkheim's Anomie theory. Hence, this study adopts Robert King Merton's (1938) strain theory. Robert King Merton was an American Sociologist who came up with strain theory as a breakthrough in the field of sociology and criminology. He developed this theory as a response to the resultant effects of the socio-economic circumstances evolving in the United States of America during the early 1900s. He developed the theory to fundamentally explain, in clear terms, the individual differences and varying patterns of deviation provided as a result of the lacuna in societies. He submits that the normative breakdown and other deviant behaviours evolving in society were borne out of the fact that there are loopholes that society unconsciously opens between culturally approved expectations and socially constructed or promoted avenues to the attainment of success (Featherstone and Deflem, 2003). Merton, however, maintains that socially accepted goals mount unnecessary

pressure on people to conform to the norms of society, irrespective of the modus operandi through which such society is being established. Robert Merton's strain theory emanated from a fundamental question he asked, why there is an alarming rate of deviant behaviour and criminal activity among people within society. He presumed that there can only be such negative acts when there is a wide gap between and among what success is and the means at which it is being achieved. According to Merton societies are comprised of two core aspects: culture and social structure. Our cultural upbringing shapes our values, beliefs, objectives, and identities. They emerge in response to existing social institutions, that in an ideal world, give the means for the general public to realize their objectives and live out positive identities. People, on the other hand, frequently lack the resources necessary to fulfil culturally valued goals, causing them to feel pressure and, in some cases, to engage in deviant behaviour. Merton established strain theory by reviewing crime statistics by class and applying inductive reasoning to his findings. He discovered that people from lower socioeconomic groups were more prone than others to conduct crimes. It was his contention that, if people are unable to achieve the "legitimate aim" of economic success through "legal means" dedication and hard work they may resort to illicit means of achieving that goal. The cultural significance of economic success is so great that some people are willing to go to any lengths to obtain wealth or the trappings of it in order to achieve it.

Conversely, the theory submits that society is capable of encouraging deviant and non-conformist behaviour because there is a structural gap and imbalance between a goal and the approved methods of achieving it. And this has watershed into the individual and social fabrics of the society. The theory affirms internal strife and pressure is mounted on citizens to achieve socially accepted goals even when they lack the requisite tools and means of doing so. This, thereby, forces them to engage in nefarious acts as current social structures and institutional arrangements are hindering them.

When this is done, it leads to strain and makes citizens anti-social or causes them to exhibit abnormal behaviours such as giving in to prostitution, doing drugs, robbery, gangsterism, rebellion, inciting revolution, committing cybercrimes, and partaking in ritualism, among other things, to gain financial and economic security. Merton maintains in his findings that all people living in the United States of America (USA) are indirectly forced or encouraged to strive towards achieving the cultural goal of monetary success. As a capitalist society, lower-class individuals (low-income earners) are also indirectly prevented from achieving this goal through legitimate means, such that families (parents and guardians) may not be able to provide the necessary skills, values, and attitudes required to solve personal as well as community problems and by extension live fulfilled lives. This is shown when they have shelter problems, fail in their career, leave their kids wandering town, have a lack of money to set up a business, have a lack of a school education, or live-in communities with inferior schools. As expected, they experience, on a large scale, strain, which is a product of poor institutional arrangements and disjunction between goals and the legitimate means of attaining them.

There are strong inconsistencies as to how success can be accomplished. Merton argues that educated elites, those that are well lettered and travelled, are respected, but bandits, criminals and men of the underworld are more admired and honoured. With this, success is honoured and seen as more important than the means to achieve it (Parnaby and Sacco, 2004). Also, Merton observed that low-income earners were unable to acquire qualitative education and if they struggle to do such, they would only be allowed to take on menial jobs. However, the same rules and standards are applied to success despite the fact that not everyone is able to attain it through conventional means. People are forced to live and work within such a system or become members of a deviant sub-culture to achieve their desired goals. Merton opines that, in coping with strain, people must adapt in line with the following typological modes of individual adaptation.

3.2.1 A Typology of Modes of Individual Adaptation

Modes of Adaptation	Cultural Goals	Institutionalised Means
Conformity	Accept	Accept
Innovation	Accept	Reject
Ritualism	Reject	Accept
Retreatism	Reject	Reject
Rebellion	Accept/Reject	Accept/Reject

Conformity: A conformist believes in cultural goals and ardently purse them through socially approved means. They believe and follow the cadre that society has put in place for achieving success and they may include civil servants, teachers, engineers, lecturers, doctors, and nurses, among other things. Trying to achieve cultural goals through accepted ways is what conformity is all about. Conformists are people who accept the aims of society as well as the methods of achieving those goals that have been authorized by society as valid. According to the "American Dream," financial security can be attained by virtue of one's ability to work hard and to complete one's education, above all. Because not everyone who want to achieve conventional success has the opportunity to do so, according to Merton, this is a significant problem.

Innovation: Merton (1957: 141) describe innovation as "the individual who has internalized the cultural focus on the goal without similarly internalizing the institutional rules defining the means and methods by which the goal is to be achieved." Merton (1957:145) states that the impoverished accept the America Dream, but the pathways available for working towards these goals are primarily restricted by the class system to those of deviant behaviour'

Further, an innovationist believes in the cultural goals of society. They think they are achievable; however, they are not convinced the means are feasible, hence, they innovate new approaches to attain the goals. This group of individuals adopts unconventional means in achieving culturally approved goals, such as prostitution, to achieve financial sufficiency. According to Merton, certain people, especially the impoverished, may be drawn to engaging in criminal activity because of the conflict between our culture's emphasis on wealth and the fact that there are less possibilities for achievement. Merton referred to this as deviant innovation, and he defined it as the use of unusual means to accomplish a culturally acceptable purpose financial security.

Ritualism: Robert K. Merton introduced the concept of ritualism as part of his structural strain theory, which he developed in the 1960s. Merton describe ritualism as a common practice in which individual engage with the motion of daily life, even if a person does not conform with the goals or ideal that are associated with those behaviours. Ritualism according to Merton's perspective arises when an individual rejects the normative aims of their society while continuing to participate in the means of achieving set out goals. While opposing societal norms, this attitude is not deviant in that the person is nonetheless adhering to them, thus it requires continuing to act in a manner consistent with the pursuit of those goals. Though ritualism is rooted in dissatisfaction with society's beliefs and aspirations, it ultimately serves to sustain the status quo by encouraging the continuation of normal, everyday routines and behaviours.

Retreatism: This entails out-right rejecting both cultural goals and the means to attain them, thereby finding a way out. This includes chronic drunks, homeless individuals, vagabonds, and drugs addicts.

Rebellion: This entails rejecting cultural goals and the modes of attaining them, thereby working assiduously to replace them. This simply means rejecting any goals and means. Rebels may include terrorists and insurgent groups.

3.3 Robert Merton's Strain theory and its application to the study

The application of theory to better comprehend and organize information on internet fraud is an important priority in cybercrime research. The application of theories such as social learning, differential association, and routine activities theories has been fruitful in recent attempts in this field, but there is still opportunity for further ideas to be implemented. While neglecting other major causative in other theories, strain theory offers an interesting explanation for the phenomenon. Exclusively, it predicts that individuals who experience frequent pressure in their social relationships and event produces negative emotional states, which in turn serve as a stimulant for violent and criminal behaviour. Specifically, this section discusses how these ideas might be used to better understand the causes and stimuli of cybercrime activities among young Nigerians. Within this framework, perusing cybercrime and other related activities have been difficult to understand, too wide to predict, and too technical to solve. Cybercrime activity is a criminal act perpetrated through the use of electronic communication networks and information systems. It is a dastardly act against computer networks and systems which requires potent modelling and review. With a long history of cybercrime and other related acts, theories and models designed and espoused by great researchers, both in the primary and secondary sources of cybercrimes and syndicated activities, are known and studied by budding institutions, researchers, and governments, among others. However, adopting Robert Merton strain theory (1938) in examining cybercriminal acts in Africa, and most especially in Nigeria, has provided leverage in understanding how cybercrime is particular to each society in tandem with its individual societal demands and the stated objectives of getting rich at all costs.

Strain theory has been tested as a result of its rapid acceptance in studying the motives behind individual engaging in criminal activities and other nefarious acts within the social sphere. This centres on the nexus relationship between ideals, goals, and individual expectations, which in most cases, if not properly curtailed, may lead to criminalities through upholding the assumptions and propositions of strain theory (Agnew, 2007). Strain theory shows the relationship between deviant behaviour and the design of the social structure. It helps to deepen knowledge and understanding by connecting the ideas of the antagonistic relationship between cultural goals and institutionalised means.

The more the deleterious a society is, the more its residents' become slaves to it and the more they engage in unlawful acts such as cybercrime. The lack facilities and opportunities will, in serious terms, drive an individual to engage in cybercrime to achieve the cherished goal of happiness by employing any means that are currently available without minding the rapacious implications and their harmful effects on people and society. This theory is relevant as the current event in Nigeria is largely based in competition, luxuries, and affluence at the expense of the weakest in the society. In a balanced society, an equal emphasis is placed upon both cultural goals and institutionalised means, and members of society are satisfied with both. But in an unbalanced society, such as in Africa and most especially Nigeria today, great importance is attached to the success of achieving goals while relatively little importance is attached to the acceptable ways of achieving the goals (Haralambos and Holborn, 2008).

The situation now becomes like a game of cards in which winning becomes so important that the rules are neglected and abandoned by some of the players. By the same way, when rules and regulations are abandoned and neglected, anarchy emerges, and it balloons to the peak of criminality and social unrest. In this situation where 'anything goes', norms no longer direct behaviour and deviance are encouraged. However, individuals will respond to a situation of anomie in five different ways and their response pattern will be shaped by their position in the

social structure. Importantly, a cybercriminal is seen as someone that believes in the cultural goals of society but perceives the means as straining and unrealistic, hence, they adopt new medium. Cybercrime is, therefore, a non-conforming medium to attaining success that has become a norm among the youth in Nigeria. Merton would call them innovationists; they believe in the cultural goals of society but reject the institutional means to achieve such goals.

3.4 Distribution of Knowledge and Skills: Innovative Activities of Cybercrime Perpetrators

The main purpose of Merton's strain theories was to explain why certain cultures, organisations, and individuals are more likely than others to engage in antisocial or unlawful activity. Merton stated that individuals of society learn about what is normal from societal institutions about certain behaviours that are acceptable, and how individuals should behave. Merton (1957: 132), opined that what is considered normal is that which is the psychologically expectable. Merton noted that response to specific social condition is considered normal and social rule of behaviour serves as a benchmark for most people. However, pressures from social institutions, notably from expectations connected with the "America dream" can motivate some individuals to engage in unconventional behaviours (Zembroski, 2011). In this context, cybercrime perpetrators (yahoo boys) can be classified as innovationists. Due to the fact that they are accepting of societally institutionalised goals. To attain success cybercriminals, reject the means approved by society as strenuous, and thus, in the bid to fast-track success, innovate a new route to achieve the societal goal of wealth and achievement which sometimes leads to committing cybercrime. However, Merton explains innovation as a process through which members of a society accept the goals of success but reject the legitimate means of achieving them and turn to deviant means, in particular crime. Merton argues that members of society that are most likely to select this route to success include: people with low social strata, people with low educational qualifications, and people whose jobs have little opportunity for advancement. In Merton's words, they have, "little access to the legitimate and conventional

means for becoming successful" (Merton, 1939:86). Since their way is blocked, they innovate by turning to crime, which promises greater rewards than legitimate means.

Merton explains that people can turn to deviance in a bid to attain societally approved goals. Strain theory is important in explaining the lived experience of cybercrime perpetrators and the phenomenon in Nigeria as several authors have argued that societal gaps, such as unemployment, poverty, and the desire to be wealthy, are important factors that drive youths to adopt deviating means to attaining success (Salami, 2013; Tade, 2013; Melvin and Ayotunde, 2010). Hence, this theoretical perspective allows the researcher to further conceptualise that societal discomfort, infrastructural inadequacies, economic lacuna, and an inability to sufficiently meet needs creates a strain that predisposes individuals to seek redress and comfort in deviant activities. Cybercrime perpetrators in this context are, however, individuals within a society that have faced strained conditions and are seeking out new opportunities and avenues to make ends meet, even though said activities are illegal.

Cybercriminals come from a remarkably diverse background. A society with a large chunk of educated, engaged, and empowered individuals who are committed to their tasks and develop skills which are necessary for their growth and development creates an environment where individuals may not necessarily engage in cyber criminalities even when targeted goals of financial success are not being attained. In the same vein, individuals who are not properly trained and cultured are likely to see criminal activities as a means to achieve enormous financial successes. Most especially vulnerable people with few computer skills may see cybercrime as permissive trend of unlocking free wealth as it immediately provides monetary reward with little investment of time and energy. Strain theory assumes people's inherent goodness and that they are driven by social factors to deviant behaviour and criminal activities in society.

The theory is interconnected and interrelated with the three concepts of adaptations, rebellion, and innovation, which have great components in criminal activities, while ritualism and retreatism are seen and assessed as mere social deviations. Conforming to social rules and regulations is a voluntary act of non-breaching modicum as a method of gaining financial success. It is said that when there is conformity, social identities are formed, fostered, and strengthened in the face of issues, rebellion, and innovation which are capable of building a society that is free from nefarious acts like cybercrime and other related acts and is suitable for the progress and growth of a functioning society that is not chaotic to live in.

3.4.1 Criticism of Strain Theory

Using strain theory, sociologists and criminologist have been able to explain deviant behaviours associated with acquisition and to provide support for research that relates social-structural conditions to culturally valued goals. Many people consider Merton's theory to be helpful and beneficial in this context. His definition of "deviant," on the other hand, is contested by certain scholars, who argue that deviance is a social construct. In order to achieve economic success, some individuals may resort to illegal activity, while others may simply be engaging in conventional activities for people in their situation. According to strain theory's detractors, categorizing crimes of acquisition as deviant may lead to laws that seek to control people rather than to make society more egalitarian, as opposed to making society more equitable.

Further, Merton’s strain theory has been criticised from various quarters. Merton is said to have claimed that his theory, which centred around the societal norms of twentieth century America, was universally applicable and that he did not consider the varying social goals in other communities. He failed to establish to whose interest society was being socialised into (Featherstone and Deflem, 2003). According to Marxist belief, the theory is adjudged to be capitalist-driven, in such that all and sundry wants to make money to buy luxuries and consumables (Cullen and Messner, 2007). As well as this, all are cowed into the belief that the

best way to achieve this is to work extremely hard for the bosses so as to earn a high income. This is purely promoting and celebrating a capitalist society where the rich continue to get rich and the poor languishing in penury, that is serving the interest of bourgeoisie at the expense of the proletariats. Merton was criticised for not considering why some select members of society find it harder to achieve their goals and enjoy life. He ignored the factors of inequality, unequal opportunities, and abilities within society and its attendant factors. Merton equally failed to consider people's varying adaptations and why many assume that the socially acceptable means to achieve goals are extremely difficult for nearly all and sundry. Bringing to the fore these inadequacies and shortcomings, in explaining non-conformity this study draws on arguments of rational choice theory to fill the gap.

3.5 The Rational Choice Theory

The rational choice theory was developed and theorised by George Gasper Homans in 1961. Homans is an American sociologist who propounded behavioural sociology and social exchange theory. He was well known for his famous work, "the Human Group", and had a career which spanned through most disciplines in the humanities (Lee, 2016). His work on social behaviour influenced notable scholars and authors like Robert Merton, James Samuel Coleman, Lauman Edward, Karen Cook, and Emile Durkheim, among others. The rational choice theory was developed by George Homans as an approach used to understand human behaviour. It has been utilised to change the paradigm, with various adaptations being applied to different fields of economics, political science, sociology, anthropology, and criminology, among others. It can also be called choice theory (CT) or rational action theory (RAT). The theory serves as a framework for the understanding, as well as the modelling, of the socio-economic behaviour of people. A famous aspect of rationality is instrumental rationality which signals to seek the most cost-effective approach to attaining set goals without reflecting on the worthiness of the said goals, irrespective of the size or forms they may take (Hodgson, 2012).

Rational choice theory brings into context free will, choice, and rationality in the examination of criminal behaviour. In this assumption, humans are rational, self-motivated, and interested beings who are subject to or affected by the consequences of their actions and inactions (Lee, 2016). To apply the rational choice theory to the study, criminalities are not different from non-criminal behaviour, the only difference is the attitudinal patterns and conduct exhibited by individuals who intentionally choose to carry out such nefarious acts (Cornish and Clarke, 2014). Criminal activities and other nefarious acts are not forced on bandits, they engage in them wholeheartedly with the illegitimate intention of making monetary and material rewards with fewer risks, minimal sweat, and energy.

Rational choice theory postulate that individuals are encouraged by their personal interests, ambitions, and personal goals. Ideally it is not possible for humans to have all of the numerous things that they desire, it is natural that decisions about these goals as well as the means to achieve those goals are made. The results of various courses of action must be anticipated, as well as the optimum course of action for the individual. At the end of the day, sensible persons choose the course of action that is most likely to provide them with the greatest amount of happiness. Rational choice theory assumes that all action is fundamentally "rational" in nature. As opposed to other forms of theory, it distinguishes itself by denying the reality of any type of activity other than strictly logical and calculative behaviours. The premise that complex social phenomena may be explained in terms of the individual acts that led to those phenomena is also basic to all kinds of rational choice theory. This is referred to as methodological individualism, and it maintains that the fundamental unit of social activity is the act of a single individual person (Crossman, 2021). In order to understand social change and social institutions, we merely need to demonstrate how they are created as a result of individual action and interaction.

The fundamental assumption of rational choice theory hinges on the total or aggregate behaviour of individuals and their decisions (Hodgson, 2012). The theory leverages on the predictor of individual choices, which is termed methodological individualism. Rational choice theory assumes that every individual has the rights to make choices for themselves as well as to face the consequences thereof. In that, out of the abundance of choices to be made and decisions to be taken, an individual has preference among the available choices which allows them to state the options they prefer (Cornish and Clarke, 2014). These preferences are assumed to be complete (the person can always say which of the two alternatives they consider preferable or that neither is preferred to the other) and transitive (if option A is preferred over option B and option B is preferred over option C, then A is preferred over C) (Hodgson, 2012). Individuals who are rationally minded are presumed to consider the availability of information, event probabilities, potential costs, and benefits in determining which action to give preference to as well as to act consistently in selecting what is the best choice of action to be taken (Lee, 2016).

Rationality is widely used as a fundamental assumption of behaviour underlying the treatment of human decision making. It simply means that people employ logic to balance costs and benefits to arrive at an action that maximises personal benefit. It is, specifically, the cherished idea that individuals are acting and exhibiting behaviours based on their selfish interests, which are logical. An individual may choose to be honest and kind to others or otherwise as it might make them feel better about themselves and vice versa. In a nutshell, rationality will continue to be a driving force whenever an individual is choosing what he or she seeks to benefit in. The rational choice theory also stipulates that all complex social phenomena are driven by individual human actions. Ganti (2019) submits that rational choice theory states that individuals rely solely on rational thinking and calculations to attain probable outcomes which are targeted at achieving personal goals. Through this people derive joy and benefits as they

are free to make choices for themselves come what may, as when they are given an array of choices they are found to act in their highest self-interest.

In agreement with rational choice theory, Zey (2001) asserts that the theory is based on the premise of people's desire to maximise the utility of their self-interest. In the same vein, Nobel laureate, Simon Herbert, propounds a theory called bounded rationality which states that people lack the mechanisms to garner the proper information they would need to pursue the best decision. Besides this, economist Richard Thaler's idea of mental accounting assesses how people behave irrationally and illogically due to the greater priorities they give to the American dollar over other currencies, even when they share nearly the same value.

3.4 Application of Rational Choice to the Study

Rational choice theory is based on the idea that all action is fundamentally "rational" in nature, which is one of its major elements. As opposed to other forms of theory, rational choice theory distinguishes itself by denying the reality of any kind of activity other than those that are entirely logical and calculative in their nature. It claims that all social activity, no matter how irrational it may appear to be, may be viewed as rationally driven in some sense. Cyber criminology is evolving in paces and exists with a staunch warning of its threats across the spectrum of society. Cybercrime perpetrators have grown in leaps and bounds and are gaining ground on critical infrastructural facilities and computer networks over the last few decades (Williams and Fiddner (2016). Recently, the hordes of cybercriminals have found their way into social structures and governmental institutional arrangements to wreak havoc and destroy classified documents and files as well as reveal information (Matusitz, 2006). The over-reliance of people, modern societies, and organisations on information technology and networks of computers has made them susceptible to attacks aimed at critical information technology infrastructures (Viano, 2016). It is equally a well-known fact that societal threats posed cybercriminals have been massive in the last three decades, but core destructive tendencies

have only begun on a large scale very recently. Statistics relating to cybercrimes lack the adequate facts and figures as perpetrators remain private and hidden due to the implication of being caught when their identity is disclosed. To significantly assess who the attackers, scammers, and hackers are and why they engage in such nefarious acts brings to bear an established theory called rational choice theory (van de Weijer *et al.*, 2019; Bidgoli and Grossklags, 2016).

The emergence of cybercrime, which only recently gained popularity on the world stage among sociologist and criminologists, has several indicators that studying cybercrime becomes more difficult with the development of new technology (Brown; 2005; Gercke, 2012). The abuse and misuse of computing devices is not new to society, what is new are the approaches and plans to which cybercriminals employ for their nefarious acts. The abuse and misuse of computing devices is as old as technology itself, however, it was a phenomenon which lacked substance before networked computers and other devices were developed and launched for public use (Gercke, 2012). In those days, only a few were able to acquire computer sets because they were extremely expensive, rare, and required high levels of technological know-how to operate successfully. All of these factors propelled the misuse and abuse of computing devices. The ultimate use and need for internet facilities began to rapidly increase as the days went by as computing facilities became less expensive and more common.

following from the above, the suitability of the rational choice theory for this study is very direct as it explains in clear terms the motives for which criminals thrive. The rational choice theory was chosen for the study because it does not support environmental forces or specific assumptions but rather the justifications and propositions of cyber criminalities. Rational choice theory is very viable for the description and explanation of cybercriminal behaviour on every front and style. Virtually all of the hypotheses raised and tested by various scholars and theorists in the field of this theory have a clear-cut relationship with this present study (Hui,

and Wang, 2017). In the same vein, it corroborates the objective of this research. The application of rational choice theory in assessing criminalities and illegalities in society dates back over five decades ago, particularly in Nigerian society. Criminals are neck-deep in the social fabric of the nation (Ibrahim, 2016). Nigerian society is pervaded with all forms of atrocities and waves of crimes, ranging from fraud, kidnapping for ransom, armed robberies, and other violent crimes (Ruwan *et al.*, 2020). Thus, these and more watershed the foundation of criminality in the nascent society. However, with the advent of technology, online fraudulent dealings rear their ugly head into society, raising the agency of social structures and policies of free will. Nigerian teenagers and youths are forced to wait long periods of time to raise money and affluence through an illegitimate means online. This, in turn, has become a cankerworm and serious headache to government at all levels, institutions, and people within society as a whole (Tade, 2013).

Cybercrime and other online related activities are fast paced but do not rule out the strong need for empirical evidence to assess the rationale behind every choice and decision made by an individual in the quest to make ends meet, whether legally or illegally. Carrying out a study on cybercrime may be a herculean task but it is worth the effort as there are numerous cases abound in society from available evidence, both qualitative and quantitative in nature. Scholars have described Cybercrime as any criminal activity engaged in through the use of computers or computing devices in whatever forms, shapes, or sizes, as well as computer networks (Wyn and White 1997:10; Shinder, 2002; Broadhurst *et al*., 2013). However, some of the examples include virus creation and distribution, hacking, creating, and circulating pornographic materials, cyberterrorism, online fraud, scams, identity theft, cyberbullying, stalking, and deviant behaviour, among other things. The rationale for engaging in these acts is questionable.

Since Nigeria's independence, there has been rapid growth and development in all spheres, ranging from politics, economics, and infrastructural facilities to the acquisitions of new skills,

knowledge, and behavioural patterns as well as the growth of cyber criminalities and other related crimes (Ogwezzy, 2012). Some are of the opinion that this has to do with technological advancement and misappropriation, while some opine that it has to do with the globalised behaviours of ostentatious living and pride. Some schools of thought affirm that it has to do with personality traits. Be that as it may, there has been value deterioration, flamboyant living, and high consumerism, a personal and societal problem which all cause a nosedive into the cankerworm called cybercrime. It has, however, become a thorn in the side of many Nigerians and society at large. The rising cases of cybercrime in Nigeria may have been propelled by a deficit in the standard of living, a non-conducive environment, and the uneven distribution of the commonwealth of all, alongside high levels of poverty and unemployment in the teeming graduates being churned out daily (Aransiola and Asindemade, 2011; Adesina, 2017).

Nigerian youths are wallowing in poverty despite the huge human and material resources available in the country. In Nigeria, cybercriminals are taking advantage of e-commerce systems available on the internet to defraud, bully, spy, and steal vital information and documents, as well as huge amounts of money and other valuables from victims, most of which are foreigners. Cybercriminals dupe victims with the fake identity of either a businessman, a government official, or someone high and mighty in society to scheme and dupe them out of their possession (Okeshola, 2013). At times, they claim to have a loan scheme or financial institution where money can be given out with little or no collateral. In this regard, so many persons have been duped or have fallen victim. However, there are countless other methods employed by cybercriminals to trick innocent minds. Every measure put in place by Government to curb excesses has not been met with great success, as the identities of cybercriminals remain silent, hidden, or inadequate. The youth in Nigeria are generally known for cybercrime and the criminal activities they indulge in so as to survive and have a taste of the good life (Adesina, 2017). Employment issues have gone overboard, most Africa countries,

including Nigeria, are living below the poverty line. Some are wallowing in abject poverty and redundancy, and their citizens are malnourished and are dying daily. Due to all of these factors, many Nigerian youths take to fraudulent activities, whether through online or face-to-face transactions to survive, irrespective of the weight of such atrocities (Adesina, 2017). The growth of cybercrime does not necessarily struggle to survive in Nigeria and the rest of African countries due to the vulnerability of the average African child.

The World Bank, (2008) in one of their communiqués, submits that African states are still facing various forms of challenges. They have to generate 100 million new job opportunity by 2020 to survive or else hostility, poverty, criminalities and related tendencies, death, infrastructural decay, and joblessness, among other awful outcomes, will continue to rise beyond the limit. The literature reviewed shows that many Nigerian youths have an iota of computer skills and internet access, which, when jobless, makes them venture easily into cybercrime and brigandage. Many of them are social nuisances who are all out to make cool cash through fewer means. With days going by, the roaring vortex of criminal activities keeps widening in Nigeria. Internet crime has taken new forms, dimensions, and exits with more new shocking cases constantly. It is rumoured online that the rampart criminal activities in Nigeria are denting the image of Nigeria within its comity of states. Criminally minded youths are stealing and engaging in illegal activities, all of which remains unchecked. People are suffering as a result of the perception of Nigeria in the international community. Businesses online are folding up and the quest to get money quickly is burgeoning among youths. Okeshola (2013) opines that cybercrime is becoming a more renown illegal business than the drug trade in the global market. The current high grossing illicit activities of the western world have dented the images and resources of countries, organisations, and private bodies in the rest of the world.

Cybercrime and other related illicit activities, such as corporate espionage, child pornography, fraudulent acts, phishing, and copyright offences, among others, constitute what is called

cybercrimes. It has been discovered by McClintock (1999:3) that those new technologies do not determine the fates of human beings, what they do is to alter the spectrum of potential opportunities within which human beings may act. The relatively low or complete lack of information required regarding the socio-demographic features and drives of cybercriminals can be attributed to a countless number of causes. Among all of these is the main aim, which is the historical trek to the unfortunate circumstances that has been underestimated, the potentially devastating societal effects and impacts of cybercrime and its attendant new behaviours and methods of carrying out nefarious acts.

Cybercrime is all-encompassing. For instance, hacking could be considered as being positively and negatively driven. It is positive when it is meant to control and check anomalies, such is the case in the concept of hacktivism, which entails the use of computing techniques to advocate for ideas, people, events, and opinions for the benefit of all. This might not be termed evil or as a criminal act, but it becomes negative when it is maliciously exhibited and is, as such, destroying people's images and information bases, downgrading and jail breaking networks and computer structures, and stealing people's private information for nefarious acts, among other things. They employ malware, which includes all kinds of malicious software such as spyware, worms, and viruses, among others. Cybercriminals use all other computing weapons to achieve what are, at most times, inordinate ambitions, and goals. Cybercrimes have posed serious threats to everyone, most especially adolescents and youths online in the form of sexual predator and the creation and circulation of promiscuous images.

Many youths and adolescents have seen the entire world from a seductive and pervaded version, in which sexual innuendoes and ostentatious living without the dignity of labour have been seen as a celebrated lifestyle. While elder members of society have been scammed and duped to the point of death through advanced fee fraud, identity theft, blackmailing, online romance scams, copyright infringement, and even contact for the sake of kidnapping for

ransom. People's susceptibility to cybercrimes can be assessed and explained largely due to decision-making biases. There is peer influence as well as low self-control in relating and engaging in online criminally related activities. Globally, it has been recognised that individuals or potential criminals, due to free will, can make measured decisions based on the observed phenomenon, expected utility, and divergent outcomes, and their range of actions and inactions may be limited by such circumstances. Within the ambit of this study, cybercrime perpetrators are viewed as entities who have weighed their options very well before venturing into such antisocial acts. This simply means that they are fully aware of their conductions and the propensity of the offences thereof before journeying into negativity as well as making innocent victims pay for things, they know nothing about. Despite being rationally minded and the consequences of their actions laid out in front of them, they believe even if they are subject to face the consequences of their actions, it is, to them, 'a win-win situation' as the punishments are minimal and the benefits are high (Tambe *et al*., 2020).

Early theories of crime view individuals as being entitled to make choices and decision as a result of free will syndrome as well as them being capable of protecting their destiny by themselves. However, rational choice theory was developed over three decades ago when it became clear that there are traits which need to be discovered and researched so as to have a full understanding of the reasons and motivations behind engaging in criminal related activities. The crusade in identifying crime-producing traits has taken place over the last ten decades but has been met with little success. Rational choice theory opines that for every step taken during the commission of a crime, a choice mode is activated, these being the brain, heart, and conscience, which are called on in deciding whether to continue or discard such acts. Cornish and Clarke (1987) submit that an individual is subject to various thought ruminations, mental taskings, and a large amount of deliberation and weighting of the gains and pains before

carrying out any actions or inactions, as the case may be. This applies to cybercriminals; they are all products of their criminalities and rather than the society in which they reside.

For an individual to engage in cyber criminalities, they must have been entangled in bounded rationality. They must have gone through a mental check as to the rationality of the actions to be taken, with due recall to the pros and cons. Cybercriminals have to have carefully weighed the benefits of their actions and the potential punishments laid down for violators. Hence, cybercrime and other related acts could be massively dealt with provided that government and other stakeholders monitor the various choices people make before venturing into it as well as meting out stiffer penalties to such acts at each stage. This will potentially eliminate cybercrime, in whatever form. The general problems as to why cybercrime thrives is because the benefits of committing fraud, phishing, and online romance scams, among other acts, outweigh the punishments.

On the Economic and Financial Crime Commission (EFCC)'s websites, August 13th, four cybercriminals were caught, quizzed, and convicted by the court for offences which cut across illegal means of collecting money from foreign victims. They were sentenced to three months in prison without hard labour or fine. The three months incarceration can be likened to the T.V reality show BBNaija, these criminals will come out and continue in their old ways of scamming and defrauding their victims without being remorseful or sober. Hence, the punishment meted at cyber bandits serves as an encouragement to continue in such acts, this must be reviewed if the war against cybercrime is sustained. An author, Cornish (20102), argues in his rational choice theory that people's decision to commit a crime is based on cost-benefit proportion. This agrees with George Gasper Homans' theory. It states clearly that people endeavour to achieve and maximise their advantages in whatever conditions they find themselves and try as much possible to reduce errors or lapses that may arise. Above all, choices, and the decision-making process form boundless alternatives, what individuals most

care about is the results or the outcomes. People are more concerned about the instrumentality rather than the action being carried out.

Rational choice theory submits that criminals of whatever form are not forced into their deeds as a result of extra motivation or coercion, they are only products of their behaviours while responding to their innate decisions and tendencies. The same goes for cybercriminals, they do not have different personalities compared to those who do not engage in criminal activities even when the environment is volatile, scary, and hunger stricken. Non-participants engage in their free will to continue working hard with their hands and conscience and wait earnestly for the blessing and products of hard work. Hustlers also have a payday. It is also imperative to note that both cybercriminals and non-participants are not socialised into a criminal belief or cultural system whose norms require crime, they both choose those behaviours based on the rational consideration of the costs and benefits of the intended actions and inactions.

According to Kubrin, Stucky and Krohn (2009), there are countless theories which explain the motives behind people committing crimes. Some of these theories opine those criminalities have a lot to do with the personality of an individual. The concept of personality simply implies a robust, longitudinal predictor of many outcomes Psychologists assert that every individual has uniqueness and peculiarities. They think differently, behave distinctly, and feel separate from others (Carver and Connor-Smith, 2010). A personality comprises of the attitudes, mindset, and characteristics which forms the make-up of an individual, their behaviour, and their modes of doing things. Each individual has an idea of their own personality type, whether sensitive, thick-skinned, or reserved. Hence, criminal acts, most especially cybercrime, are due to a collection of traits or personality types that propel an individual towards said lifestyle.

Some scholars submit that people indulge in criminalities when they are led or when they have found themselves in an environment or cultural setting where drive and love for materialism

and ostentatious living are in high demand. In a classed society, like most African countries, the rich will always get richer while the poor poorer. Hence, the poor will do everything within their power, even acting outside the stipulated rules and regulations, to measure up and attain the most flaunted and celebrated societal prides such as monetary and material success. These individuals, who sit within the lowest rungs of society, are usually denied the modus operandi through which success can be achieved, yet many still claim that criminalities occur only when people are recruited and socialised into cultures, subcultures, sects, and other illegal groups like cults, ritualist societies, brothel societies, or drug syndicates, that tolerate and promote such illegal acts and behaviours.

Some scholars also affirm that potential cybercriminals and other related offence perpetrators would avoid offences for the fear of the potential punishment. The assumption that individuals are free to make a choice, even at choices at the detriment of their lives and those of the people around them, will continue to raise and promote a strong interest in cyber criminalities. For instance, cyber stalkers commit crime after weighing their prospective rewards against the potential risk. Stalking via internet facilities allows offenders to carry out such acts from a relatively exclusively and distant area. This type of offence inflicts the same type of fear and harassment in a victim as if they were in direct contact with cyber stalkers. The rational choice theory has gained popularity and has been widely accepted by many because it allows a rationally minded individual to make decisions. On this basis and through many findings, it is shown that cybercriminals are extremely talented and well educated, not necessarily in a formal manner, but they can make logical statements, cajole victims to make money, as well as use their skills in an illegal form to dupe, scam, and hack people's computing devices and networks.

The analysis of this theory demonstrates the value of personality traits, risk propensity, and logical and critical thinking in various cybercrimes and other related activities and how they relate to the decision-making processes. Cybercriminal personality traits, according to

literature, were found to be the most important factor capable of influencing the execution and success of cybercrime, time-bound acts, an assessment of risks, and the overall efficacy of the attacks carried out. The importance of rationality as a domicile factor has been linked with the financial considerations, needs, motives, opportunities, and inducements of the perpetrator. Many cybercriminals are jobless, this makes the quest to quickly yield to subscribing to cybercrime easy, direct, and widely accepted, without fear or favour. Many cybercriminals are driven by financial consideration when they decide to opt for online fraud and other related criminalities. The continued involvement develops over time. Rational choice theory lays emphasis on the important two core personality traits of every individual, most especially online bandits. These are the ability and capacity of cybercriminals to deliberately assess and weigh the outcomes of their alternative actions and inactions and the strong will to take risks.

To buttress this assertion, the general theory, which was propounded by Gottfredson and Hirchi (1990), assesses both personality traits as two key components that entail low self-control. While with consideration to desist from cyber criminalities, risk related deliberations may be most influential as a dossier for cyber criminalities as they have perhaps engaged in hunting and this has invariably instilled in them palpable fear, caused massive problems, as well as jeopardised their chances of having a legitimate career and life. Also, because they have engrained themselves in such nefarious acts, the quest to leave their life of crime becomes a great problem, hence, getting monetary rewards may, over some time, change into them carrying out their hobby, even if it is disastrous and inimical to the growth of the society at large, but because of a parochial motive they continue their actions.

The rational choice theory postulates that criminals deliberately enter into crime-related activities. They have a good sense of judgment and their actions to themselves in that they have considered their options and evaluated the implications of their actions thoroughly before undertaking them. Cybercriminal and those involved in other related offences have made a sane

and rational choice in that they wish to carry out such nefarious acts, means, gains, and pains. Hence, to prevent criminalities, emphasis should be laid on strong and corrective punishment as a deterrence for others. Keel (2005) opines that in American laws, "three strikes, you are out" policies are a strong yardstick which could be used to measure cyber criminalities in Nigeria society. The historical or family background, such as an individual's upbringing, level of parental education, family socioeconomic status, tribe, and environment may equally go a long way to determine why cybercriminals engage in the activities that they engage in criminal behaviour.

The rational choice theory argues that criminal acts and tendencies are promoted because of perception of them as preventive measures. It's like abandoning the root cause of an ailment while treating the symptoms (Satz and Ferejohn, 1994) For instance, when an individual mentally thinks of exhibiting criminal behaviours, such as defrauding innocent citizens of another country, they withdraw from doing it because of the consequences if get caught. Such an individual can be said to have withdrawn from such criminal acts and tendencies as a result of the punishment already equated with such acts, for example an individual could be said to have been deterred due to the laid down rules in the form of fines or penalties. If this has been the case, many cybercriminals would not have ventured into the swindling mission, irrespective of the gains thereof. Nigeria as a country may not be getting this right as the penalty meted out to cybercriminals is weightless and a non-deterrence to others engaging in it. It is, however, important to note that, coupled with the dynamic and ever-changing social condition of human beings within the society, Nigerians could subscribe to the fact that the poor economy, scarcity of employment, and weak institutional arrangement lead them to such acts.

3.3.2 Criticisms of Rational Choice theory

The rational theory is suitable for this study as its assumptions and behavioural predictions reflect the core reasons underlying the decisions for engaging in crime. However, this approach

has been criticised as its normative assumption of an individual in that decision making is faulty as individuals are not likely to think deliberately, calculate mentally, and assess the pros and cons of every decision before venturing into such acts, particularly not to the level of information processing as presumed by the normative model of the rational choice theory (Tambe *et al*., 2020). Instead, they only make voluntary decisions, without the predetermined motives and consciousness as advocated for by rational choice theory. It is also recognised that while an individual can make a measured decision based on the expected utility of various outcomes, their range of actions may be limited by their circumstances (Kiser and Hechter, 1998). In this context, cybercriminals are thoughtful, energetic, rational, and bold enough to opt for such an action despite their prevailing circumstances and conditions. There is a sole belief that if caught, the gains of duping and scamming people is greater than the potential punishment.

Another perspective to this theory is that it submits that criminalities and other related acts are normal in human society but making opportunities to commit a crime will aggravate tendencies and promote a lawless society in which fraud, corruption, illegality, poor attitudes to work, and ostentatious living without the right sources of income thrive. It is a well-known fact that crimes thrive when there are motivated offenders due to the lapses in society that make them susceptible to committing such crimes and more responsive to such nefarious acts. Secondly, when there is a suitable target, people are willing to double their hard earn currency through illegal means. This has to do with victims who are sourcing more money without work, subscribing to online scams, and falling for fictitious romance scams, among others. Hence, when there is a field of engagement, an avenue to thrive, unlimited fun, and money seekers online due to the vastness of internet availability, then there will always be criminalities in full gear. These and many more who lure unengaged youths to venture into cybercrime and ride on the gullibility of foreign crooks like they do. There must indeed be a suitable target.

The final straw has to do with porous security borders, where there are no facilities and strategies designed to curb people's excesses, criminalities will thrive. Cybercriminal activities would have reduced drastically to the barest minimum in Nigeria, but unfortunately the absence good measures, plans, or strategies to curb the menace of this act makes the county's online infrastructure weak and susceptible to all forms of cybercrime activities (Adesina, 2017, Ibrahim, 2019). This has propelled bandits to garner the energy to continue to thrive in impunity and illegality in the country. Tracking down targets and swindling them has grown to become a syndicated act. People are forming organisations and groups to defraud bodies, institutions, and private individuals irrespective of their location or social standing. Guardians may not necessarily be a shield from targets to cybercriminals, but they are an eye which can destroy the ladder, arrest the situation, and bring to book culprits involved in the game. In Nigeria, there is an absence of a monitoring scheme, as such thriving cases of criminality continue with impunity.

Nigerian youths are seen as the leaders and movers of tomorrow's society. They reflect the society, but what future is Nigeria society laying out for these youths. The nature of the socio-economic and political structure available has not been able to meet the needs, yearning, and aspirations of the Nigerian populace. It is crystal clear that no nation can thrive without due recall to its youthful citizens but with the rising introduction of the internet, crime has been growing. Countless numbers of criminalities are equally borne out the fact that many youths are not properly monitored, encouraged, or orientated, whether by their parents or even the society at large. Many had unbridled access to internet, literature, and graphic materials depicting crimes and nefarious schemes among other things. Some students are exposed through the internet to unwholesome literature by reading junk mail. Some of them visit pornographic sites to share the fun with people of the opposite sex. It is not pleasant for parents and guardians to run permissive homes at the expense of their children and wards.

In Nigeria, the three-pronged emergence of technology through mobile devices, phones, computers, and the internet has given rise for the burgeoning cybercrime. It appears clear that cybercriminals and online bandits ride on the privacy and facelessness provided by the internet to scam, defraud, and swindle unsuspecting innocent victims. Scammers and fraudsters are notable for impersonating and stealing people's identities to perpetrate their acts as well take undue advantage of innocent victims (Tade and Aliyu, 2011; Ibrahim, 2019). Cybercrime has come to stay but the menace is not indelible. Since massive losses suffered by victims create serious image denting and trust problems, many foreigners do not want to partake in any transactions with people from the country, particularly those from specific tribes or regions. Many countries have developed and are still pilling resources and strategies for protecting internet users and preventing, detecting, and containing the excesses and threats associated with it (Shank, 2011). While it is recognised that the strong factor that propels cyber criminalities is greed, as the most victim are covetous, the significance of cyber legislation is of paramount importance in our already crime clustered society. The imperativeness, as well as global best practices in solving such acts, could be viewed within the ambit of the capacity building, public enlightenment campaigns, compliance and enforcement mechanisms, and standards and regulations, among other things. Thus, from these, penalties, and punishments alongside a dossier of information infrastructure must be developed and should be at the forefront of correcting the abnormalities that have pervaded the entire society.

3.4 Conclusion

The dynamic characters of modern society are seen in the mirror as reflections of the porous and weakened institutional arrangements put in place to cater for all and sundry. With the introduction of new patterns and modicums of behaviour and cultural traits in the society, new social changes emerge. Also, with the advent of technology and the predominance of computers and other computing devices, as well as the connectivity through internet facilities which

indirectly force people to live in a global world, there is abound complexities which are overblown and have shown how cyber criminalities have permeated the entire socio-cultural fabric of the society. The entire world has gone global, information seeking, and garnering has also gone global. Thus, in the quest to get information, people become connected, networked, as well as wired and poised to become victims to be duped, harmed, defrauded, scammed, and maimed, as the case may be. In Nigeria, the information technology world came with attendant forces which tampered with the patterns and standards of living. Nigerians and many other people rely solely on technology for many needs, yearnings, and aspirations. However, the abuse and reckless use of technology has given strong backing and rise to new waves and shades of cyber criminalities. The emergence of virtual societies across the entire world came with high risks to health, wealth, and even relationships. This is characterised by instant communication, discussion, sharing, and the sending of money and materials from far and near as well as the geometric growth of anonymity, deceptions, and disguises. Various proven theories and their explanations provided deep bases for the escalation of cybercrimes and other related acts across the world. The in-depth curiosity about the use and abuse of technology and how it has given rise to the growth of cybercrime births various schools relating to the subject matter, such as the classical and modern theorists. The classical theorists posit that the emergence of criminalities can be associated with the advancements in science and technology. While modern theorists advance and discusses the effects of technology on contemporary society which they posit as promoting dehumanisation, separation, and anomie among other things. Post-modernists perceive the world as hyper-real and virtual and full of faceless fantasies, simulations, and technological intensities which promote spatial interactions and provide anonymity to cyber criminalities and those engaged in other related activities. This study employed two core theories with opposing views to peruse the rationale behind engaging in cyber criminalities within the nation of Nigeria. The main criminological theories discussed

are strain and rational choice theory. Strain theory by Robert Merton submits that society is guilty when talking about why people engage in criminal activities. He opines that society births leverage for people to pursue inordinate ambitions through any means. Strain theory condemns society, while rational choice theory states that criminalities occur because of the benefits accrued to it and the gains thereof outweigh the pains when caught. The potential consequences are trivial compared to the privileges of going scot-free if the decision made is executed successfully. Many institutions are unwilling to employ legal means to avoid image denting which may harm the perception of their products and services. Rational choice theory submits that to fight and combat cyber criminalities heavier corrective measures should be meted towards online bandits and criminals, which should be packaged and codified into Computer Misuse Acts.

It is an affirmative fact that cybercrime has a serious psychological impact on society in the form of image denting, economic losses, the collapse instructional arrangements, and the development of psychological disorders, among other things. Even when many suffer massively from its hurts, the most vulnerable are youths and adolescents, who are frequent users of the internet, whether for fun or illegitimate dealings. Contemporary adolescents and youths are technology-wise, savvy, and employ opportunities for various purposes, ranging from social media activities to buying and selling online. With a reasonable number of youths using the internet, it is of paramount importance to investigate how these networks and their usage are employed by cybercriminals to lure people. It became necessary to carry out a criminological study which would x-trays the lived experiences of cybercrime perpetrators in South-West Nigeria.

CHAPTER FOUR
RESEARCH METHODOLOGY

4.1 Introduction

This chapter focuses on the methodological approach used in addressing the lived experiences of cybercrime perpetrators ('yahoo boys') in South-West Nigeria. While there is wide-spread literature on cybercrime in Nigeria, many have categorised the menace as an old-age social problem because of the incessant activities characteristically perpetrated by youth.

The methodological approach adopted by research determines the process of gathering information. Therefore, research methodology is considered a strategy, action plan, process and design that supports the choice and the implementation of specific methods in achieving the objective of a study (Crotty, 1998). To begin with, this chapter accentuates the difference in the meaning and application of research methodology and the methods since both terms serve different purposes in the study. It is important to explain and appreciate the shades of difference between them because the meaning and use of such definitions remain a subject of controversy. Emerging scholars associated with some peer-reviewed journals have classified using a methodology in the place of methods, while others replace methods for methodology. Therefore, there is a need to dissect these two concepts.

First, research methodology comprises the systematic process the research study should undertake before the aims and objectives of the study can be achieved. For instance, it brings up the theory of how research can be conducted (Saunders *et al.*, 2009). Conversely, research methodology emphasises the research design, such as the phenomenological design adopted in this study that addresses the questions of what, how, and when in the study's approach to the research questions. Further, it explores how the researcher proposes to address the research problem of the study. Secondly, a research method explains the systematic process and the techniques used to collect and interpret research data. It utilises structured, semi-structured, or

unstructured methods, interviews can also be generated from individuals and observations for qualitative research methods. It also includes the use of statistical tools and questionnaires for quantitative research methods (Qu and Dumay, 2011).

Finally, to capture appropriate explanations for issues related to the methodology and methods used in this study, this chapter is divided into research philosophies, research approaches, research design, data collection techniques, sample size and sample technique, and the population of the study. In the same way, the chapter depicts the instruments and procedures used to ensure the credibility and trustworthiness of the research, the steps and methods adopted for data analysis, ethical consideration, and how the challenges faced during fieldwork were addressed. Also, the study location is discussed. Consequently, these themes are positioned to shed light on the complete activities provoked for addressing the research questions.

4.2 Research Philosophy

To achieve the aims and objective of this research, it is important to capture philosophy underpinning this study. According to Saunders (2009), significant assumptions can be made by looking at the philosophy of a study; the philosophy describes the researcher's perspectives of understanding the world. The key question faced by many researchers is, how knowledge is created and developed. However, to find answers to this question, the researcher must utilise a research philosophy that underpins the study. According to Saunders *et al*. (2015), a research philosophy refers to the various types of perspectives or beliefs employed for a specific study which influence the choice of research design, techniques, strategies, and analysis which will be utilised to meet the research objectives. This philosophical belief helps researchers to conceptualise the phenomenon or topic to be investigated and describes how the researcher proposes to go about investigating it. By doing so, the researcher gains a clear understanding of the phenomenon (Gill and Johnson, 2010). This study, therefore, highlights four major types of research philosophy and adheres to the most suitable for the study. The following are the

types of research philosophies; interpretivism, positivism, realism, and pragmatism. This study, therefore, adheres to interpretivist approach.

4.2.1 Interpretivism

Interpretivism originated in Europe between the early and mid-twentieth century and became popular through the work of German and French philosophers. The interpretivism believe that the researcher should be aware of the differences between humans in terms of their responsibilities as social actors (Saunders et al., 2009, p.116). This philosophy of any research is based on the central concept of the researcher's interpretation of human social roles in connection to the set of meanings derived from the research study itself. The fundamental sources of interpretivism are two traditions: phenomenology and symbolic interactionism, which are both rooted in the philosophy of mind. Phenomenology can be defined as the process through which humans make sense of their experiences. Symbolic interactionism sees humans as continuously and engaged with interpreting the social world by interpreting other people's actions with whom the researcher interacts.

Interpretivist scholars contend that people of different cultural backgrounds make different meanings and thus establish and experience social realities under different circumstances, different times, and at different levels (Crotty, 1998). In other words, interpretivist scholars are critical of the positivist attempts to find concrete, universal rules that apply to all. Instead, they encourage the need for researchers in their capacity as a social actor to demonstrate deeper understanding on the topic or phenomenon under investigation so as to grasp a better understanding of their participants. This can be achieved if the researcher does not manifest some kind of sympathy (Saunders *et al.*, 2009). Also, Saunders (2009), opines that the significance of interpretivism philosophy is centred on the willingness to engage in research while adopting an empathetic position. Interpretive analysis is holistic and contextual, rather than being reductionist and isolationist. Interpretive interpretations tend to focus on language,

signs, and meanings from the perspective of the participants involved in the social phenomenon, in contrast to statistical techniques that are employed heavily in positivist research. The need to investigate and interpret the social context of participants, as acknowledged by the interpretivist school of thought, provides ample understanding of events in their world that captures the qualitative dimension of this study where they lived experiences of cybercrime perpetrators are uncovered through semi-structured interviews. This study employed a qualitative method and an interpretivist philosophical assumption as the standalone research philosophy.

4.2.3 The Rationale for the Research Philosophy Employed in this Study

Interpretivism approach is well-suited for investigating hidden causes of multiple social processes and complicated phenomena, such as delving into the lived experience of cyber criminals, where quantitative evidence may be erroneous or otherwise difficult to collect. A phenomenon such as cybercrime (yahoo-yahoo) is explained by the researcher based on previously conducted research and published literature on the subject matter in question. Moreover, qualitative research is adopted for this study which is related with the interpretivism approach. Conversely, this approach is suitable for this study to understand the research problem, in light of the research questions, it becomes necessary to adopt a qualitative research method to investigate the lived experiences of cybercrime perpetrators in the South-West region of Nigeria. This research philosophy incorporates a human interest in the study and promotes qualitative analysis over quantitative analysis in an attempt to generate multiple meanings from the responses of the participants. This means that a semi-structured interview was used to provoke qualitative responses from cybercrime perpetrators, popularly referred to as ‘yahoo boys’ in Nigeria. Through these interviews their knowledge and perceptions of cybercrime in Nigeria were uncovered and analysed with qualitative content analysis tools. To

put this into perspective, the choice of research philosophy for this study offers answers to the research questions.

4.3 Research Approaches

A research approach is a plan and process consisting of different steps employed in gathering, analysing, and interpreting data (Johnson and Onwuwgbuzie, 2009). It thusly focuses on the essence of the issue being investigated through the method of data collection and data analysis. The research approach is divided into two different types, these being inductive and deductive approaches. The choice of either of the approaches for a study is largely dependent on the philosophical premise on which the study is rested. For instance, the assumptions of the interpretivist scholars are usually predictive and thus take an inductive approach, whereas the assumption of the positivists leans strongly towards the deductive approach (Creswell, 2014; Sekaran and Bougie, 2016). It is enough to conclude that, on the one side, the deductive method is biased towards the objective evaluation of the construct (quantitative), and on the other side, the inductive method is intensively assisted by the subjective (qualitative) exploration of the research issue. According to Newman and Benz (1998), cited by Creswell (2014), it is argued that it is not appropriate to consider qualitative and quantitative approaches as, "rigid, distinct categories, polar opposites, or dichotomies, rather they represent different ends in a continuum". This implies that research can appear to be more qualitative than quantitative or vice versa. These two research approaches are discussed below.

4.3.1 Qualitative (Inductive) Approach

The qualitative research approach employed in this study, also known as the socio-anthropological approach to research, is historical, intuitive, and empirical by nature. The main purpose is to seek a deeper understanding of complex situations. It is typically exploratory, more systematic, and emergent, with precise focus on the research design, measuring instruments, and data interpretation which could swing along the way. The philosophical

position of the qualitative approach assumes that reality is not easily divided into measurable values. Therefore, an inductive approach specifically explains how findings are interpreted in their real-world (Lancaster, 2005). For example, an investigation seeking a comprehensive understanding of why and how a social issue or phenomenon exists, such as cybercrime activities among Nigeria youth, will focus its concentration and importance on the inductive exploration of the phenomenon at hand rather than statistically analysing the problem (Bryman and Bell, 2011). A small sample size, as opposed to large sample size, will be needed to reflect upon a particular context, as would be the case for a quantitative deductive approach (Smith *et al*., 2008). This study calls for a thorough exploration of the phenomenon, therefore, a small sample size of cybercrime perpetrators was interviewed. The qualitative or inductive approach appears to be result-driven where participants are questioned on their understanding of a research problem, this occurred in the context of cybercrime in Nigeria. Therefore, it is necessary to denude the narratives of cybercrime in Nigeria from the perspectives of the perpetrators. In comparison to the deductive quantitative approach, Johnson and Onwuwgbuzie (2009) argue that the inductive approach is subjective because of the immense involvement of the researcher at the point of collecting and analysing data.

The extensive scope of this approach assists researchers to collect data through sufficient observation and explanation during the process of conducting the research. It contends that trustworthiness is more important than attempting to rigorously describe what is being observed or researching the entire phenomenon. In an attempt to investigate any social issue, qualitative approach assists researchers to depict the "virtues of qualitative terms outside of the parameters that are typically applied in quantitative research, credibility and internal validity are also considered to be parallel concepts" (Bayens and Roberson, 2011). Trustworthiness is an essential aspect of this approach; it seeks to study the entire situation to evaluate the phenomena. Therefore, the inductive approach sufficiently supports the qualitative strand of

this study. This stance is also linked with the interpretivist philosophical assumption embraced in this study.

4.3.2 Justification for Selecting Qualitative/Inductive Approach

The above exposition examined the strength and importance of both inductive and deductive approaches. This section explains the justification of choice made by the researcher in the study. The inductive approach of generating data is aimed at exploring a social phenomenon, for example cybercrime, the subject under investigation which is destroying the moral fabric of Nigerian society. This study is connected to the assumption of inductive research which allows the researcher to examine social phenomenon. Therefore, the adoption of this approach is considered suitable for a study of this nature which seeks to explore a rich explanation of individual experiences (Denzin and Lincoln, 2003:16). Similarly, the qualitative method of generating data has often been recommended for studies that intend to elicit the contextualised nature of experience and action and attempt to generate analysis that is detailed, "thick and integrative" (Liamputtong and Ezzy, 2005:2). Hence, adopting this approach aimed to inspire this study to outstrip the inadequacy of questionnaires and to avoid potential errors produced by a dominant, quantitative approach centred on a positivist paradigm. Therefore, this study utilised an inductive instrument, like the semi-structured interview which was utilised to harvest data from the participants of this study, rather than a deductive philosophical assumption that prefers to administer questionnaires to sampled participants.

4.4 Research Design

A research design is a strategy used to oversee the collection and analysis of data; it addresses the research questions of a study. Therefore, it is significant to state that all academic and scientific research can be achieved through a particular research design. Having mentioned earlier, the methodological design is a philosophical assumption that is related to the methods the researcher adopts in conducting research. In the process of actualising a study through the

application of fieldwork, researchers utilise inductive reasoning to gather ample understanding of the topic within its context and thus uses an emerging design (Creswell, 2007). Further, Smith (2009) opines that qualitative research studies contend to describe and interpret personal and social experiences and to divulge a rich description of the topic under investigation. Therefore, this study adopted a phenomenological design to explore the experiences of the participants of the study. Phenomenology has been described as a principal object through which phenomenologists seek to particularly explore the experiences of the participants in a study.

Therefore, in attempting to explore a phenomenon, qualitative research seeks to provide a comprehensive understanding of individuals' experiences (Louw and Louw, 2007). Also, Denzin and Lincoln (2005) suggest that qualitative research examines the social issues in natural settings and attempts to makes sense of the phenomena. Therefore, the method used to gather information was talking to the participants and seeing them behave in the context of the phenomena, which is an integral aspect of qualitative research. Besides this, qualitative research suggests the 'how and why' questions of a phenomenon. The nature of this research is qualitative and this, therefore, suggests that the research is non-experimental and thus based solely on the participants' expressions and experiences (Newman 2003). Different from other approaches, sequential strategies are not part of phenomenological research but rather include an understanding of the processes that are used for guidance to establish plans suitable for the investigation of the phenomenon. Characteristically, the purpose of phenomenological designs can be achieved through human experience that entail phenomenological inquiries. Over and above, phenomenology stresses subjectivity over objectivity, as it depends more on description and interpretation. In this case, the position of the researcher is to observe and explain a well-known social phenomenon.

Finally, this study rests on the social constructivist paradigm, in which an individual seeks to understand the society they live and create meaning of these socially constructed experiences. Social constructivism imparts grandness on the importance of culture and context when a researcher seeks to understand a particular phenomenon as human development is socially constructed within these concepts (Ornmston *et al*., 2014). Participants in this study were observed inductively to capture their experiences, while at the same time unravelling the meaning attached to the phenomenon (Gray, 2004; Willig, 2003). To gain insight into the lived experiences of the participants regarding the phenomenon, the phenomenological design was considered the most appropriate, because the phenomenological approach to qualitative research generally aims at identifying, explaining, and validating the commonality of the lived experiences of a particular group (Creswell 2010).

4.5 Phenomenological Method

This section dissects the concept of phenomenology and how it is related to this study. Phenomenology is a method of abstemious reflection on the fundamental structures of the lived experience of human existence. Method in this context refers to the technique or approach with which a phenomenon is approached. And abstemious is the ability to think critically while avoiding presumption and emotional influences (Willis, 2014). Phenomenology is a pre-reflective method of gaining access to the world as we experience it as humans. Ordinary human experiences are things that we go through in our day-to-day existence. Our day-to day experiences can be conceptualised as pre-reflective experience from a phenomenological point of view. Conceptualising phenomenology from a philosophical point of view, Van Manen (2016) posit that phenomenology is largely an inquiry-based philosophical approach of asking, rather than a way of answering questions, discovering, or drawing definitive conclusions. However, there are possibilities and potentialities for experiencing openings, understandings,

and insight, as well as producing cognitive and non-cognitive perceptions of existentialities, as well as providing glimpses of the meaning of occurrences and events in their uniqueness.

As Van Manen (2016) rightly noted, phenomenological research is the school of philosophical ideology and beliefs that qualitative research rests upon. This type of research is a distinct qualitative method for exploring fundamental structures, such as the common meaning of social phenomena. In the words of Van Manen (2016),

> "As Human beings, we live in a world that is given to us and actively constituted by us, therefore, is it important to reflect on it phenomenologically, because this provides us with the possibilities of individual and collective self-understanding and thoughts".

This quote describes the importance of examining the life and journey of human existence because it is a chain of lessons which should be lived to be understood. Flowers and Larkin (2009) argue that phenomenology is not only interested in our experiences as people but is primarily concerned with our perception of our worldly interactions. Correspondingly, Vaviani (2011) opines that the understanding these experiences gives the researcher insight into the experiences of the participants and creating meaning from these experiences becomes necessary. Through the process of making meaning, people understand their outside world. This is an integral aspect of phenomenological research. In light of this, it is the responsibility of the researcher to collect data from individuals that are engaged with the phenomenon and then create comprehensive discussions of the experiences of those involved, as stated by Creswell (2007).

Phenomenology is popularly enhanced with a detailed description of a person's personal experience of specific societal problems and issues. Given this, Creswell (2013) maintains that phenomenological studies are distinctly set aside for addressing detailed understanding and the knowledge of a person's experiences. However, to achieve the essence of phenomenological

design, semi-structured and in-depth interviews are important because they urge participants to reflect on the meaning of their experiences in a manner beyond possibly ignoring the true complexity of a societal problem related to their present circumstances (Creswell, 2013). The main objective of phenomenological research is to investigate what an experience means to a person and how they narrate a comprehensive account of their experiences, and hence, their experiences provide a universal meaning, as described by the person (Bevan, 2014). This study, through descriptive phenomenology, focuses on both the description of the participant and the researcher's interpretation. In the course of conducting interviews with the participant, the researcher, in his capacity, utilised bracketing. This is to assist the researcher to nullify preconceived impressions of the phenomenon which were gained from the general discussions around the phenomenon in Nigeria. In consideration of the individuality of the experiences of each participant, bracketing allows the researchers to approach the participants with a "sense of newness" (Creswell, 2007).

The explanation above reflects that this study is phenomenologically set out to explore the lived experiences of cybercrime perpetrators in the South-West region of Nigeria. This is to establish a clear consciousness of their mind regarding their activities by concentrating on the following questions:

- What are the key narratives among cybercrime perpetrators and their activities concerning cybercrime in Nigeria?
- What are the perceived circumstances which led some Nigerian youth to become involved in cybercrime?
- What meaning do cybercrime perpetrators construct out of their criminal activities?
- What are the links between their lived experiences and the ineffectiveness of the mechanisms put in place by the government?

In reality, the study under investigation demands a design that can make meaning from the participants' experiences. Therefore, this study necessitates the collection of qualitative data and demand the use of phenomenology research design.

4.5.1 Exploratory Research Approach to Phenomenology

Creswell (2007) depicts exploratory research as a prerequisite needed to explore a population and, "hear the silent voice". Creswell stresses the importance of exploring a social phenomenon concluding with predetermined information that exists in pieces of literature. Qualitative exploratory research is conducted to understand the context within which participants' addresses and explanations to the researcher describe the circumstances that birthed their actions and the environment in which they act. Further, De Vos *et al*., (2011:95), views this approach as a way to explore how things are and what they represent. By doing so, it systematically allows the researcher to develop a deeper understanding about a phenomenon and, from this perspective, the researcher attempts to identify and provide a rationale for reoccurrences of a phenomenon or its causes. This type of study aims at testing scientific predictions and research findings. Reflecting on the demography of studies on cybercrime in Nigeria, there seems to be a dearth in the voice of the perpetrators. To gather rich information for this study, the researcher ensures that the selected participants are well informed on the topic under investigation, this is to ensure they are comfortable to discuss and to give the researcher vital information.

4.5.2 The Quest for Adopting Phenomenology: The Researcher's Perspective

In the course of the researcher's previous fieldwork in 2017, which explored youth's perceptions on 'yahoo-yahoo' in Ado-Ekiti, Ekiti State, Nigeria, the researcher was privileged to meet some 'yahoo boys', as they are popularly called. Although, various informal conversations with some of them left the researcher troubled by the abundance of challenges that fuelled their involvement. For example, some of them claimed that the socio-economic

situation in the country and a lack of belief in the stakeholders and the government with their expected resources were major reasons for their involvement. Also, some admitted that laziness on their part to cope academically in school was a justification for them to embrace the 'yahoo-yahoo' enterprise. However, their laziness is not replicated in their commitment to the 'yahoo-yahoo' enterprise. In their views, some of them admitted to the fact that cybercrime is a way to reach their expected goals without conforming to the normative way of achieving them. In some of the conversations, their zeal to continue and not quit became evident to the researcher.

These conversations, therefore, encouraged the researcher to investigate the experiences of being a 'yahoo boy'. 'Yahoo boys' implicitly describe their understanding and learning process based on the perceptions of their environment. Merleau-Ponty (1945 and 1962) argue that as individuals we grow to fill the space and environment that we exist in. This idea fascinates the researcher and provides desire to unpack the motivation behind this famous group of individuals called 'yahoo boys. The essence of this journey is to ransack their hidden world in their subconscious mind and to understand how they perceive themselves, either as a 'yahoo boys' or as criminals. To understand how these group of individuals experience being cybercriminals or how they perceive themselves will assist the researcher to hear their silent voices and understand their journey. At that time, it never occurred to the researcher's consciousness that he was aiming at pursuing a phenomenology study.

4.5.3 Limitations and Strengths of Phenomenological Research Design

When undertaking a phenomenological research study, it is essential to understand the pros and cons. One of the key strengths of a phenomenological design is its ability to bring on board a unique perspective on the phenomenon by investigating the views of the people who have experienced the particular phenomenon rather than evaluating how the phenomenon exists in a vacuum. The most significant strength and weakness of a phenomenological qualitative inquiry and analysis is the human factor. This provides a robust understanding of the human

experience which allows findings to emerge rather than them being imposed by the researcher (Patton, 2002). This approach gives the researcher the opportunity to understand the phenomenon and the perceptions and perspective of the respondents, and then use the findings to create an understanding of their experiences. Maxwell (2013) suggests this to be an advantage if researchers have a keen interest in the topic.

Beyond the above advantages of phenomenological design, in that it provides rich and convincing data, some limitations are obvious. To start with, from an individual and broad perspective, the issue of bias remains a subject of controversy when using this design. A researcher's induced bias can have an impact on the study, and this is predominantly true in phenomenological research (Creswell, 2014; Janesick, 2011; Patton, 2002). furthermore, this design is subject to interference in the interpretation of data, which may arrive as a difficulty when trying to maintain and establish pure bracketing. Bracketing in phenomenological research is the setting aside of personal experiences, biases, and preconceived notions about the research topic (Beech, 1999). This demands that the researcher set aside their understanding of the phenomenon in an attempt to understand how others experience the phenomenon by detailing the respondents' experiences with the phenomenon.

4.6 An Overview of the Three fieldwork Sites

This study was conducted in three research locations: Lagos, Ibadan, and Ado Ekiti. These research locations are located in the South-West region of Nigeria. These study sites are very distinct from each other. As such, in this section the demographic data form the sites will be discussed separately and in detail. after which the reasons for selecting these study sites are discussed as well.

4.6.1 Lagos City

Cybercrime as a culture is popularly called 'yahoo-yahoo', as used widely across the country of Nigeria, and it is not only perpetrated in Lagos. In Sub-Saharan Africa, Lagos is the largest

city in the Nigerian state. It is one of the fastest growing economies in the world. The metropolis of Lagos consists of the island and the mainland, which are further divided into 20 local governments. The economic capital and formal federal capital city of Nigeria was chosen as one of the study sites for this study since the bulk of Nigerians live there. The metropolitan area of Lagos has a population of almost 20 million and is Nigeria's most populous urban centre (New York Times, 2015). It is projected that 78 per cent of metropolitan population growth is caused by rural to urban migration. Nevertheless, the lack of an efficient transport network in the metropolitan area has turned transportation chaos into a metropolitan feature. The metropolis of Lagos has the highest attention to trade in Nigeria. More than 80 per cent of Nigeria's maritime businesses are traded in Lagos. Besides this, the city has the busiest airport in the country. The city of Lagos consists of five tertiary institutions that include both private and public universities. There is also the presence of some notable five-star hotels. In 2006, UN-HABITAT predicted that by 2020 Lagos would become a megacity, with an estimated 35 million inhabitants. Because of its cosmopolitan status, the city has the highest concentration of cybercrime perpetrators in Nigeria. The massive land space of Lagos city restricted the researcher to a certain area where the study was conducted. The researcher aimed to explore the lived experiences of some of the cybercrime perpetrators in this region.

Some participants for this study were recruited on Lagos Island, specifically from Lekki. This was an area of concentration for the researcher so as to understand the dynamics and perceptions around 'yahoo boys' in these locations. It is believed that high profile 'yahoo boys' reside in this location in order to engage with their enterprise. Therefore, the researcher assumes it is imperative to draw comparisons between the 'yahoo boys' from Lagos Island and the mainland, as well as the other study locations. Truly, the calibre of 'yahoo boys' in these areas is distinct from other 'yahoo boys' in the city and across the South-West region, because of their profligate lifestyle. There is not much difference between the celebrities and successful

businessmen who live in the area and the ‘yahoo boys. In contrast, Ikeja and Ikorodu were other areas in Lagos where participants were recruited for this study. On the mainland, these regions comprised of different categories of ‘yahoo boys’, among which are undergraduates, middle-class ‘yahoo boys’, and those aspiring to be part of the most popular youth culture in Nigeria. Therefore, the Lagos metropolis was considered appropriate as one for study sites to harvest data that would be useful for the study.

4.6.2 Ado-Ekiti

The dominant activity of cybercrime among youth is like a cankerworm that has penetrated deeply into Nigerian society, and over the years has mounted into a glamorised culture, especially among undergraduates. Ado Ekiti is another study location where data was generated for this study. The city is located in Ekiti State, in the South-West region of Nigeria and it is recognised as the capital city of the state. The predominant ethnic group in the city are Yoruba people. However, the existence of some tertiary institutions located in the city has assisted the city to grow in size and population. These tertiary institutions consist of the state university, popularly known as Ekiti State University (EKSU), Federal Polytechnic, Ado-Ekiti, and a private university named Afe Babalola (ABUA). The existence of these institutions contributes to the social organisation of cybercrime among undergraduates in the state, and thus, precipitated the choice of the location.

Cybercrime perpetrators found in Ado Ekiti were likely to have common characteristics with other perpetrators in other cities within the country, assuming the fact that the phenomenon of ‘yahoo-yahoo’ is common among youth and undergraduates irrespective of their location or ethnic affiliation. However, the researcher insisted on Ado Ekiti as one of the study sites because of limited funds and his familiarity with the terrain, since there is easy accessibility to participants in the area. ‘Yahoo-yahoo’ boys recruited for the study in Ado Ekiti provided an

insight into their lived experiences by narrating the factors that influenced their participation in cybercrime.

4.6.3 Ibadan City

The city of Ibadan is the most populous city in Oyo state. According to the National Population Statistics in 2006, Ibadan, the ancient capital of Oyo State with a landmass of 27,249 square kilometres, had a population of about 5.5 million. Oyo State has 33 local government areas (LGAs), with Ibadan being the capital and the administrative headquarters of the state.

Ibadan's economic activities encompass farming, trade, crafts, factories and other commercial services. Ibadan is a major business centre and almost every corner and street of the traditional city centre has a market square or stall, even in the inner suburbs. Ibadan is divided into 11 LGAs: five in the city and 6 in the peri-urban areas. The population of the area is mainly Yoruba. Ibadan North, Ibadan South-West, Ibadan North-West, Ibadan North-East, and Ibadan South-East are the five urban LGAs in the Ibadan metropolitan area.

4.7 Study Population and Sample Size

A population is identified as the total number or group of individuals or events to be analysed by a researcher to generate data using the selected sample (Sekaran and Bougie 2016). In conducting a research study, population refers to the entire collection of elements through which a phenomenon can be explored (Sekaran, 2003). Conversely, Okeke (1995) defines a population as all conceivable elements, subjects, or observations relating to the phenomenon of interest to the research. The population for this study is cybercrime perpetrators within South-West region of Nigeria. The prospective population of cybercrime perpetrators were ranging from the penal age of 18 and above. The criteria of this age were based on the assumed maturity of the participants and their ability to be coherent when giving an account of their lived experiences over the years.

Furthermore, gender peculiarity in the sample population was not considered because the 'yahoo-yahoo' enterprise is dominated by males. The projected possible sample for this study was originally 40 participants, however, due to the significant arrest of cybercriminals by the EFCC across the country, the participants were limited to 29. The participants comprised of 29 male participants who were purposively selected for a semi-structured interview across the study locations, 7 from Lagos Island, 11 from Ado-Ekiti, and 10 from Ibadan city. The numbers of participants interviewed across these cities were based on their availability and willingness to participate in the research. It is also important to state that even though the research set out to interview 40 participants, the researcher was only able to get 29 across the cities who were willing to participate in the study. Part of the observable reasons that might have influenced this number is the remarkably high spate of arrests and prosecutions of cyber criminals around the time the researcher carried out the field work. Mason (2010), cited in Creswell (1998:64), suggests that in a phenomenological study this sample size is sufficient to understand the key narratives and commonality among cybercrime perpetrators. Besides this, qualitative research enjoys a small sample size for the level of detail required to investigate a research question.

4.7.1 Sampling Techniques

Sampling is commonly characterised as the method of selecting a certain number of individuals in a sample, such that the selected person will represent the large group since the sample of a whole population is essentially unworkable (Creswell, 1999; Pattern, 2005). In the same vein, Sekaran and Bougie (2016) view sampling techniques from two lenses; probability and non-probability sampling. Probability sampling requires all elements of a given population to have the same probability of being selected as the entire population. In other words, the participant is selected randomly from the total population. However, referring to non-probability sampling, not all elements that make up a population have the same probability of being in the same representative sample, and research questions that rest on the quantitative paradigm are not

answerable under this technique (Saunders *et al.*, 2009). Equally, simple random, systematic, and stratified sampling techniques are classified as research strategies within probability sampling, while non-probability consists of purposive sampling, convenience sampling, and quota sampling, respectively (Sekaran and Bougie, 2016; Saunders *et al.*, 2009). Thus, given the nature of this study, the non-probability sampling methods were adopted for qualitative data collection (in-depth- interview).

As fitting for this study, purposive and snowballing sampling techniques were adopted to select the participants. Purposive sampling, also known as judgment sampling, is a technique in which a participant is deliberately chosen based on the characteristics that the informant demonstrates. This approach is a non-random technique, because it does not necessitate the use of underlying theories or a predetermined number of informants (Bernard 2002, Lewis & Sheppard 2006). In simple term, the researcher determines what information is required and then sets out to locate individuals who are capable of and ready to supply the information as a result of their knowledge or experience. Yahoo boys in this context are key informants and observants that have a broad knowledge about several internet frauds and willing to share their knowledge. Conversely, due to the clandestine attributes of cybercriminals they can referred as a hidden population. A hidden population, such as the yahoo-yahoo boys, is a subset of a population that are inaccessible because of their criminal activities, therefore snowballing is most suitable to recruit participants from this population. Snowballing is built on the logic of social networks, in which people are linked together by a web of social interactions and connection. Participants are asked to name or reference additional people who are eligible for a research population in order to take advantage of this social network (Petersen and Valdez, 2005).

This approach was utilised in selecting participants for the in-depth interviews, and the procedure of selecting participants followed the primary criteria, purpose, and significance of the participants to the theme of the study. Sekaran and Bougie (2016) opine that purposive

sampling is adopted in a study when relevant information is confined primarily to a group of small of individuals who possess extensive knowledge and are in a better position to give such information. Thus, to answer the research questions, the researcher takes on the responsibility of identifying these individuals who are willing to provide rich information for the sake of the study. The selection of participants, locations, and other sample units are purposive (Mason, 2002; Patton, 2002). According to Manion and Morrison (2011:156), researchers deliberately choose purposive sampling for certain reasons. Firstly, to able to make a comparison, to concentrate on specific issues, to achieve representativeness, and finally, to generate theory through accumulated data from various sources. Purposive sampling is suitable for this study since the aim of the research is to investigate the lived experiences of a specific and unique group, colloquially referred to as 'yahoo boys' in the local parlance of Nigeria.

The recruitment of appropriate participants for this study was facilitated by ensuring that participants all understood the aim of the study. Highlighting from the researchers' fieldwork experience in 2017, the researcher made initial contact with some 'yahoo boys' who started the referral chain for the recruitment of participants for the study. However, their choice to participate in this research was strictly voluntary and based on severe privacy and anonymity. To be fair on part of the participants, it was a difficult period to participate in a study that seeks to explore the lived experiences of cybercriminals because the Economic and Financial Crimes Commission (EFFC) was clamping on 'yahoo boys', but having access to an informant, Dr Buhari, a lecturer from the department of sociology Ekiti state university, was indispensable. Because of the nature of cybercrime, as carefully unpacked in the literature review section, information sharing, and networking are some of the strongest attributes of the illicit industry. As such, perpetrators build a wide range of contacts with others within the same trade across the country, but this research relied on the social network of the participants already identified

to make referrals for friends based in Lagos, Ibadan, and Ado-Ekiti only. Hence, the choice of snowball or referral sampling as explained above.

4.7.2 Data Collection Instrument

There are different types of interviews, including structured, semi-structured, and unstructured interviews. The adoption of any these interview methods is largely based on the requirement of the study (Sekaran and Bougie, 2016; Wilson, 2010). This research endorses the semi-structured interview method to investigate the lived experiences of cybercrime perpetrators in South-West Nigeria. Ritchie *et al*., (2003) describes the use of semi-structured interviews as an interview technique which is widely used and that follows a pattern to address key themes rather than particular questions. This allows flexibility during the interview process and enables researchers the opportunity to probe responses further and elaborate on explanations for the comprehensive coverage of developing themes (Rabionet, 2011). A semi-structured interview is required to have a flexible structure that is constructively tailored to benefit the research purpose. This flexibility is typically supported by an interview guide that outlines key questions for the interview, equally, the interviewer can amend the chronology of questions or probe with additional questions for clarification if necessary (Ritchie *et al*., 2014). According to Ritchie *et al*. (2003), the most suitable interview format for qualitative research is typically semi-structured interviews, otherwise known as moderately scheduled interviews. An interview guide with questions was adopted to direct the interview process and ensure that interviewees answered the same questions (see appendix). The interview guide was not intended to limit the researcher and the participants, because the researcher had the liberty to explore beyond the questions mentioned in the guide to obtain a more thorough understanding of the participants' opinions. Nevertheless, this liberty to probe further does not imply a change of questioning different from what the interview guide contains, but rather a follow up to elaborate unclear responses.

The selections of interviewees across the South-West region were to expand and offer a comprehensive understanding of the research problem from a different individual perspective. Each interview lasted 45 to 60 minutes and all responses were recorded during the interview with an audio recorder to allow the researcher to focus on the interview as it developed. The study participants provided consent to the use of a tape recorder before the commencement of the interviews. They were also reminded about their confidentiality through the interview and were also informed that the study is merely for academic purposes, hence, they were assured their identities would be protected. The interviews were conducted in English and recorded and transcribed at the end of each session, each of the participants was handled a notebook and a pen as an incentive. Also, the researcher took notes during each interview and gave each interviewee a distinct identity. Field notes are used in conjunction with interview questions that could be treated as a secondary data construction method, as expressed by Miles and Huberman (1984) and Emerson and Shaw (2011). Throughout the data collection process, field notes were utilised to observe the mannerisms of the participants by taking note of participants' choices of words, gestures, and posture. This provided an understanding of participants' emotional expressions, reflecting the mood and atmosphere in which the interview was conducted.

4.7.3 Describing In-Depth Interviews

In-depth interviews are one of the main methods of data collection used in qualitative research. Gray (2013) regards in-depth interviews as one of the most effective qualitative approaches that reflects the human voice in research. It offers both the participants and the researcher a mutually beneficial opportunity to engage and speculate on the topic under investigation, while there are incentives for participants to express themselves. This qualitative approach encourages participants to narrate their stories and also assists the researcher to gain an inside experience into social reality (Ritchie *et al*., 2013). In reality, people find it emotional to discuss their experiences and have someone listen to them. This suggests that interviewers who engage

participants in an in-depth interview have strangers trusting them with their experiences and stories. Consequently, this approach is structured to capture participants' perspectives in a fully informed way. This approach has been characteristically described as a conversation with intent because it reproduces the fundamental process through which knowledge about the social world is reconstructed (Rorty, 1980). Also, qualitative research can be conducted using different data collection techniques, perhaps in some cases, one technique can be adopted. Data collection in qualitative research maybe divided into four categories: firstly, the participant's observation; secondly, direct evaluation, or the non-participant's views; in-depth interviews and the examination of the documents, respectively (Kawulich, 2005). However, this study adopted the in-depth interview technique as the primary source of qualitative data collection. This technique involves conducting well detailed interviews with individuals to explore their perspectives on a particular phenomenon, this approach is considered the best in collecting and analysing qualitative data because it gives flexibility where necessary (Boyce and Neale, 2006; Hancock *et al*., 2001). Similarly, Ritchie *et al*. (2013) refers to in-depth interviews as an effective way of describing and understanding the social context of people. This approach to knowledge inquiry values interaction as a medium to generate robust descriptions of social phenomenon.

> "In-depth interview allows researchers to engage those who have knowledge or experience with the problem of interest and by so doing explore in detail the experiences, motives, and opinions of others and learn to view the world from a perspective other than their own" (Rubin and Rubin, 2011).

Moreover, the use of in-depth interviews was considered suitable for this study as interviews were generally oriented towards the interviewee's knowledge, feelings, recollections, and experiences. They also enabled the interviewer to reveal participants, "meanings and interpretations, rather than impose the researchers' understandings (Charmaz, 2006). At the

beginning of each in-depth interview, the researcher elicited biographical data about the participants before proceeding to the open-ended questions. The structured questions were used to generate biographical information such as age, marital status, and gender.

4.7.4 Negotiating Access and Recruitment of Participants

Gaining access to a study site with the intent of conducting research often starts with engagement and negotiation with gatekeepers. This is a customary prerequisite for research to be conducted. It is a cogent fact that gatekeepers play an important role in any social research (de Laine, 2000). Although, there are possibilities for researchers to encounter challenges in the process of obtaining approval for the gatekeeper, for instance, if the institution or organisation refuses to grant the researcher permission to research their sphere. Therefore, the inability of a researcher to gain access to the research site can stop the process of conducting a research study (Fobosi, 2019). In contrast, obtaining approval from the institutions or individuals that govern or stand in the position of the gatekeepers of a research setting determines the success of the study (Blaxter and Tight, 1997). In this study, obtaining formal approval letters from the local government offices that govern the geographical location of the research site was the starting point for the preparation of the fieldwork of the study (See Appendix B, C Gatekeepers' Letters). Thereafter, the School of Applied Human Sciences at the University of KwaZulu-Natal granted the researcher ethical clearance approval from the higher degree committee (Appendix A: Ethical Clearance Certificate). Afterwards, the researcher proceeded to the fieldwork site of the study. This allowed the opportunity for the researcher to travel to the different cities where the research participants were located, thus, accessing and recruiting participants on arrival in the field was enabled.

4.7.5 Data collection procedure

Without a doubt, the data collection process for a study involves several procedural steps followed to guarantee that the necessary and usable data is obtained from participants.

However, this does not rule out the necessity of gaining an understanding of the nature of the participants in the study. In this study two important procedures were put into consideration which include pre-fieldwork and the conduct of interviews. As part of the study, two research assistance from social sciences from Ekiti State University were recruited as research assistants for the interview, and they were subjected to an intense training session on how to collect qualitative data using in-depth interviews before going on to the field. Over the course of the training, they were also given proper instruction and briefing by the primary researcher on the ethical issues that should be considered while conducting research of this nature. Furthermore, their abilities were also accessed prior to the commencement of the interviews, so they can be fully prepared. Immediately after the pre-field exercise, the researcher with the assistance of two research assistants approached the identified participants. Between December and April 2019, the fieldwork was conducted in three different cities.

The entire interview was divided into segments, with each interviewee having a different appointment date than the others. Each identified participant was given a brief explanation of the purpose of the research and what the study aims to achieve during an individual encounter before the interview began. They were also instructed that they should interpret the interview questions exclusively for research purposes and reply in the same manner. Each participant was given a consent form, on which they could indicate whether they were voluntarily prepared to participate in the research, whether they were willing not to participate, or whether they would decline as the research progressed. The researcher made it clear to the participant of the confidentiality of their conversations. They were properly informed that the study was been conducted for academic purposes and that their identities would be protected. All the interviews were conducted in English, while the participants were allowed to express certain points in the language of their choice. Each interview session lasted about 60mins.

Additional, qualitative data were acquired through in-depth interviews, supplemented by open-ended interviews, to get qualitative results. The participants gave their express permission to record all the information on audio tape. Also, field diaries were used to document numerous important topics that were observed and discussed during the interviews, which helped to round out the process. The latter procedure was regarded necessary and beneficial in terms of confirming the findings of the study enquiry. The primary researcher evaluated and edited the recorded interviews and field diaries at the conclusion of each day of interviews to ensure that they were free of errors in terms of voice frequency, internal consistency, accurate recording, completeness, screening, and other relevant issues. The primary researcher was always present at the study site during the duration of data collection, the study was considered successful.

However, one major disadvantage was the need to constantly remind few of the participants that suggested another date for collection, this is because some of the participants were sceptical to participate due of the widespread crackdown on internet fraudsters in many parts of the country, therefore acquiring access to participants was difficult. This turned out to be a significant difficulty for the researcher because some of the participants felt hesitant to participate in the study, which created a difficult situation for the researcher.

4.7.6 Challenges Encountered During the Course of Data Collection

This research study is not free from any hitch, regardless of its success. Considering the distance between the demographic locations of the study, and the selection of the participants that occurred in different locations in the South-West which required vast travelling for the researcher. Although it would be undisputable to conclude that with the normative perception around cybercrime in Nigeria where the illicit industry has been perceived by many as a redemptive way to success, one would think gaining access to the perpetrators (‘yahoo boys’) would be easy. In contrast, it was difficult gaining access to the perpetrators. Furthermore, gaining access to participants was difficult because of the heavy clamping down on internet

fraudster in various part of the country. This turned out to be a huge challenge for the researcher because some of the participants became sceptical in their participation in the study. Another prominent problem was that a significant number of the participants were concerned about their voice being recorded on tape for security reasons. Equally, it was challenging for the researcher to secure approval of gatekeeper letters from the local government that governs the affairs of the study locations.

4.7.7 Trustworthiness of the Research Findings

Reliability and validity are important factors for achieving excellent research results. In reality, the credibility of a research finding is determined by the extent to which a research instrument is reliable and valid (Simon and Goes, 2016). These factors are rudimentary for any empirical research to be considered authentic and accurate to an appropriate degree. This qualitative research study demonstrates a clear advantage in that enabled participants were able to share their perceptions and lived experiences of the topic under investigation. Moreover, data gathered from the participants were obtained from their natural settings where they articulated their positions in regard to study.

With Trochim and Donnelly (2007), four measures of the reliability and validity of qualitative research instruments were developed to ensure the reliability and validity of qualitative research instruments. These indicators include credibility, transferability, dependability, and conformability. By accurately representing the views of the participants on the qualitative findings of this research, credibility was assured by reporting the participants' languages verbatim. In consonance with the conception of external validity in quantitative research, transferability helps to assess if the findings relate and can be transferred into another context (Lincoln & Guba, 1985; Miles & Huberman, 1994; Amankwaa 2016). Also, Lincoln and Guba (1985) argue that the contrast and triangulation of the research results are the validation of research findings. In that case, transferability was attainted by ensuring that the qualitative

results are transferable to other or similar context through the generalisation of research findings. Thirdly, dependability was attained by following and observing appropriate ethics regarding secrecy and the accuracy of information gathered. This further explains the anonymity of participants and the storing of the interview information under lock and key to avert a possible breach of ethical standards. Lastly, confirmation means that the results reflect the views of the participants as reflected in the data, instead of representing one's assumptions or prejudices. Through presenting the views and opinions of participants only as recorded and written directly from the audiotapes, the validity of this study has been kept intact. Also, it should be noted that this research study was not influenced by the researcher's own perceptions on cybercrime and its related activities in Nigeria.

4.7.8 Ethical Considerations

Ethical consideration is designed to assist researchers and the research community to recognise their ethical responsibilities, important codes of conducts, and attitudes in conducting a research study. Haverkamp (2005) opines that ethical consideration assists researchers to understand conflicting issues and enhances the researcher's ability to make critical ethical decisions when researchers encounter conflict issues. As a starting point for the ethical aspects of this study, the researchers adhered strictly to the ethical guidelines for post-graduate research as outlined in the guidelines of the Ethical Committee of the University of KwaZulu-Natal. Following the research ethical standards, the interview protocol guide was structured in a way that there was no infringement on the privacy of the participants, neither does it unearth responses that were not relevant to achieving the aim of the study. Further, the principle of informed consent was addressed by discussing informed consent with participants. Bryman (2012) suggests that participants should be given ample information to determine whether or not they would like to partake in a study. In light of this, participating members of this study were advised to sign a consent form indicating their readiness to participate in the research

study. This was to establish that participants have a complete understanding of what they were participating in, and also to bring to their awareness that their participation is strictly by choice, and they are entitled to renegotiate consent during the research process or disregard specific questions and discontinue their participation even as the study unfolds. However, before the commencement of the study, participating members of this research were provided with written consent forms that were signed and returned to the researcher (see Appendix D: Participant' Consent forms).

Lastly, it should be acclaimed that the confidentiality of participants remained intact during and after the completion of their fieldwork. Also, all names used in the analysis chapter were pseudonyms and all interviews were conducted in environments preferred by participants. Further, in the course of data presentation and interpretation, the identity of the participant was not reflected. All data generated were kept confidential and used merely for academic purposes. In compliance with the University of KwaZulu-Natal's ethical guidelines, the audiotape interview and the transcribed text were kept under lock and in a place only accessible to the researcher and the supervisor.

4.8 Conclusion

In conclusion, this chapter explains the research methods, approaches, data collection strategies, and research design used in the study. It is important to note that, despite the challenges encountered by the researcher during the fieldwork, this chapter was still able to demonstrate the appropriateness of the research. Similarly, with the fact that this study seeks to answer the research questions through a qualitative approach from an interpretivist perspective that focuses on the in-depth description of cybercrime perpetrators through the use of purposive and snowballing sampling techniques which were utilised to generate and unravel various predisposing factors that influenced youth involvement into cybercrime. Also, this chapter addressed the ethical concerns of the study by ensuring that the standards of

confidentiality, privacy, and informed consent were adhered too throughout the study. To summarise, the chapter reflected on the credibility and trustworthiness of research findings and addressed the justification of methodological approaches.

CHAPTER FIVE

ANALYSIS AND PRESENTATION OF DATA

5.1 Introduction

The objective of this chapter is centred on the presentation, interpretation and analysis of the data collected during the field work. The data collection process was conducted using a qualitative methodical approach which employed a semi-structured, in-depth interview as the research instrument. Also, this section presents the thematic content analysis for data analysis. Further, the section is rationally designed to provide a deeper understanding on the research questions.

The rationale for employing thematic content analysis becomes imperative in the research inquiry. This is to strengthen the trustworthiness of the research by way of enhancing the credibility and dependability of the data. This procedure is necessary to shed rational meaning on the subjective understanding and interpretation of collected data, and also to contribute to existing bodies of knowledge on the subject matter. The second part of the chapter focuses on analysing the findings using the relevant themes that emerged from the data. This chapter examined the theoretical framework that guides the study in succinct terms.

Theories are sets of ideas that serve as a blueprint to explain and understand a social phenomenon. Therefore, the study adopted Robert Merton's strain theory (1938) and the rational choice theory to understand the attitudinal patterns and behavioural manifestations of cybercrime perpetrators ('yahoo boys') in Nigeria. This theoretical approach examined delinquency among youths from a micro level as well as societal point of view. Further, the theoretical approach enhances the credibility and dependability of the data and findings of this research. Finally, the chapter, immerses itself in the study findings to provide a detailed discussion of the phenomenon of cybercrime ('yahoo-yahoo') in Nigeria.

5.2 Presentation, Interpretation, and Analysis of Data

The main objective of the study is to investigate the lived experiences of cybercrime perpetrators ('yahoo-boys') in Nigeria, and to keep abreast with their everyday meaning of the phenomenon. This study postulates upon the socio-economic context and normative considerations of 'yahoo-yahoo' (cybercrime) in Nigeria by addressing the research questions, which were thoroughly examined and answered in regard to the theoretical lens of rational choice theory and Robert Merton's strain theory of crime. The research questions are:

(a) What are the perceived circumstances which led some Nigerian youth to become involved in cybercrime?

(b) What are the key narratives among cybercrime perpetrators and their activities in relation to cybercrime in Nigeria?

(c) What are the links between their lived experiences and the ineffective strategies developed by the government in combatting cybercrime?

The in-depth interviews conduct in this study revealed the socio-economic factors responsible for youth susceptibility to cybercrime in Nigeria. The participants were also given an opportunity to offer critical analyses of the influential factors that lead individuals to participate in cybercrime, as well as the common narrative among 'yahoo boys' (cybercrime perpetrators) since the emergency and growth of the menace. Many discussions were offered by the participants on the socio-economic problems in the country, giving examples from various circumstances as causation for 'yahoo-yahoo' in the social context of Nigeria. They also emphasised various possible measures that could improve the existing measures to be more effective in curbing the menace. Finally, the findings in this chapter were reported based on a thematic analysis of the data obtained from the semi-structured interviews conducted with the participants.

5.3 Thematic Analysis

This section aims to explain the application of thematic analysis to the data collection. This assisted in identifying the emerging theme from the data. This process begins with the translation of the data from audio-tape recordings and field notes to transcribed text. Data reduction begins with the reading and re-reading of the transcribed data. Themes begin to emerge with the initial reading of each transcript. This process was followed by an open coding procedure which was utilised for the identification of all emerging themes that were deemed most relevant to understanding the research phenomenon.

The three main emerging themes are the common narratives among participants about cybercrime, unpacking the narratives in the process of learning and perpetuating cybercrime ('yahoo-yahoo'), and examining participants' perceptions of government initiatives and strategies for combating cybercrime. The emerging of themes, as described in the voices of the participants, gave deep understanding into their experience as cybercriminals. In the analysis of the findings, the discussion drew upon Robert Merton's strain theory that describes crime as a product of disjoints between cultural goals and the means of achieving them and that people are aware of their decision to commit crime. This is relevant to the study because it practically explains the prevalence of cybercrime in Nigeria. The societal goal of achieving wealth and living flamboyantly is commonly achieved in Nigeria via the crooked means, rather than the legitimate means of hard work and educational attainment.

The section that follows presents the socio-demographic background of the participants as well as a full discussion of their experiences as expressed in the words of the participants. It is from these transcriptions that the major findings emerged and were evaluated in accordance with each theme that was identified. The transcribed words of the participants are presented verbatim and, to some extent, in everyday vernacular. Their perceptions are presented in this

style to reflect the authenticity of the data and to enhance the reader's submersion into the reflections and thoughts of the participants.

Table 5.1 Showing the Demographic Information of Participants

Participant Pseudonym	**Gender**	**Age**	**Years Active**	**Educational Background**	**Marital Status**	**City**
Mikky	Male	32	8 years	University graduate	Single	Ado Ekiti
Chinco	Male	28	5 years	Undergraduate	Single	Ado Ekiti
King	Male	31	7 years	University graduate	Single	Ado Ekiti
Sommo	Male	24	4years	Undergraduate	Single	Ado Ekiti
Mario	Male	26	4 years	Undergraduate	Single	Ado Ekiti
Bella	male	27	3 years	Undergraduate	Single	Ado Ekiti
Gabby	Male	27	4 years	Graduate	Single	Ado Ekiti
Yoni	male	25	2 years	Undergraduate	Single	Ado Ekiti
Amigo	Male	34	12 years	Graduate	Married	Ibadan
Steady	Male	23	2 years	Undergraduate	Single	Ado Ekiti
Jago	Male	25	2 years	Undergraduate	Single	Ado Ekiti
Sleek	male	28	3 years	Undergraduate	Single	Ado Ekiti
Johnson	Male	34	10 years	Graduate	Married	Ibadan
Agba	Male	36	10 years	Graduate	Married	Ibadan
T.K	Male	32	9 years	Graduate	Single	Ibadan
Richmond	Male	33	10 years	Graduate	Married	Ibadan
Blackie	Male	35	10 years	Graduate	Single	Lagos Island

Danny	Male	30	11 years	Graduate	Single	Lagos Island
Drama	Male	32	10 years	Graduate	Married	Ibadan
Max	Male	34	10 years	Graduate	Married	Ibadan
Don	Male	38	10 years	Graduate	Married	Ibadan
Kai	Male	30	8 years	Graduate	Single	Lagos Island
Ivy	Male	33	12 years	Graduate	Engaged	Lagos Island
Kadriz	Male	29	6 years	High school Graduate	Engaged	Lagos Island
Milo	Male	34	12 years	Graduate	Married	Lagos Island
Sunny	Male	35	6 years	Graduate	Married	Ibadan
Junkie	Male	29	6 years	Graduate	Single	Ibadan
Grape	Male	33	7 years	Graduate	Engaged	Lagos Island

This table describes the demographic features of the research participants that were identified who agreed to participate in the study. The table demonstrates how interviews were spread across different study locations; this approach allows a deeper understanding the dynamics of 'yahoo-yahoo' from an explicable perspective of the perpetrators. This table shows that age was considered a factor for participants. The requirement was based on the participants' capacity to coherently narrate their experiences and their engagement in the fraudulent activities.

For this study, the age limit was 18 years, which means that only individuals of this age bracket and above were allowed to participant in the study. In total, twenty-nine (29) participants comprising only of males were interviewed using a semi-structured interview as an instrument. Further, it must be noted that the participants of this study were knowledgeable and educated,

most were undergraduates or had achieved some form of tertiary degree. With reference to the marital status of participants, ten of the participants of this study are married and 19 of them are single, which suggest they are undergraduates at the time of this study.

5.4 An Overview of the Common Narratives of Cybercrime Among Participants

Cybercrime is a popular phenomenon and deviant behaviour among the Nigeria youth. The phenomenon can be explained in various ways, ranging from labelling the perpetrators as outright criminals to excusing their action because of the poor state of the country's economy, hence, the increased justification of its rampancy. This section, therefore, explores the factors predisposing youths to cybercrime within the study locations and Nigeria in a broad sense. In the discussion, participants emphasised that unemployment, poverty, and other hidden socio-economic problems are the main economic factors influencing cybercrime. The study found empirical evidence to argue that cybercrime has become a social phenomenon in Nigeria because of the failure of the political system and a lingering effect of years of buffoonery and corruption that characterised previous and present Nigerian democratic administrations. This argument aligns with the beliefs of Ojedokun and Eraye (2012), Tade and Aliyu (2011), and Ninalowo, (2016), which is that cybercrime is an end product of the systemic failure of the social, economic, and political structure. In support of the above argument, Amigo stated the following:

> *"Since I graduated from the university, have been job hunting for years but no employment. When you live in a country like Nigeria where everything goes, and you have to hustle for yourself, yahoo- yahoo became an option and opportunity for many young people to quickly make it in life. Imagine the current state of a country known as the Giant of Africa, a country that is blessed with good mineral resources, but cannot meet the basic needs of the people, especially the youth. It is a shame that future of the youth in this country is not prioritise by the government, politicians are only busy*

enriching their pocket. As a young man who has a dream I have to hustle, and yahoo is our hustle here" (Amigo).

To buttress the above information, another participant justifies their reasons for engaging in cybercrime ('yahoo-yahoo'):

"*For too many years we have believed in our leaders, in government, and politicians for a better Nigeria, that will be easy and convenient for citizen to live. See my brother an average Nigerian is a hustler by default, but when the government have to improve in the aspect of unemployment, imagine the number of unemployed youths, look at the economy of the country, look at the hardship in the country, you will see that there is no hope anywhere. Those of us doing yahoo-yahoo is like placing trust and responsibility ourselves to find a better future, because if you depend on the government nothing good will come" (Max).*

The above submission describes that unemployment in Nigeria is one the major symptoms that upturn youth to become cybercriminals. As we all know, an idle hand is the devil's workshop. Generally speaking, the youth are essential productive assets in the act of nation building, particularly in a developing economy. There is no doubt that the youth are an undeniable resource a country in order to boost its social economic development. In addition to being large in number, the youth are energetic, courageous, and pose new ideas that can make changes to social economic development if they are well coordinated and involved in the economic activities of any country. Regardless, the youth have been faced with many challenges, one of them being the unemployment problem. Youth unemployment is among the largest challenges facing both developed and developing countries in the world. In reality, if the youth are not consequentially empowered, they become a socioeconomic threat to the nation by involving themselves in various criminal activities, for example cybercrime ('yahoo-yahoo'). Which, in

the Nigerian context has the deep-seated consequence of destroying the moral fabric and values of the nation.

From the vantage of the strain theory, this study discovered that unemployment plays a significant role in the criminal activities of cybercrime perpetrators in Nigeria. The youth in Nigeria are encouraged to thrive for success with the goals of reducing poverty. Thus, citizens are encouraged to work hard, but unfortunately many people, especially youths, are denied the opportunity of being financially liberated because there are an inadequate number of jobs and limited prospects to achieve this. As a consequence, people in Nigeria, particularly the youth, are experiencing the strain of unemployment and are exploring illegal channels such as cybercrime. Consequently, the manner in which the unemployed have understood their social environment plays a significant role in shaping their responses towards the crisis of unemployment in Nigeria. The effects of unemployment on crime are primarily mediated and moderated by other variables; however, in the context of this study, anger over unemployment and poverty have conditioned many unemployed undergraduate youths into partaking in illicit activities to reduce financial problems (Tade and Aliyu, 2011; Ojedokun, 2012).

Another undergraduate participant from Ado Ekiti submitted that:

> *"They are saying 'yahoo-yahoo' is bad, we should stop, if we do how are we going to survive there is hardship in the country. People are in dire need of food, there are no jobs anywhere either, graduates are becoming hopeless, I'm surprised they want us to stop, when politicians are recycling wealth. I'm graduating next year there is no hope of getting a job and you want me to stop what is bringing me money, they are joking" (Mario).*
>
> *"The current situation of the country speaks for herself. People are suffering, unemployment rate is increasing, there is not security to protect the lives of the citizen,*

you can literally say nothing is working and the destitutions is in the country is becoming unbearable… So, you have struggle to survive and take care and support your family, but the sad reality is that yahoo-yahoo is a sustainable means for young people…" (Grape).

Examining the above data, one could comprehend that the fight for financial liberation is a driving factor for various crimes, particularly cybercrime ('yahoo-yahoo') in Nigeria. Unemployment, which has been identified as a major cause of poverty, is a worldwide economic problem. However, in understanding the nexus between cybercrime ('yahoo-yahoo') and poverty, it is imperative to explain what poverty is, even though this concept can be related in a multitude of ways; "poverty is a fundamental denial of choices and opportunities, an infringement of human dignity" (Emeile, 2019). This definition suggests that there are no primary opportunities for significant social benefit. In fact, when people are disadvantaged and have limited access to social welfare and other things such as employment or a growing economy, then they are deemed to be poor irrespective of their income (Adesina, 2017). Practically all the participants submit that the rationale behind their involvement in cybercrime has to do with the failed Nigerian society, massive unemployment, poverty, and the quest for economic liberation.

"Be honest my brother, what is really out there that would make you think there is hope for the next generation in this country… for so many years the situation of the country have not changed since I was growing up and now, tell me what has really changed nothing, It is the same old story that Nigeria will be great one day, but how will this be possible when politicians occupying political landscape are corrupt and don't have the interest of the citizen at heart then poverty becomes a problem, see some of us dreams and they can only come to reality through what we doing to survive" (Agba).

A married participant was of the opinion that the hardship and level of poverty in the country is the reason why he still participating in 'yahoo-yahoo'. He stated the following:

> *"I was into cybercrime before I got married, after some years of quitting the game with the hope of getting a legitimate job I couldn't get any job, so I reconsidered joining the game again because of frustration of being jobless. The government is not supporting us from yielding away from this crime, there are lot of graduate like myself with no job, I'm a married man with kids and I want a good life for my kids, I don't want them to experience what I went through as a young man, because really things have not changed, so I'm hoping to make something meaning from the business so I can give my family a better life overseas." (Milo)*

In being probed further on his decision to go back to crime, he said:

> *"Have graduated many years ago. If you don't have any connection in Nigeria, you know that the chance of getting employment is very slim. After many years of job hurting, I went back to doing the game because things have become difficult at that time. Of course fraud is bad but is the only option, I believe it will give me the result that I want, I'm married already, how will I take care of my family and I know friends and people around me are cashing out and doing well, I didn't have a choice than to contact my friends for update on the street, some of them laughed at me, and called me names and said things, like why did you quit before" (Milo).*

Interviewer: "does your wife know you are into 'yahoo-yahoo'?"

Respondent: "*Well, at the beginning I tried to hide it from her, but now she knows. She knows I'm trying to survive on the street, she knows the money is on the street man" (Milo).*

In another in-depth interview, another married participant corroborates with the above:

"Bro, my wife is aware, and she does not have a problem with that, as a man in as much you are able to provide for your family who cares about what you are doing? Money is the most important thing in marriage.... We are in a society whereby you have to survival and make everything work for yourself, nobody is going to help you, she does not complain but rather supports me with prayers" (Agba).

The fight for economic liberation is common among the participants, although they acknowledge the means by which they are fighting are illegal, but they are left with no choice. As a consequence of the social unbalance between government and citizens, the socio-economic requirements of the citizens, especially the youth, has not materialised in the aspects of improving unemployment and poverty rates (Aransiola and Asindemade, 2011). This argument was inclusively endorsed by the works of Adesina (2017), Suleiman (2019), Ojedokun and Eraye (2012), and Tade and Aliyu (2011), who note that a majority of the youth in Nigeria are unemployed and live-in extreme poverty as a result of the systemic failure of the political system and a lingering effect of years of the buffoonery and corruption that has characterised previous and present Nigerian democratic administrations. Thus, this bitterness and anger gives the impression that many youths are motivated to partake in this trend. It is deplorable to know that the youth now think 'yahoo-yahoo', or cybercrime, is a way to make their Nigerian dream come true.

Following the findings of this study, and in sharp comparison with previous research, this study asserts that socio-economic complaints are factors responsible for the emergence of cybercrime in Nigeria. In support of the argument, the derelict attitudes of politicians and stakeholders towards unemployment, poverty, and the underlying socio-economic problems in Nigeria have made the youth vulnerable to the social pressures of 'yahoo-yahoo'. These submissions could be illustrated as a conscious being living in a society where citizens are in languished by poverty that quickly awakens the consciousness of their existence, to realise that the struggle

of the government to bring people out of extreme poverty cannot be accomplished, at least for now, because of corruption and a lack of basic social amenities, like electricity, that could be used to create and sustain commercial businesses in the local context of Nigerian society. Hence, cybercrime perpetrators become innovationists and reject to conform to society's norms of striving for success through accepted means, which have produced nothing but outrageous unemployment and impoverished poverty. In reality, it becomes an individualistic struggle to survive because of the poor situation in Nigeria. To satisfy their reason of intention, their consciousness is not based on them being successful by conforming to societal norms, rather it is based on their distinctive journey to achieving success through unconventional means, which promises greater rewards than legitimate means, as argued by Robert K Merton.

5.5 Unpacking the Narratives in the Process of Learning and Perpetuating Cybercrime

In Nigeria, youth involvement in cybercrime is tremendously increasing to the extent that the general perception of what cybercrime represent has become irrelevant. The disreputable identity of fraud in relation to crime is now accepted as normative behaviour among young people, in the sense that yahoo-yahoo as a phenomenon has maintained a distinctive youth culture that over the years has become difficult to tackle. The premise for this menace is the impact of the economic problems in Nigeria. The aim of the section is to answer the second research question, the response from the participant reveals some common narratives that exist among yahoo boys (cybercrime perpetrators) which has assisted in the growth and sustainability of yahoo-yahoo among young people. It is important to recapitulate the interest of section shifted from the economic incentive pressuring young people in yahoo-yahoo, but instead it focused on all narratives about cybercrime as related by participants.

5.5.1 Conceptualising cybercrime from perpetrators perspective

From the findings of this research, this section seeks to explore and understand what cybercrime ('yahoo-yahoo') means to perpetrators. All the participants in this study admit to

the fact that cybercrime is a criminal offense, punishable under the law. However, the poor economy state of Nigeria has frustrated a majority of the youth into partaking in conventional and non-conventional crimes, such as 'yahoo-yahoo' (cybercrime). As criminalised as the offense is, a majority of the participants sees yahoo-yahoo as a redemptive way to succeed, ignoring all the legal implications. It is interesting to know that 'yahoo-yahoo' represents a paid position of regular employment to some of the participants. Also, 'yahoo-yahoo' is represented as what can be equated to a jostle or shove in the context of some of participants, meaning 'yahoo-yahoo' is socially synonymous to hustling among perpetrators. Having identified what cybercrime represents in the context of the participants, the following supports what 'yahoo-yahoo' (cybercrime) represents in the voices of the participants.

In this interview the conducted with Mikky, he postulated that:

> *"Cybercrime is an internet fraud to make fast money, cybercrime is an industry on its own in Nigeria that is why most Nigerian youth are psychologically conducted to this industry, in the sense that as a youth, or as young man even though you have a legitimate work, you are still aware of yahoo- yahoo, you are aware of some group called yahoo boys, you cannot pretend that you don't know them, especially the rich ones. Because they live the life an average young Nigerian person dream of. That is why you see some people working legitimately and still want to participate in this crime" (Mikky).*

Correspondingly, Danny's understanding of cybercrime (yahoo-yahoo) is as follows:

> *"According to stories have heard, back in the days 'yahoo-yahoo' is a game when it broke out in the early 2000s, it was a trend that many people jumped on without knowing the implications people saw it as an avenue to make money, even though just few numbers of people were participating at that time, But as years evolved with*

modern technologies advancing, yahoo-yahoo in Nigeria an smart way of making money online, although people know is a crime, but that is our hustle" (Danny).

To buttress the above information, the following participant noted:

"Bros, it I true that 'yahoo- yahoo' or cybercrime, whatever you call it, is a crime, but that is our hustle, that is the only means of survival at this point in the life of many young people In Nigeria now. If you ask around, most youth will rather choose to be a yahoo boy than to be an armed robber. Ole le bo mo je" (Richmond).

The findings above, reveal the common understanding of what 'yahoo-yahoo' is from the perspectives of the participants. Although, a large number of the participants agreed that 'yahoo-yahoo' (cybercrime) is a fraudulent act, but cybercrime is different from other malicious crimes such as armed robbery, murder, and other street crimes. In fact, the findings suggest that 'yahoo-yahoo' has taken a large number of young people away from street crimes, since people can make a living from the illicit crime without involving themselves in physical theft thanks to the assistance of internet and other advanced technological devices. Against this background, cybercrime in the context of the participants is a hustle and they are not necessarily committing crime.

5.5.2 Apprenticeships and Mentorship in the 'Yahoo-Yahoo' Learning Process

Apprenticeships and mentorships are an increasing feature among 'yahoo boys' (cybercrime perpetrators) in Nigeria. These elements are connected to the practise of 'yahoo-yahoo' in Nigeria. The phenomenological findings from the study confirm the existence of mentor-like individuals in the learning process of cybercrime ('yahoo-yahoo'). The general role of mentorship relates to teaching and advising (Kram, 1988; Levinson, 1978). According to Sutherland (1947), "knowledge, beliefs, and rationalism are common elements that expedite young people into deviance, this can easily be achieved mainly through interactions with others." This is germane to the study in understanding the common narrative in the learning

process of ‘yahoo-yahoo’ in Nigeria. One commonality that is prominent among young people is the interaction that provides training and guidance, a relationship that can best be described as a dyad. However, the data gathered in this study shows that the recruitment and learning roles of ‘yahoo-yahoo’ appear in a diversity of settings because of the evolving dynamics in the enterprise. Cybercrime in Nigeria has its own rules of engagement, and everyone must go through the process.

A participant stated:

> *“It is beyond having a laptop and internet, you can’t wake one day and say you want to start doing ‘yahoo-yahoo’. There is process to everything in life, usually we learn the game from our cycle. Basically the learning process is not difficult but there must be someone that will guide for instance, when I started gaming years ago it was my brother who thought me the trade, he registered me on dating website with a white guy picture and gave me the bombing format, then I started shooting (contacting) older women on the dating website, so in the evening when he returns, I will sit next to him and watch him replying to the messages, learning how to keep conversation going and building trust and relationship with a client” (Sleek).*
>
> *“…ahh, ‘yahoo-yahoo’ is like a school that has different levels, there are people we call OG’s (people with vast experience) in this game, they have been in the game for years, and what they do is, they bring together young people that are interested in doing yahoo-yahoo especially the ones that look up to them as, mentors, sometimes they even rent apartment for them or they stay with them, this boys will be working for them, looking for client…” (Scoob).*

Interviewer: “Why do they do this?”

Respondent: "*You see it gets to a point in 'yahoo' when you get comfortable and, you don't have the time to sit down and be looking for clients, that is why young fellas are recruited into the game, they still have the hustling spirit in them, so what happens is that when they find a potential client that is rich, they had over the client to the boss or mentor" (Scoob).*

> *"I think the learning process is simple. I have a friend during our undergraduates that was like my boss he taught me things like how to join a dating website, what kind of pictures should be on my profile, what my profile should look like, because the more genuine your profile looks the more likely you are to meet a client. When you eventually find a client, he has the format to convince the client to pay, sometimes the format works, and sometimes it does not work. So, (Pause) overtime I learnt on the job, so I call him my boss, and we still share updates till now, I also have some people who have taught things too and they call me boss, so with all of these, the learning process will continue to be simple because of the information shared among us (Mario)"*

> *"Bro, see ehen, know there are different types of cybercrimes, I will not say the process is easy, it depends on the type of work (typology) of cybercrime people around you are doing, because there are different types, but usually dating is where most common type of work most youth are doing before, they advance to other work. And to advance to other type of work you will [have] to pay for that service because of the resources that some of those work require" (Kai).*

On asking further about why one has to pay to learn about other forms of cybercrime the respondent stated:

> *"Aha, that is simple nah, it to make more money. For instance, almost everybody doing 'yahoo –yahoo' have a knowledge of the dating job, it is usually the starting point because it does not require sophisticated resource. It is relatively most accessible type*

of cybercrime because you have to join a dating site and most of the site are free. So why people pay to advance in this job is because they want to hit big. For instance, one hit of wire work (slang for wire transfer scam) can change your life, but the return from dating is not as much as that. My brother this is our hustle, people will do everything learn new jobs, this is street, and we are talking about hustle here" (Kai).

Supporting the points made by the participant above, the following participant stated:

"If you quickly want to make it big in 'yahoo-yahoo', you must learn other type of work trending are going at a particular time. But it not easy to learn this work, because only few people know them, so that is why they charge you if you want to learn. For instance, if you are doing dating work, and transfer work is going, you will see some people paying to learn because they want to hit big too" (Bella).

On why romance scams are very crucial, the participant noted:

"As you know, romance scam, is like a relationship so to speak, you build the relationship to the point whereby the client will trust you enough to give you her personal information, like bank details and even run errands for you, so dating is very important because you are dealing with someone directly and you can manipulate them into doing whatsoever for you" (Sunny).

Reflecting on the analysis above, one could understand that the learning process and recruitment into 'yahoo-yahoo' in Nigeria is diametric to the advancement of technology and to gain easy access to internet services. From the narrations above, many of the participants describe the learning process, as detailed above, as easy because the knowledge and the skills needed to be successful in the enterprise are mostly shared through interaction within the groups. In this study, participants' observations, as mentioned above, were evaluated. It was established that the recruitment parameters into cybercrime ('yahoo-yahoo') exist through

associates, friends, and other perpetrators with vast knowledge of their illicit activities who recruit young people who show interest in participating in 'yahoo-yahoo'. As such, the chain of recruitment and learning process creates a vertical line of operations and organisation that enables cybercrime perpetrators to advance to a higher level of criminal activities.

Conversely, the differential associate theory that has been adopted comprehensively by scholars in the fields of sociology and criminology conceives that young people learn deviant behaviours through interactions with their peer group. This theory conceives that 'yahoo-yahoo' is a phenomenon that is learned by young people from their routine interactions with other cybercriminals within their social contexts (Adeojo *et al.*, 2019). However, findings from the study suggest that there is a new twist in the learning process in respect to the typologies of cybercrimes. Cybercrime perpetrators in this study are involved in various types of cybercrimes, like spamming and romance scams. The responses above suggest that there is a shift in the learning process of cyber fraud in Nigeria. Apart from the fact that people learn criminal behaviours within their social contexts, criminal activity has been commercialised in the participatory context and there is an organisation of cybercrime in Nigeria. Therefore, the findings from the study establish that there is a trade exchange in which one learns a new skill to perpetrate fraud from 'yahoo boys' (cybercriminals).

5.5.3 Social Networking and Peer Influence

A leading narrative among 'yahoo boys' is the influence of their social networks, and the effects peer pressure has on promulgating youth participation in the e-environment and invariably the use of the internet to commit cybercrime related offenses. Obviously, modern technology aims to solve all human problems, but on the contrary, it has posited enormous threats to the physical and psychological well-being of humans, thereby generating a plethora of unpredictable influences which help to produce the present youth related cybercrime condition in Nigeria. In all facets of human interaction, specific attitudes combine with social factors to produce

behaviour. This is further reinforced by the subjective norms that are often driven by our beliefs regarding what others think we should do. In essence, social pressure to conform often leads us to behave in ways that are at odds or incongruent with our inner convictions. Based on the information received from the participants, it became crystal clear that there is synergy among youth peer influence and the modern economy. Empirical evidence in support of the above submission is captured in the statements of the following participant:

> *"To be honest there are few activities that young adult can engage or participant in to keep them busy apart from going to school in Nigeria. Being an undergraduate student was basically what got us busy as youth 10 years ago, so when the 'yahoo-yahoo' came around in the early 2000s, a lot of undergraduates engaged in it as a new phenomenon, in the name of having fun, until people started making money from it. Then it started spreading among young people and became a culture, people started teaching each other, people started opening cybercafés as businesses because of 'yahoo boys' at that time. So, it was something really big that over years became a culture among youth in Nigeria… So, when I got to the university, 'yahoo-yahoo' was something already popular among students, some students who were yahoo boys would rather choose cybercafés over classes. Being a 'yahoo boy' was something really big on campus, girls wants to associate with 'yahoo boys', you want to be better than that 'yahoo boy', it turns out to be competition among boys, lecturers getting from yahoo boys to pass them, I already have friends involved it and making money from it, so I started going to the cybercafé with them, so basically all these pressurised me and the association of friends at that time was the reason I started doing 'yahoo-yahoo'" (Amigo).*

An in-depth interview conducted with this participant brought about the following extract:

"Well, have been involved in cybercrime or 'yahoo-yahoo' for a while now, roughly 9 years. It all started during my undergraduate days, 'yahoo-yahoo' was a big deal on campus then, as an undergraduate, if you are not a yahoo boy, your friends that are doing it will insult you and call you names. Even if they don't insult you, you feel intimidated by their new lifestyles, so this pressure gets heated up and before you know it, you want to try it out. In my case, peer pressure was the reason I started 'yahoo-yahoo', because there is this street mentality that yahoo boys are hustlers and street smart" (TK).

Another student revealed that:

"My decision to become a 'yahoo-boy' was through the influence of my friends, they influenced me by their lifestyle, the things they have acquired, some of the things I have wished for they got already through 'yahoo-yahoo', like cars, staying in nice apartment and wearing nice and latest clothes and taking responsibilities of paying their school fees and taking care of their family as an undergraduate, was really inspiring for me, I was like, if these guys can be doing this much and fending for themselves with this 'yahoo-yahoo' thing, why can't I try it too" (Steady).

Social pressure and peer pressure refer to the influences exerted by a peer group in encouraging a person to change his or her attitudes, values, or behaviours in order to conform to a group. Social groups affected include membership groups, when the individual is formally a member (for example, political parties or trade unions), or a social clique. A person affected by peer pressure may or may not want to belong to these groups. They may also recognise dissociative groups with which they would not wish to associate, and thus, they behave adversely depending on that group's behaviours. Social pressure can cause people to do things they would not normally do, for example the use of drugs or smoking. Youth peer pressure is one of the most

frequently referred to forms of negative peer pressure. It is particularly common because most youths are forced to spend large amounts of time in fixed groups (in schools and the subgroups within them) regardless of their opinion of those groups. In addition to this, they may lack the maturity to handle the pressure. Also, young people are more willing to behave negatively towards those who are not members of their own peer groups. However, youth peer pressure can also have positive effects. For example, if one is involved with a group of people that are ambitious and working hard to succeed, one might feel pressured to follow suit to avoid feeling excluded from the group. Therefore, the youth would be pressured into improving themselves.

Another participant's thoughts were captured which also and resonate with the above findings.

> *"Honestly, peer pressure among guys is one of the causes of the spread of 'yahoo-yahoo' in this country, the competition is extremely too much particular on social media and offline, most girls like me engage in 'yahoo-yahoo' are also pressed by the fact that if these guys can be making money then it possible for ladies too, since we are the ones helping them with the calling and they give you token" (Sleek).*

In the above excerpts, the participant's submission indicates that social pressure is a factor that predisposes youths to cybercrime in Nigeria. Many factors were noted to be promoting this trend. Apart from the fact that the youths of contemporary times are privileged to have varied technologies at their disposal, they are equally advantaged in that they benefit from their outputs. Notwithstanding, these advantages are not without one hick-up or another. With so many of them utilising the medium for self-development, it is incontestable that so many others have adapted the medium for nefarious activities. As a result of this, the upsurge in cybercrime and other related activities of online fraud among the youth has increased rapidly. Brown (2004) described peer pressure as the hallmark of adolescent experience, relating this to the Nigerian context, the lived experiences of the participants of this study reveals that social

pressures like ‘yahoo-yahoo’ that come with gaudy benefits might be difficult to resist as many youths and unemployed graduates are now attracted to and dependent on this enterprise. The existence of strain caused by economic closure forms the basis for group identity and several resultant activities related to crime.

The hopelessness generated by Nigeria’s socioeconomic climate of mass unemployment, deprivation, hunger, starvation, and poverty affects the studied group’s behavioural choices. Further, the glorification around ‘yahoo-yahoo’ and cybercrime in Nigeria makes it almost impossible for young people to ignore the social pressures. Some of the glorification that has emerged from hip hop songs has been used in a way to promote cybercrime and represents the social structure that created them.

5.5.4 Revenge as a motivation for cybercrime

Cybercrime has grown to become extremely popular across West Africa, not just as an act that defrauds millions of dollars but as a surviving strategy for youth in the face of harsh socioeconomic conditions within the region. Cybercrime in this region, particularly in Nigeria, has grown into a popular culture among Nigerian youth. The insidious social acceptance of the practice is fuelled by notions that these cybercriminals are taking back from citizens of the Western world, who historically championed slavery and colonialism. The act is, therefore, seen as a redemptive and as a wealth redistribution process. The European imperialists push into Africa was motivated by three main factors, these being economic, political, and social (Bulhan, 2015). Colonialism developed in the nineteenth century, following the collapse of the profitability of the slave trade, its abolition and suppression, as well as the expansion of the European capitalist industrial revolution. Thus, the imperialist, capitalist industrialisation, which included a demand for assured sources of raw materials in Africa, spurred the West to scramble to take control of countries which had an abundance of resources and the partition and eventual conquest of Africa followed. With such mentality circulating among young

individuals and new generations becoming conscious and analytical of the historical escapades perpetrated by the Europeans, alongside numerous socioeconomic factors that have pervaded the entire continent for decades, cybercrime in Western Africa could be a remote factor by which they get revenge on Europeans.

The study of Warner (2011) also asserts that cybercriminals in Ghana (Sakwa boys) believe their decision to perpetrate fraud on innocent people in the West is a way of getting back at them. Similarly, Suleiman (2019) opines that some Nigerian youths have a strong belief that colonial masters had brutally enslaved their great grandfathers, hence, their activities towards the west are for economic liberation, an opportunity which their fore- fathers were denied. This perception is promulgated in Africa, and most importantly, Nigeria is blessed with natural resources, but the colonialist came and catered away these resources to develop their respective countries. Now, there are economic problems everywhere in Africa, specifically in Nigeria. So, if the youth devise a means, whether legal or illegal, to scam them, it is a welcome development.

> *"For me it is a yes. People have different view about this though, they stole from our forefathers all our inheritance according to the stories, maybe if they did not our leaders won't be this greedy too. However, that is not my motivation for engaging in cybercrime. For me it was poverty and the hope of liberating my future" (Sunny).*

> *"Historically, yes. from a slavery perspective I would think so. Maybe if the colonialist didn't steal all our resources from us maybe our country and Africa generally maybe it will be a different story by now. Because Nigeria and Africa are places with natural resources that could have used to develop our continent. But the colonialist so the good in Africa and they came to exploit, thank God this is the only way to go make some money off them too" (Blackie).*

"Yes. Because we were brain washed by our colonialist and we are serving them with their own kind of spoon. What they have done to Africa is terms is pathetic, they took everything that we could have used to develop our continent away from us, contemporary we are still being enslave mentally, economically with most of the policy the West has implemented. So, you will see that they are on a mission to make Africa a shithole and through cybercrime some of us are financially liberated to an extent even though our leaders in Nigeria and Africa are corrupt and mentally enslaving us" (Richmond).

In a similar interview, the following participants gave a holistic and different opinion.

"If I have to be honest it all lies, we are all of doing 'yahoo-yahoo' because we want to make ends meets, in reality nobody thinks of what the west has done to Africa. Even the government at hand, the ones we can see here in Nigeria who cannot provide basic amenities for citizens we cannot fight them, cannot start a revolution against them, we cannot demand citizen rights from them, but you hear people say it a fight against the West. Well, I totally disagree… Cybercrime is just an opportunity to make money and fight for your head, the story about trying to get back at the west is nonsense, why are we not using the money gotten from the victims to develop Africa or Nigeria if that is truly the case" (King).

Similarly, another participant also said:

"That is absolute lie, I don't think anyone would want to label a criminal because they want, they want to get the western people. In my opinion, the first intent of 'yahoo boys' is to make money and be financial liberated, the people we are scamming today are not the ones who made Africa what it now. Our leaders, our government is corrupt, is an

unfortunate situation that we have to make money illegal through some innocent people" (Mikky).

Drawing from the narratives discussed above and putting into context their implications on the dynamics of 'yahoo-yahoo' within the study location, it can be inferred that the monologue about colonial exploitation and justified fraud is a common narrative among cybercriminal perpetrators. Cybercrime is understood to get revenge on the western world and the collective narcissistic fantasy continues, as chronicled among some cybercriminals. Although there are different opinions shared among the participants, some argue that the narrative of getting back at the west is a *façade* because there is no moral justification for such nefarious acts; hence, cybercrime has rather become a survival strategy in making ends meet for both employed and unemployed people in Nigeria. Further, this suggests that cybercriminal activities are not a yardstick to measure back to the western world, but many are driven by money, other economic materials, and the social standings that come with the gratification of 'yahoo-yahoo' in Nigeria. In retrospect, given the current socio-economic imbalance in Nigeria that features the detrimental impact of poverty and lack of opportunities for the youth, both employed and unemployed, many have sought solace in criminal activities for the purpose of economic liberation.

5.6 Combating Cybercrime: Understanding Participants' Perceptions of Government Initiatives and Strategies Aimed at Combatting Cybercrime

The ubiquitous growth in cybercriminal activities in Nigeria for decades is a consequence of relative social deprivation variables, and it seems the only way the government is fighting the menace is mainly through the arrest and prosecution of cybercrime offenders. To proffer solutions to cybercrime prevalence, the Federal Government of Nigeria enacted an act to provide for, "the prohibition, prevention, detection, response, investigation, and prosecution of cybercrimes and other related matters" (Oke, 2015). The Cybercrimes (Prohibition, Prevention,

etc.) Act 2015 provides, “an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria” (Eboibi, 2018). To be precise, the cybercrime Act 2015 and other legislations, like the Economic and Financial Crime Commission Act 2004, the Advance Fee Fraud and Other Fraud Related Offences (AFF) Act 2006, and the Evidence Act 2011 are current mechanisms put in place by the government to address or combat cybercrime in Nigeria (Odumesi, 2014; Oke, 2015; Eboibi, 2018).

The threats cybercrime poses are due to technology moving more rapidly than the lawmakers. Cybercriminals are not concerned with the punishments associated with cybercrime; hence, the strict legislation and existing legal frameworks are not sufficient to address the menace of cybercrime directly. The reality is that cybercrime cannot be separated from the punitive economic situation and abject poverty in Nigeria. To curb the activities of cybercrime and cybercriminals, there is need to address the sociological factors that predispose youths to crime and to address these factors in this context means the advocacy for good governance and youth empowerment. The reality in Nigeria is that no one is reliant on the government for anything, the means for survival become an individual struggle and people have the ability to make rational choices that describe their experiences. The fact that there are no basic social amenities or opportunities for youths to apply their skills to in any sort of way makes them more susceptible to all kinds of crime, particularly cybercrime.

Conversely, digital paraphilia, the internet, and the anonymity characteristic of cybercrime have provided numerous opportunities for the youth to both ends meet. Thus, this explains the upsurge in its prevalence. The findings from this study reveal that the current strategies and frameworks put in place by the government to combat and deter youth from cybercrime are not adequate enough because of the massive gap between young people and their reality, the findings further show the lacuna and challenges faced by many institutions, particularly the

Economic and Financial Crime Commission (EFCC) and the Nigeria Police Force (NPF), and how they are functioning within the framework of the laws that oversee cybercrime in Nigeria. So, to address this research question, participants were asked if these strategies and frameworks are effective in curtailing cybercrime ('yahoo-yahoo'), their responses are shown below:

> *"In Nigeria, there are some ways the government are trying to curb or stop cybercrime, but in my opinion, they are not effective because the people in charge are also not innocent of the cybercrime activities in Nigeria. The police department in charge of anti-fraud, which is called (SARS), I will tell you that this unit has been become another scam for years. All they do is to extort from you and want their share of money in your account. Their motive is not really to arrest and prosecute 'yahoo boys', their intention is to arrest you and extort you, they can only take you to the jail if you don't have money to bribe. So, both 'yahoo boys' and SAARS are guilty" (Danny).*

> *"Of course, the laws are there, the EFCC and the police are making arrest[s] which is fine. In truth a lot of 'yahoo boys' are worried about the EFCC because of the threat they carry, even at that, the number of youths they have arrested you will think people should have stopped by now but that is not the case, meaning that both the police and the EFCC alone can curtain or stop 'yahoo-yahoo' in Nigeria. That is just the fact until the government, our leaders, start creating strategies or approaches to change the perspective of the youth and coming generations about this social issue, cybercriminals are being convicted into jail. Our leaders are as well corrupt, launder public funds and not convicted for these crimes which is another fuel to perpetrators activities. As long as the government are not ready to do the needful, people will continue finding a means of survival irrespective of how much they put" (Mikky).*

Another participant said:

> *"Sir, if police arrest you for 'yahoo-yahoo', they are not taking anywhere than the ATM machine or the Bank, they will want you to give them part of the money. In fact, they are terrible that those of us perpetrating the crime. A police office will arrest demanding 400k from you, imagine if they arrest five 'yahoo boys' in a day and they extort that hug amount of money from them…they think the job is that easy, the only time you will get to the police station is when you don't have money to give them. Even when you get to the station and lock you up, they are still demanding money from you, asking you to call your friends to come and bail you out, they don't prepare you to face the law" (Tkay).*

Probing further, the participant said:

> *"Yes, sure I've had a few encounter[s] with the police couple of times and just like I said above, you bribe your way out. It's the usual trend" (Tkay).*
>
> *"The police officers arresting yahoo boys are also on the street hustling, they arrest those haven't paid theirs to them. Can you tell me about the sense in arresting 'yahoo boys' hen police cannot refund what they collect from us to the victim" (Bella)*
>
> *"Which police? Even some of these police officers are 'yahoo boys' too, or they are friends with 'yahoo-boys'. See, in Nigeria some police officers are on the pay roll of 'yahoo boys', that is why they cannot be caught, even if they are being caught, they know how to bribe their bosses, expect you don't have money. There are levels in the games, for example if SARS is coming to arrest you in the house, you might have gotten the info from one of their officers that is your friend, that is the person that give you first-hand information all the time" (Amigo).*

The data above evaluates the current strategies and frameworks in use by the government to curb the widespread of cybercrime in Nigeria. Without a doubt, the strategy and approach to curb cybercrime has been effective to a degree because of the massive apprehension and prosecution of cybercriminals across the country. In fairness, the EFCC and SARS has made a significant number of arrests of cybercriminals, but this effort is not enough as many of the perpetrators can still manoeuvre their way out because of corruption. The participants acknowledged the existence of cybercrime laws as a deterrence for cyber citizens from engaging in cybercrime. However, the existing legal framework is not enough in the fight against cybercrime, the government cannot depend on it alone if they truly want to combat the cybercrime menace that has deepened into the social fabric of the society. The emergence of cybercrime in Nigeria is interconnected with corruption and poor living conditions of the average youth and the struggle for survival (Suleiman, 2019; Tade, 2013; Adesina, 2008). According to Eboibi and Suleiman (2018; 2019), cybercrime is a phenomenon in Nigeria that has gained global recognition. It is no wonder that Nigeria was identified as the country with the third highest rate of cybercrime in the world (Tade and Aliyu, 2013; Suleiman, 2015). Therefore, there should be urgent calls for *exposé*s and a more erudite approach to prevent the cybercrime menace and crime in general rather than combatting the menace in the future.

The findings corroborate literature that claims that the existing measures and punishments for cyber offences are not sufficient in themselves as they are without the proper measures of enactment and implementation; this represents the chronicles of Nigerian society in regulating cyber offences (Adomi, 2008, Umejiaku and Anyaegbu, 2016). Equally, other studies have argued that, in Nigerian society, political impunity, bribery, and corruption have created a social environment in which fraudulent practices are normative for ordinary Nigerians. As such, the situation encourages cybercriminals to perpetrate their illicit acts with the mind set of bribing their way out if apprehended (Nhan *et al*., 2009; Smith 2007; Tade and Aliyu, 2011).

The deficiencies in the implementation of regulating acts continue to serve as the bane to the progress recorded in the fight against cybercrime in Nigeria.

> *"The police officers that is supposed to arrest yahoo boy is also looking for how to make money. This is why they stop you and find evidence on your phone for example, they demand that you pay a huge amount of money to bribe" (Grape).*
>
> *"Have had encounter with police and they ask me for money. If they continue to take bribe from us, are we going to be scared of them or the laws when you know that you can easily bribe your way out. You already know that if you are arrested the outcome is that go and bring money" (Sleeky).*
>
> *"See every one of us is corrupt, the police are even the worse, they are always out there waiting to collect their share of the money, some of them are even on the pay roll of yahoo boys, so tell me how this will stop, when the government is not addressing the main issues facing this country. The salaries of the police officers are not good enough, why won't they be on the street looking for yahoo boys, when what they make on the street is more than their salary. To stop yahoo-yahoo in Nigeria, the government must grab the bull in the horn and fix the social problems Nigerians are facing, they are the only way, the poverty is in the land is too much, only the politicians are the ones enjoying in this country" (Grape)*

The above excerpt shows that there are external factors that promulgate the prevalence of cybercrime apart from the underlying socioeconomic problems in the country. The police force, as a unit, is customarily responsible for being the guardians of social order. As an institution, Nigeria Police Force (NPF) helps to protect, strengthen, and reproduce the prevailing social order in contemporary society. Without the Nigerian Police Force it would be difficult to maintain law and order. Although various factors have threatened police effectiveness in

combatting cybercrimes, such as unemployment, population growth, and corruption, advancement in technology and new economic opportunities are also leading to a wide range of criminal problems, including cybercrime, corruption, terrorism, and criminality in politics. These are some of the challenges that has engulfed the force (Kasali and Otedola, 2016). The findings of the study reveal that corruption and the taking of bribes from cybercrime perpetrators have impaired the war against cybercrime, as some officers are allegedly found to have been demanding money from cybercrime offenders instead of arresting them and indicting them. This shows a lack of enthusiasm and determination in some of the officers of the force. Considering the rise of cybercrime and its newfound prevalence, questions need to be asked as to whether the institution is capable of tackling the bizarre upsurge of this crime. From the above findings one could infer that more steps are needed to effectively combat 'yahoo-yahoo', as systemic corruption and flagrant abuses of power among policemen is one of the major hurdles preventing the effectiveness of curbing cybercrime, because police officers regularly extort money from cybercrime perpetrators. According to Alderson (1979), police corruption exists on two levels, the individual and departmental levels. Individual corruption generally includes individual men in the force who use their roles as personal aggrandisement law enforcement agents to commit their crimes. Institutional corruption may take place within committees or departments in which junior officials perpetrate corrupt practices for the sake of financial gain. This institutional corruption has contributed to the ineffectiveness in combating 'yahoo-yahoo' (cybercrime).

A participant noted this:

> *"Bros, there are senior officers in the police, EFCC that knows biggest boys in these games, but they are not arresting rather they give me information. This is to tell you that the more you have money and connection at the top there, the more you are free as*

yahoo boy. It is very simple, make money and know the top officers, nobody will disturb you" (Junkie).

Further, the notion that arresting cybercriminals would make a dent in the industry and minimise the number of victims does not seem realistic to cybercrime perpetrators, even though Nigerian cybercrime law Section 419 clearly states that internet scamming is a felony (Otedola, 2016). This implies that participants from this study might be arrested and face the consequence if been caught. The wars against cybercrime and 'yahoo boys' in Nigeria is a very challenging one. This is perhaps because the subject matter itself is an intricate phenomenon. From this background, criminal behaviour is indicative of social structural strain derived from social factors that influence the rational decisions of individuals causing them to partake in unconventional behaviour in the society. However, if the government are serious about combatting cybercrime and other street crimes, then there must be a change in the current approach of arresting cybercrime perpetrators and the miscellaneous prosecution of cybercriminals, because that alone cannot deter the intention of a person to commit all kinds of crimes. There is a bigger picture that can address the unconventional means the youth have employed, because currently cybercriminals do not believe there is anything wrong with criminal activities. Their actions are rationalised by combining the existing state of society in accordance with their own conditions, which naturally negates agreed norms. Some studies argue that, in Nigerian society, political impunity, bribery, and corruption have created a social environment in which fraudulent practices are normative for ordinary Nigerians (Pierce, 2016; Smith, 2008).

"*Obviously, cybercrime is a criminal offense under the laws in Nigeria. So, I think the government is heading into the right path with the massive arrest and prosecution of cybercrime perpetrators in Nigeria, because EFCC carries serious threat. With social media platforms, you can conclude by saying EFCC is doing a great job with this arrest,*

because people are scared now and I will say it is time to rethink especially 'yahoo boys', the truth is no body want his name it be tarnished. With this new collaboration between EFCC and the police I think it is productive because I know some of my colleague doing this have quitted because of the threat from the government. These days when you are arrested and found guilty, everything you have will be seized and I think the penalty is seven years in prison. Is a good development, because an average Nigerian is being identified as a criminal overseas, because Nigerians still go overseas and continue with this. So, the government are trying everything in their capacity to curb cybercrime in Nigeria and hopefully they are successful" (Gabby).

"Lately, there have new approaches in curbing cybercrime in Nigeria with EFCC working hand in hand with the police makes it scarier and put everyone on their toes, this will reduce the participation of youth involvement in cybercrime. I think the mechanism are working but people do not seem to care, with this number of arrests by EFCC I think 'yahoo-yahoo' should have stopped., but the fact is if we stop what are we going to doing? The prayer is makes dem no catch us." (Chinco).

"Of course, the EFCC are working hard and all of that which is fine, in fact a lot of 'yahoo boys' are scared of EFCC, not because they are better of the police, but we believe that when they catch you the money, they will demand from you will be too outrageous. Well, this is my opinion, because the corruption in Nigeria is too much. Even at that, with the number of youths they have arrested you will think people should have stopped by now but that is not the case, meaning that both the police and the EFCC alone can curtain or stop 'yahoo- yahoo' in Nigeria that is just the fact until the government, our leaders, start creating strategies/approaches to change the perspective of the youth and coming generations about this social issue, cybercriminals are being convicted into jail. Our leaders are as well corrupt, launder public funds and

not convicted for these crimes which is another fuel to perpetrators activities. As long as the government are not ready to do the needful, people will continue finding a means of survival irrespective of how much arrest they make" (Mikky).

Owing to the global nature of the internet and municipal regulations, strategies to combat cybercrimes are also exceedingly difficult to put into effect. Many countries, including Nigeria, have institutions such like the EFCC and the ICPC to tackle all forms of financial crimes. The data above indicates that cybercriminals in Nigeria are wary of the activities of these institutions, particularly the Economic and Financial Crime Commission in apprehending cybercrime perpetrators. In contemplation of the menace of cybercrime, cybercrime laws were enacted. The law is very comprehensive and provides severe punishment for impersonation and identity theft, the law recommends seven years in jail or a five million Naira fine, or both, as the penalty for anyone who is convicted of impersonation with intent to defraud any person. The laws permit the Economic and Financial Crimes Commission (EFCC), the police, and other law enforcement agencies to the mandate to arrest and charge cybercrime perpetrators (Eboibi 2017; Oke, 2015). In Nigeria, the EFCC have been at the forefront of the apprehension and prosecution of cybercrime perpetrators ('yahoo boys'), although, the EFCC does not act alone, because cybercrime involves vast criminal networks. The Institution, therefore, collaborates with other law enforcement agencies such as the NPF, the ICPC, and foreign organisations, like the Federal Bureau of Investigation (FBI), to address issues of cybercrimes from a wider angle. This came into effect under the agreement of MLATs. According to Deloitte (2008), MLATs are agreements between two or more countries to gather and share information pertaining to criminal activities and the permitted use of such information to enforce laws. In relation to this, the FBI, along with the operation of EFCC, focuses on dismantling the most significant cybercrime perpetrator enterprises. By doing so, there was a repress on cybercrime in Nigeria in that 281 fraudsters were arrested, mostly in Nigeria and the

United States, in May 2019 (Tech Explore, 2019). Another report suggested that an ample number of the Nigerian suspects were arrested in coordination with the US law enforcement agency (FBI), including 167 of them being detained since August for alleged computer-related fraud (Tech explore, 2019). In curbing cybercrime, so many polices, and suggestions have been brought forward by scholars. For instance, Bola-Balogun (2019) submits that government should create cyber awareness programs or encourage the sensitisation of the populace as this will go a long way in educating the masses on how to prevent common forms of cybercrimes like email fraud and malware attacks as well as limit the access of sexually explicit content of children and young people. In the same vein, more universities should introduce cyber security as a full-fledged course under the school of computing. This will accord a benefit for young Nigerians to pursue a career in the field of cyber security and work in tandem with other professionals to tackle cybercrime. The government should implement cyber security best practices, especially in the financial sector, to prevent cybercrime and prosecute perpetrators. Umana (2015) affirms that security software should be installed on personal devices. Finally, the government needs to create an enabling environment that would encourage the unleashing of people's potentials. Putting one's creativity to work should earn them benefits that would make life enjoyable. When people cannot profit from using their creativity in good ventures, they will invest their potentials in negative ventures that would yield to them larger benefit. It is a common idea that money and material things are a very necessary motivation, whether you are doing something good or bad.

To conclude, internet scams have persisted despite legal instruments primarily because of different factors. The overview of this argument is that Nigeria does not have sustainable anti-corruption policies or strategies to entirely deal with cybercrime. It is a complex social problem that has rooted deep into the moral fabric of young people in Nigeria, thus, it requires a multifaceted approach, starting with government taking responsibility by providing a thriving

environment for the present youth and the next generation. There is a socially relative deprivation issue that has led to intense poverty. The participants' views on the role of government agencies in curbing cybercrime in Nigeria revealed that cybercrime is a social menace that is currently spreading despite the existing laws against cybercrime. The data reveals that the ability of law enforcement agencies to live up to expectations in terms of carrying out their constitutional responsibilities is largely due to the alarming incidence and prevalence of 'yahoo-yahoo', because cybercriminals are confident that the corruption in the country is a wave, they can use to manipulate law enforcement agents if at all they are arrested. The inadequate performance of the law enforcement agencies in Nigeria to reduce the social problem of cybercrime is connected to many systemic impediments, varying from material to personal and exterior problems, including corruption and low public opinion.

5.7 Conclusion

This chapter discusses participants' perceptions and the common narratives of cybercrime. It started by presenting the demographic descriptions of the study participants, followed by an overview of the common narratives of cybercrime among participants. Following is a detailed discussion of the factors sacrosanct in the process of learning and perpetuating cybercrime ('yahoo-yahoo'). Some of the important narratives identified include that cybercrime means different things to participants. While some of them are aware of its criminality and the havoc it could wreck on the victim, most participants describe how poverty and unemployment has influenced their choices. Another important factor that was common to participants is that cybercrime is not morally questionable, because to them it is an avenue for repatriating wealth from supposedly wealthy nations that have, at some time in history, looted and exploited the natural resources, cultural and economic wealth, as well as the human manpower of countries like Nigeria. It was discovered that 'yahoo-yahoo' has continued to grow in Nigeria because it has established itself as a functional illicit institution in Nigeria that thrives on networking and

connections. Finally, this chapter was a discussion of participants' perceptions on government initiatives and strategies for combating cybercrime.

CHAPTER SIX
DATA INTERPRETATION AND DISCUSSION OF THE FINDINGS

6.1 Introduction

This section focuses mainly on the themes that emerged from the research findings. Evidence from both the discussed literature and this study suggests that more attention needs to be paid to variables linking youth and cybercrime ('yahoo-yahoo'). The findings from literature on cybercrime in Nigeria and this study suggest that the way the youth understand and interpret the situation in their environment and how they have been influenced by these factors is crucial to understanding cybercrime in Nigeria. The findings from this study argue that the youth are challenged by and discontent with numerous social constraints with respect to gaining a better livelihood in Nigeria. In essence, this section makes analysis, drawing on both strain and rational choice viewpoints, to explain the role unemployment and other predisposing factors play in the criminal behaviours of some youth that engage in 'yahoo-yahoo' (cybercrime).

An element that is interesting is the way in which the youth interpret their experiences, and how these interpretations and experiences influence their criminal actions. The findings show that the effects of socio-economic problems on crime are mainly modified and moderated by other external variables. In particular, the long-lasting issue of unemployment depends on external attributions which anger youth and push them towards lives of crimes, in particular 'yahoo-yahoo'. In addition, the lack of support from the government, a decrease in social control, and prolonged absence of youth empowerment have increased the participation of the youth directly involved in cybercrimes. This participation is also encouraged by peers and their disregard for penalties incurred for their crimes.

6.2 Classification and Discussion of Emerging Themes

The finding and analysis of the participants' accounts uncovers the subjective experiences of many participants. Significant factors are responsible for the youth participants' criminal

activities. Furthermore, the dynamics around cybercrime industry in Nigeria were unravelled in four major themes, these being the systemic failure of the social, economic, and political structure; networking and collaboration as a transnational operating system built on reliance and collaboration; the 'yahoo-yahoo' enterprise and its link to spiritualism; and romance scams.

6.2.1 Systemic Failure of the social, economic, and Political structures

Poor economic conditions and their significant impact on the social lives of the participants is one of the reoccurring themes that emerged from this study. It was revealed from the participants' explanations that the incessant participation and involvement of the youth in fraud and other computer crimes is a result of poverty in the country. One would expect that 'the giant of Africa', as Nigeria is colloquially called, should not be trapped in poverty and destitution. This, unfortunately, is the nation's reality, because of the absolute mismanagement and downright corruption of politicians that has plagues the country with socioeconomic problems such as unemployment, poor educational structures and system, and a lack of basic social amenities, simultaneously creating a derelict society. Poverty has become one of the most significant socioeconomic issues challenging Nigeria today. This is evident in terms of its reach, as shown in the reliable statistics obtained from the Federal Bureau of Statistics on the number of unemployed youths in Nigeria. Conversely, the figures derived from the Federal Statistics Bureau reveals that unemployment in Nigeria has jumped from 29.7 to 34.49, indicating that many youths are unemployed. Also, a recent report revealed that Nigeria became the poverty capital of the world, with 8.9 million citizens in poverty, overtaking India who reportedly has a population seven times larger than Nigeria (Slater, 2018). As recorded in literature, the unemployment rate in Nigeria as of 2011 stood at 23.9 per cent. Thus, the precarious growth of 'yahoo-yahoo' was mentioned to be a result of people's fear of unemployment at that point in time (Adeniran, 2008; Adomi and Igun, 2008; Tade and Aliyu, 2011). Recently, statistics supported the aforementioned and predict that the unemployment

rate will jump to 33.6 per cent by 2020 (Times, P, 2019). These statistics proves there is failure in the social and political structure of Nigeria, and this has been acknowledged as a massive susceptibility factor to criminal behaviours, particularly the enterprise 'yahoo-yahoo' which is common among the youth. The findings from this study identify that unemployment and poverty are the main factors that influence the promulgation of cybercrime in Nigeria. As such, unemployed youth and employed youth are now involved in cybercrime as a means of survival. The following responses were gathered from the participants:

> *"I couldn't get a job since I graduated, what can I do? And 'yahoo-yahoo' is what is common among youth is like how people in Jamaica are known for marijuana, Nigerians are known for 'yahoo-yahoo', even though we are the Giant of Africa, we are oil-producing country, our leaders don't see a need to improve and empower youth in this country. This is not something new it has been happening since democracy, youth in Nigeria are never prioritise, what do you expect when there are no jobs, no plans from government to help us, we have corrupt leaders, we have to save ourselves and our future, that is why I'm into the game" (Amigo).*

Another participant justifies the reasons for pursuing 'yahoo-yahoo' as a means of survival below:

> *"For too many years we have believed and trusted the government, politicians, for a better future by creating jobs, companies where we can work with our certificates. Instead, they are making their pockets richer and sending their children overseas, look out the numbers of unemployed graduates, look at the economy, you will see that there is no future is this country expect we want to deceive ourselves… Those of us doing 'yahoo-yahoo' is like placing trust in ourselves and finding a better future. If you depend on the government nothing good will happen" (Max).*

In accompaniment to the above, an undergraduate noted:

> "…. *The system has failed us, almost every youth are thinking towards 'yahoo-yahoo' direction" (Ivy).*

This following participant shared a similar view:

> *"The country is bad; nothing is going well that is why you see so many youths doing 'yahoo-yahoo'. To show you how bad it is, ladies are now joining the boys in doing this fraud of a thing…" (Sommo).*

This data reveals that unemployment is an enormous social problem affecting the lives of many Nigerians, and this challenge is economically and psychologically crippling for both individuals and the society at large. Unemployment is an economic, political, and social conception that is difficult to describe and measure because it depends on the economy and social settings of a country as well as its educational system (Msigwa and Kipesha, 2013). Typically, youth are essential productive assets in nation-building, particularly in a developing economy. For instance, youth are considered as a "vital sources of manpower for development" in Nigeria (Olujide, 2008). Generally, youth are seen as the leaders of tomorrow, hence, they are the prominent tools in the development of any country. Therefore, the kind of exposure and education they acquire becomes imperative and determines the overall development of the country. However, the situation is not the same in Nigeria, as many youths are disadvantage because of employment and poverty. This gap in the social structure of the country has birthed various crimes, ranging from traditional crime to cybercrime. The involvement of young people in traditional crimes and cybercrimes describes the extent of the social and moral cadence of Nigerian society in general. This depravity exhibits itself in various social defect which are characterised by corruption. Conversely, it is evident today that if the youth are not consequentially empowered, they become a socioeconomic threat to the nation by involving

themselves in various crimes, such as cybercrime (yahoo-yahoo), which has turned out be a deep-rooted problem destroying the moral values of the country.

From the perspective of strain theory, which argues that social structures may pressure citizens into committing crime and social barriers can restrict people under certain socioeconomic conditions from having access to the legitimate means to achieve culturally valid goals. This generates pressure, forcing individuals into the adoption of illegitimate means to pursue culturally accepted goals (Featherstone and Deflem, 2003). Strain theory is based on the idea that delinquency results when individuals are unable to achieve their goals through legitimate channels. In such cases, individuals may turn to illegitimate channels of goal achievement to lash out at the source of their frustration in anger. The findings from this study reveals that the frustration of young people is a result unemployment. The unemployment and poverty rates in Nigeria play a significant role in the criminal activities of cybercrime perpetrators. The priority of an average youth is to be financially independent, thus, citizens are encouraged to work hard. Unfortunately, many people, especially youths, are denied the opportunity to be financially liberated because there are an inadequate number of jobs and limited prospects through which to achieve this. As a consequence, of this strain, young people now explore illegal channels to achieve socially encouraged goals.

Consequently, how the youth have understood their social environment, particularly those that are unemployed, plays a significant role in shaping their responses towards the crisis of unemployment in Nigeria. The effect of unemployment on crimes is generally primarily mediated and moderated by other variables; however, in the context of this study, anger over unemployment and poverty has forced many unemployed and undergraduate youths into partaking in illicit activities to reduce their financial problems (Tade and Aliyu, 2011; Ojedokun, 2012).

An undergraduate participant from Ado Ekiti submitted that:

> *"They are saying 'yahoo-yahoo' is bad. We should stop, if we do how are we going to survive, there is hardship in the country, people are in dire need of food, there are no jobs anywhere either. Graduates are becoming hopeless. I'm surprised they want us to stop when politicians are corrupt and stealing from our wealth. I'm graduating next year there is no hope of getting a job and you want me to stop what is bringing me money, they are joking" (Mario).*

Examining the above data, one could comprehend that poverty is a driving factor for various crimes, particularly cybercrime ('yahoo-yahoo') in Nigeria. In understanding the nexus between cybercrime ('yahoo-yahoo') and poverty, it is imperative to explain what poverty is, even though this concept has a multitude of definitions. According to Adesina (2017), poverty is the fundamental denial of choices and opportunities and an infringement of human dignity. This suggests that there is no primary opportunity for significant social benefits. In fact, when people are disadvantaged and prevented from accessing social welfare, like good health care and employment, then they are deemed to be poor, irrespective of their income. Practically all of the participants submit that the rationale behind their involvement in cybercrime has to do with the failure of Nigerian society, massive poverty in the land, the absence of jobs, and the quest for economic liberation.

> *"The current situation of the country speaks for herself. People are suffering, the unemployment rate is increasing, there is no security to protect the lives of the citizen, you can say nothing is working and the destitutions is in the country is becoming unbearable… So, you have struggle to survive and take care and support your family, but the sad reality is that 'yahoo-yahoo' is a sustainable means for young people" (Grape).*

"Be honest my brother, what is really out there that would make you think there is hope for the next generation in this country… For so many years the situation of the country have not changed since I was growing up and now, tell me what has really changed nothing, the politicians are enriching their pockets, sending their kids overseas to a better future, while the masses are languishing in poverty…. some of us have been to fulfil some dreams thanks to what we are doing we just have to survive" (Agba).

The fight for economic liberation is a common narrative among the participants, although they acknowledge that how they are fighting for this is of course illegal, but they are left with no choice. As a consequence of the social imbalance between the government and citizens, the socioeconomic requirements of the citizens, especially the youth, have not materialised in the aspect of improving the unemployment and poverty rates in the country (Aransiola and Asindemade, 2011). This argument was inclusively endorsed by the work of Adesina (2017), Suleiman (2019), Ojedokun and Eraye (2012), and Tade and Aliyu (2011), who note that a majority of the youth in Nigeria are unemployed and live-in extreme poverty as a result of the systemic failure of the political system and the lingering effect of the years of buffoonery and corruption that have characterised previous and present Nigerian democratic administrations. Thus, the pain, bitterness, and anger expressed gives the impression that many youths are motivated into the trend of 'yahoo-yahoo'. It is deplorable to know that the youth now think that cybercrime (yahoo-yahoo) is a way to make their Nigerian dream come true. The data gathered in this study reveals that the current poor economic situation in the country has influenced the decision of some ex-cybercrime perpetrators to enter back into the illicit industry. To confirm this, a participant noted:

"In my undergraduate days, I was engaged in 'yahoo-yahoo' for two years, then I stopped because I felt it was bad. After years of job hunting, I'm back in the hustle for

survival even though it was not easy but there is hope and that something good will come out of it" (Agba).

Married participants from Ibadan who related state:

"I was doing 'yahoo' before, but I stopped. After three years of quitting the game with the hope of getting a legitimate job, I couldn't get any job, so I reconsidered joining the game again because of the frustration of being jobless. The government is not supporting us from yielding away from this crime, there is lot of graduates like myself with no job. I'm a married man with kids and I have other responsibilities to take care of" (Milo).

On being probed further, the participant said:

"*Have graduated many years ago, I was hurting for a job for so many years of course fraud is bad but is the only option, so I went back to the game. I believe it will give me the result that I want. I'm married already, how will I take care of my family and I know friends and people around me are cashing out and doing well. I didn't have a choice than to contact my friends for an update on the street, some of them laughed at me, and called me names and said things, like why did you quit before" (Milo).*

Interviewer: "Does your wife know you are into fraud?"

Respondent: "*Of course she knows. I tell her everything. She knows I'm trying to survive on the street, she knows the money is on the street man" (Milo).*

In another in-depth interview, another married participant corroborates with the above:

"Bro, my wife is aware, and she does not have a problem with that. As a man in as much you can provide for your family who cares about what you are doing? Money is the most important thing in marriage.... We are in a society whereby you have to survive

and make everything work for yourself; nobody is going to help you. She does not complain but rather supports me with prayers" (Agba).

All the above submissions by the participants reiterate that the derelict attitudes of politicians and stakeholders toward unemployment, poverty, and the underlying socioeconomic problems in Nigeria have made youths morally bankrupt to the extent that cybercrime does not represent crime and is rather a computer business. Their submissions could be illustrated as a conscious being living in a society where citizens are in languished poverty which quickly awakens the consciousness of their existence to realise that the struggle of the government to bring people out of extreme poverty cannot be accomplished for now because of corruption and a lack of basic social amenities that could be used to create and sustain commercial businesses in the local context of Nigeria society. Hence, cybercrime perpetrators become innovationists and reject to conform with the social norms of striving for success through the accepted means which have produced nothing but outrageous unemployment and impoverished poverty. In reality, it becomes an individualistic struggle to survive because of the poor situation in Nigeria. To satisfy their reasons of intention, their consciousness is not based on them being successful by conforming to societal norms, rather it is based on their distinctive journey of achieving success through unconventional means which promise greater rewards than legitimate means.

6.2.2 Networking and Collaboration: A Transnational Operating System Built on Reliance and Collaboration

Another emerging theme is how participants described the organisational structures and transnational operating systems of cybercriminals and how the structure improves their ability to defraud people. There is no doubt, the complete dependence on the internet in our contemporary society has increased the risks modelled by cybercriminals over the last few years. A global statistic report of internet users indicates that there are about 4.5 billion active

internet users in the world over (Global digital population, 2020). The launch of the internet and the mass production of sophisticated technological devices has transformed human interaction, it has also naturally moved criminality into the cyberspace. The organisation of the networks of cybercriminals are a strong indicator that cybercriminals can break through almost every cyber security defense protocol and execute their actions on potential victims. In fact, the operations and dynamics around cybercrime have transcended beyond physical boundaries and immediate virtual limits. Contemporarily, cybercrime activities have become a collective phenomenon among perpetrators. The operational pattern of organised cybercrime is a threat to the global economy and the mode of operation remains indescribable, networked, and highly complex (United Nations, 2013; Hutching, 2014) Therefore, organised cybercrime consists of a network of criminals constituted by functional skills that enable them to collaborate in perpetrating various internet crimes (Hutchings, 2014).

In this context, much of the literature claims that organised crime can be described as the natural revolution of crime through the evolution of cybercrime by dominant groups (Kshetri, 2010; Von Lampe, 2015). The bureaucratic practice of organised cybercrime among cybercriminals, as revealed by the findings, demonstrates how the complexity of their modus operandi enables cybercriminals to perpetrate fraud in many respects. The cybercrime perpetrators interviewed in this study discussed the collaborative networks and operations of 'yahoo-yahoo boys' and how these networks have contributed to the success of 'yahoo-yahoo' in Nigeria. The following responses were attained from the participants:

> *"What people don't know about 'yahoo-yahoo' is that the game has grown within different groups and generations. In the sense that in the early 90s, when this thing called 'yahoo-yahoo' started, there are some groups of people doing it at that time right? Over the years some of them will continue doing it and some of them will stop doing it for various circumstance. So, what I'm saying is that, over the years the*

activities of 'yahoo boys' have developed into different phases… Now we hear from credit card fraud, romance scam fraud, hackering, carting. In those early 90s to early 2000, the common thing among 'yahoo boys' then was carting, they cart good from shopping sites using people's credit card. So, imagine those guys at the time started or introduced 'yahoo-yahoo' in Nigeria at that time, that has still done fraud till now, imagine the kind of networked and experience they will have now. So, coming to the middle generation of 'yahoo boys. I mean my generation that was when 'yahoo-yahoo' and 'yahoo boys' became popular, this will be around 2005, people in this age bracket will be guys in their late 30s. At that time, doing fraud became a new reality to us... We were doing it for fun, we were making money as well, and the same time it was growing into various types, new things, new ideas, information start developing among 'yahoo boys', mind your things were not as desperate as now …. Even though it was growing into something more popular among youth then, the ultimate reason was just to survive, it was not a do or die something. At this time cybercrime offence has not been enacted into the Nigeria constitution… So, coming the last generation, which I think practically started in the 2016, where it now appears that it has been socially accepted in Nigeria. High school student, even babies, know what 'yahoo-yahoo' in Nigeria is today. So, it is not industry that has evolved in different generations, where experience differs, level of desperation differs" (Ivy).

In a similar in-depth interview, the following respondents' opinions corroborate the above:

"You know there are various types of cybercrime, and they are interconnected together through 'yahoo boys'... For instance, if am a guy whose is doing dating and there is a guy doing another job let say spamming or check and his client wants to pay, that person will look for someone who has an account where the client can send the money to, in that way we collaborate together, because is very difficult to send money straight

to Nigeria. Nigeria is a red flag once the clients hear Nigeria, they don't want to be pay anymore, but if the account is still on America or European is fine" (Tkay).

"Most of the collaborative and networking in this game is all about money and how to make the money, so it very important you have a good network among friends, because it will help me with the latest update in the job" (Junkie).

"The network of 'yahoo boys' is established both internationally and in Nigeria among friends or colleagues also doing 'yahoo-yahoo' to this to effectively scam people. It is through networks and collaborating, that you will meet people, for example hackers, or some guys that are IT guru, which their job is to provide tools and software" (Grape).

Also, some of the participants reiterated the roles of hackers in cyber fraud and how the collaboration has been effective. The following responses were captured:

"If you don't have a sure hacker that can give you updated tools you will face some challenges… That link is very important for the type of my job which is spamming, in spamming you need companies' emails address or account officers' emails, to gain access to this personal information you need a hacker" (Max).

"Hackers are the ones who provide the necessary tools like coding, credit card login, because you cannot just gain access to this personal information without these hackers. you don't know these hackers, you meet online as well, it is strictly business most of the time, but you can build a friendship with the hacker to gain trust, because they are scammers too. You give them money for tools, they will give you fake tools or even ignore you… but the truth is that we need them, and they are very important in this our game, without them there is no way we able to get the login for into some banks, or credit cards, or join a paying dating site" (Yoni).

The above information suggests that cybercrime perpetrators are very dynamic in their fraudulent ways. Hence, it is difficult to commit the crime alone in most cases. The connectivity in which the world's population requires relies more than on the state of network architecture, it is more organic, which makes both individuals' and organisations' vulnerability increase exponentially. The data above demonstrates that the organisational network of cybercrime perpetrators in Nigeria is carefully crafted, like a pyramid that allows 'yahoo boys' (cybercrime perpetrators) to conceal and share information among their peers through the established organisational networks and to encourage collaborative means of defrauding victims. These established networks among cybercrime perpetrators enable them to recruit others and improve on their operational skills on the job. Without contest, the development of new technology and new skills has influenced the growth of cybercrime in Nigeria.

The exponential growth of cybercrime practices among youths in Nigeria comes in various forms. Through the operational dynamics of 'yahoo boys', cybercrime in Nigeria has transcended from an individual approach of targeting potential victims, into an organised group that collaboratively spreads attacks on innocent victims. This network architecture and the collaborative enterprise of cybercrime is very broadly connected to their structural organisation. This present study found that the youth that are involved in 'yahoo-yahoo' (cybercrime) in Nigeria participate in their illicit activities independently, following their initial learning process of the cybercrime enterprise in Nigeria. The following thoughts were captured from the participants.

> *"Usually, it not easy working independently these days because so many constraints, so working together as a group assist us in fast-tracking or sometimes beat the system… Every individual or person doing 'yahoo-yahoo' always rely on each other at some point to work together, because we believe that if two people or more work together it*

easier to cash out funds. No man is an island, so we share ideas and views and when the money is out, we share based on percentage" (Chinco).

"There are levels to this job as well. For instance, you can have a rich client, but if you don't know how to manage the client well you might not get as much as you expect, so in that case you will network with other guys who are either advanced in experience or resources" (Mikky).

"The essence of working in group sometimes is to support each other. Take for example if I bring job to you, certainly you will be happy after we have cashed out, with that we have established a network. So, next time if there is an update or job I can easy contact you to work with you again, so we work together to support each other" (Don).

Another participant describes dynamics on how 'yahoo boys' operate in their networked settings:

"There so many categories and dynamics on how 'yahoo-yahoo' is perpetrated among 'G boys' because of the various types of cybercrimes. So, technically, everyone needs each other to cash out… In this game everybody has their area of strength. For example, a 'yahoo boy' that is specialised in online bank transfer or wire transfer, will surely needs an account for his job. In that case what does he do? He will advertise to his friends, maybe through WhatsApp, that he needs a particular type of bank and the bank information, so basically like advertising your product, people interested will contacted you, or refer you to someone if they cash out money will be shared accordingly. The forces at work in this industry is extremely broad, each level in the game requires the experience of an expert sometimes. Some people, their job is to edit documents, graphic designs that can be used to convince a client" (Danny).

All the above submissions support the work of Castell (2011), "Network Society theory." The theory suggests that technology globalisation has enhanced the functions of organised criminal groups worldwide. The ability to do anything from anywhere, because of the opportunity to have pervasive interactions with communication technologies, has cause crime to transcended place and time (Castell, 2000). Cybercriminals interact among themselves on a broad scale and combine their diversified interest in line with this theory. The data reveals that cybercrime perpetrators can establish a clandestine relationship with their counterparts, both online and offline, through their coterie structures cybercriminals can share knowledge and develop new tricks in their fraudulent activities.

Holt and Lampke, (2012) note that, as much as cybercriminals operate in groups, they are still involved in other types of illicit activities to advance their knowledge in the cyberspace. The cybercrime perpetrators interviewed noted that individuals within the groups are allowed to perform on their own, however, some circumstances force them to work collectively as a group to progressively defraud innocent victims. Conversely, within the operational network of cybercriminals, there are a plethora of experts in different fields that enhance the dynamics of cybercrime perpetrators. Some individuals are more advanced in their knowledge than others; for example, those with more technical abilities in graphic design and the construction of websites focus primarily on ensuring the right documents are available to fellow conspirators to defraud victims. They concentrate more on their area of expertise, and hence, collaboration and networking become a mechanism within cybercrime perpetrators.

6.2.3 The Yahoo-Yahoo Enterprise and Spiritualism

Spiritualism is a complex word to describe. It takes on different meanings, relating to things ranging from religion to developmental and personal experiences. Spirituality is another theme that emerged from this study. In West Africa, spirituality is a concept fully derived from Africa's primeval cultural and religious heritage, which includes mythology, beliefs, and the

customs of the people (Mbiti, 1990). This type of practice is common across cultures and is not exclusive to 'yahoo boys' (cybercriminals). Despite Christianity and Islam are the main religions practiced in Nigeria, many of the ethnic groups and tribes belong to their own traditional religious groups (Whitty, 2018). According to Attri (2012), spirituality is, "the basic feeling of being connected with one's complete self, others, and the entire universe." If the essence of spirituality and its importance in human life can be described in an expression, it would be 'interconnectedness'. However, the trend towards globalisation does not have any significant effects on the belief and practices of spiritualism in Nigeria. The fact that contemporary society operates in an e-environment does not discourage the interest of people in using spiritual elements to solve their problems as well as fulfilling their personal interests. Despite the multitude of practices in spiritual belief, people are not misjudged regardless of their religion, belief, or social class.

However, it is important to note that the intention of people who use spiritual elements in their daily activities are motivated by different circumstances rather than always serving their divinity for good causes. In the case of cybercrime perpetrators in Nigeria, literature reveals that cybercrime perpetrators ('yahoo boys') mix in spiritual elements into their practices to boost their chances of quickly attaining success in their enterprise. There are numerous forms of charms that are used in achieving life desires and indeed these charms exist to serve the quest of the procurer (Monsurat, 2020; Whitty, 2018; Tade, 2013). The assumption in Nigerian society is that success is not only attributed to conventional means, rather there is notion fuelled on the belief that a combination of spiritualism and conventional means can encourage success in accomplishing one's goals. The response of this participant corroborates this assertion, as shown below:

> *"As a man, you have to be spiritually rooted in this life to be successful. You need to do some spiritual cleanse in life that will attract luck, protection in your daily life. I do*

things that attract luck and boom my business but this not 'yahoo plus', this is just a way of appealing to the gods to favour me in my deeds. 'Yahoo-yahoo' is my source is source of income, so I do spiritual prayers taking bath in shower to cleanse me away from bad luck or any form delay in my business" (King).

"We have to be honest with each other, to have breakthrough in life, it requires a lot of spiritual intercession. Tell me, how do you think most successful businessmen survival in their business today despite all the competition they face. In my opinion hard work and spiritual intervention is a way to succeed in life. One needs a sort of spiritual back up to break through in their businesses, even politicians have spiritualist working in the background for them. People running small scale business have one or two spiritual element they use to boom their business. That is why if you enter some shop and houses today you will find some sort of spiritual elements for different purposes. So, the same can be said of 'yahoo-yahoo', today in Nigeria 'yahoo boys' use sort of spiritual element in their work to eliminate any kind of delay or bad luck" (Scoob).

An analysis of this data strongly supports the notion that the use of spiritualism could be of importance in the activities of cybercriminals. Although, the discourse in literature describes the combination of spiritualism and cybercrime as cyber spiritualism. In simple terms, the use of supernatural elements to captivate and improve the success of cybercrime is described as cyber spiritualism (Whitty, 2018; Tade, 2015, Monsurat, 2020). This phenomenal practice employed by cybercriminals entails the use of mystical elements to cast spells on innocent people. Through this method, victims become enthralled and, without objection, succumb unconsciously to the requests of these fraudsters (Tade, 2013; Suleiman, 2019). In this social context, the belief in spiritualism cannot be exempt from the mundane activities of 'yahoo boys. There is enthusiasm in 'yahoo boys' to consult with a spiritualist, when they find themselves financial crisis, who assists them to prepare supernatural powers for the sake of their financial

survival and to encourage success in their innovativeness. Another participant, shown below, explained why cybercriminals ('yahoo boys') believe in using spiritual powers to support their work:

> *"At some point most 'yahoo boys' consider using juju, charm, or black powers if they are experiencing a long drought or no returns from activity after investing time and money for a long time. This game is not easy like it used to be some years ago, things are hard now, so you need some spiritual interventions. Personally, I believe in the use of traditional things because everything requires prayers in life. For example, my family believe so much in the use of traditional powers, growing up have experienced some many rituals, like going to the river to wash away bad luck, having incision on my body. Have not even thought of anything like 'yahoo-yahoo', all that was done for me as protection. So, when I started 'yahoo-yahoo', I approached my grandmother who is spiritualist, she helps me with some prayers and some stuffs for me to be favoured in whatever I'm doing. But this is not 'yahoo plus', but it [is] sad that people mistake these prayers, incision, as 'yahoo plus'. In my opinion, if a 'yahoo boy' uses any part of the human body, or sleeping on the burial ground, I consider that as money rituals and not seeking for favour" (Bella).*

In similar interviews, other participants declared:

> *"My brother, in all honesty I will tell you that I consult with spirituality like Alfas and pastors, even herbalist. In all sincerity what I get from them is the e yo nu (appeasing) soap. This soap is for me to see favour in my daily doings which could be offline and online activities. And in reality, it is essential for the existence of man, I have never involved in any rituals that requires human bloods. That is blood money, honestly, and I cannot do that" (Chinco).*

"I'm into romance scam, as you know it is love affairs between me and my clients. So, to make the relationship bond emotionally and spiritually, I take their names to spiritual leaders for prayers and spiritual consultations. The spiritualist performs certain rituals on their names, which makes them extremely fall in love. Many times, the spiritualist ask me to Bo ogun and some other gods with a dog sometimes pig, that my path will be straight, there won't be any difficult. These things work for me. Whenever I make the sacrifices, I start seeing changes. It is better to belief in what works for you" (Tkay).

Another participant mentioned:

"It is normal thing among 'yahoo boys' to consult with a spiritualist, most of us have spiritual fathers we run for help. It depends on your belief, some people prefer going to Alfa, some Babalawo, or pastors. We are looking for where our prayers will be answered. It is particularly important to have these consultations because it not easy to breakthrough in this life. Since 'yahoo-yahoo' is our hustle, everyone wants to be successful in their endeavours. For example, now you might be talking with a client for many weeks, and you ask him or her money, they may say no at first, or they may prove to be stubborn, but once you do some spiritual prayers on them, they will send what you ask them" (king).

The importance of spiritual elements and consultations with spiritualist cannot be understated. The data reveals that 'yahoo boys' firmly believe that combining spiritualism with their enterprise assists them in coercing innocent people into giving away their treasures. Studies have observed that the practices of rituals and spirituality are common attributes among cybercriminals and the main reason of this is to achieve success with their crimes. Some of the elements used by cybercriminals are, "*ase* or *mayehun* (unarguable order), magical rings (*oruka-ere*), and incisions made around the wrist to cast spells on their victims" (Tade 2013,

Monsurat, 2020). The data reveals that these spiritual elements enchant people who are seeking love and romantic affairs online, these groups of people are the most vulnerable and are easy targets for cybercriminals. In recent years, what is remarkable is that most of these victims are mainly swindled in the context of false love and friendship (Trend Micro and INTERPOL, 2017). Therefore, many cybercriminals (Yahoo-Boys), through 'African Jazz', manipulate their susceptible clients into doing their bidding (Ajirola, 2015; Information Nigeria, 2017). These elements cast on the victims puts them under a spell and unblocks the negative energies and thoughts surrounding them.

In regard to the effectiveness of spiritualism in romance scams, these participants' views were captured:

> *"When you use the charm as prescribe by the spiritual leader, with consistency and hard work you will eventually meet someone that will be captivated by your presence, and they fall in love with you. Confidently I can say spiritualism works for 'yahoo boys' in defrauding our clients. It makes our work to yield quick result and elongate the relationship between us and the client. At times it gets to a point these clients are aware they are being scammed but because they are under some spiritual enchantment, they find it difficult to end the relationship" (King).*

> *"Even If the client does not have enough money, in as much the client is under a spell the client will find a mean of getting the money. That is when they apply for loans or sell some properties, until the client pays the money, they won't have peace of mind, but it is usually great to cast spell on the client that is rich" (Don).*

> *"See everything in the life requires prayers. This, our job, is becoming difficult every day, and you can be working for months or even years without making money. For instance, there was time, I was working for almost 5months, and there was no luck, so*

I approach one of my friends that is doing well in the business, I told him about my challenge and frustration on the job, so he decided to take me to his spiritualist for spiritual consultation. The man was an Alfa. When we got there, the man first check what will work for me and told me things about my personal life. That was first time consulting with a spiritualist, I was surprised about some of the things he told me because that was my reality. The man gave me some soap to bath with at a particular time of the day with other things. After few weeks I started seeing changes in my work. This is common thing among 'yahoo boys. There is usually dry season in the job, when things don't go well… you must use spiritual forces to open the doors for yourself. This life itself is difficult, even if you are not a yahoo boy, as man you need it, you need luck and favor in your life, not to talk of this work that we doing that is a spiritual work" (Grape).

In conclusion, in the traditional and cultural perspective, mystical powers are considered to be used in times of frustration or emergencies to find solutions to pressing problems. Although the use of *juju* or charms serve different purposes in life accomplishments, due to a strong desire to quickly achieve success, 'yahoo boys' seek support from spiritualists like herbalist, pastors, and *alfas*, to make enhancement charms to boost their chances of achieving their objectives. The use of these charms and diabolical materials in their search for victims on the internet improves success in cyber criminality. However, this depends on the manipulative proficiency of cybercriminals and the compatibility of the charm or *juju* with their fate, and the authenticity of the spiritualist (Monsurat, 2020). The data above suggests the description of the type of spiritual help they adopt in carrying out their trade brings to the fore the interesting narrative of how spirituality is conceptualised. While most participants agreed that they seek spiritual help from pastors, *alfas*, and traditionalist, they distance themselves from using any form of *juju*. So, spiritual activities like bathing with special soap, fasting, and prayers are

common activities they engage in. The connotations of cyber spiritualism being related to negative sacrifices that have been argued to be remarkably like money rituals, sometimes using human body parts, makes most 'yahoo boys' publicly distance themselves from those practices. Hence, the perception of cyber spirituality is very dynamic. While arguments in literature report various types of spiritual help sought out by 'yahoo boys', findings in this study suggest that most 'yahoo boys' believe that getting spiritual help in the form of prayers, fasting, and bathing with soap for good luck are very normative and more aligned with their cultural practices. God, or rather the supernatural, is believed to be the custodian of success and must be consulted in all matters.

6.2.4 Romance Scams: Understanding One of the Most Common Types of Cybercrime in Nigeria

The last theme that will be discussed is romance scams. This type of cybercrime is the most common among cybercrime perpetrators. Online dating has been an important part of modern life. It is one of the most popular activities in the cyberspace. According to Paisley (2018), 41 per cent of online singles have used dating apps and dating websites, globally. Data from the study shows that men are more likely to be more involved in online dating than women. Social networking has become the conventional way of interaction, whereby people meet in the digital space. However, some people have benefitted while others have fallen victim to romance scams. Thus, concerns regarding identity and trust are considered. For instance, when two people establish contact on the dating website, the issue of trust and identity do not take long to come to the forefront. Cybercriminals are notoriously known for using fake identities on dating websites to trick into people who are seeking for relationships to fall in love with them (Whitty, 2018). In spite these concerns, people still desire companionship in life through dating websites.

The embryonic trend of social networking has made many falls victim to the activities of cybercriminals who use dating websites to defraud people. The massive growth in internet users is a driving factor for more social media and dating website platforms. The social media community provides ample space to build new relationships outside the existing social networks of humans while ignoring geographical boundaries, thus, increasing the potential numbers of victims. This can be observed in the following narratives, as expressed by participants:

> *"Dating job is what many yahoo boys start with, this is because it is easier to access and it does not cost much, to begin with, all you do is sign up on a dating website posting as a white man or woman depending on who you choose to chat with, but most of the time is usually women because their heart is soft and they fall in love easily, unlike the men they don't fall in love with you easily. But to attract potential clients your profile most be very attractive, that is the first step, if your profile is that attractive clients will be the ones writing to you and wanting to meet you. So, on the website you start liking their profiles and start a conversation, these conversations could go on for days or week before asking for their contact like email address, phone number. The essence of this is that it makes communication more private and to build a more solid relationship" (Amigo).*

> *"I use various dating websites to search for my clients by creating an attractive profile using a white man's picture to attract women. As you know the site is free, that makes it easy. On the site I talk to many women, maybe 10 to 15 people, then I start examining who is likely to be a potential client base on our conversation, some people will like you, some people won't give you attention, so it varies but at the end I might end up talking to only one or two women that will be my client. As soon as I'm able to realise that she a client what I do is to take her away from the site and tell her to delete her*

profile, this is a way of preventing her talking to others and concentrate on me. At this point I will ask for her phone number then we start an intimate conversation through WhatApps or text messages" (Gabby).

On being asked further what the relationship with the so-called clients is like, the following participant noted:

"[Online] Dating is like traditional dating too; it takes a while for the client to trust you and want to commit to you. The main key is keeping constant communication with your clients for example in the morning, I write my baby or call her on the phone and at night I call her too and we talk for hours, I make love to her on the phone. I make her happy and put a smile on her face. For instance, one of my clients, when comes back from work and tell me her colleague says she lively and happier lately, this is to tell you that these women are lonely they need someone to talk too. She will tell me her colleague at work knows she been very happy late, then gradually we start gaining each other's trust. Once I'm able to do that for her it's easy to commit to the relationship" (Scoob).

"By talking to my client every day makes them happy and they get excited to meet up with me because of the emotions and feelings that has developed between us" (Blackie).

Interviewer: "How do you gain their trust of the victims?"

"You know online you meet different people with different characters. Some are very curious and ask a lot of questions if you able to answers all the questions satisfactorily they assume you are real and they start doing anything for you, like sending you money" (Blackie).

When asked what the appropriate time to ask the client for money is, the respondent stated:

"Well, it depends on how deep the relationship is, how emotionally connected the client is, it also depends on how the client has been able to gain your trust and believe you, then you can ask her money. There are some clients that are willing to give you everything in a way to meet you because they are already in love with you. And there are some based on their experience they don't even want to hear about money, once you mention money, they stop talking to you. But mostly the reason for asking them money is for us to meet up and start a relationship together that we have both fictionalised together" (Blackie).

Another participant noted:

"*These clients when you are able to get them to fall in love with you, they become desperate to meet you, so you take advantage of the moment to ask for money. Because they are already in love and they are desperate to meet you, they submit to your offer" (Jago).*

Comparing the responses of various participants, the following was stated by another "yahoo boy":

"I talk to male clients; these men are usually not after love or affection unlike the women. You can arguably say that most of the older women on dating websites are genuinely looking for love, while the older men are looking for younger girls to take advantage of. Most of them just want to have sex and they are very greedy, so it different from talking with women. Women easily fall in love with you but the men they don't fall in love like that, they are after sex most of the time that is why they fall victim of scam. In this form of relationship, the man is after sleeping with you, or after your own money too, because you also tell them you have money or something very valuable. In their

mind they think if they are able to meet you, they sleep with you and take your money or valuable good" (Drama).

Another participant relates through his experience in this context:

"It is similar to that of older women you meet online looking for relationship too, you will create a profile of beautiful, young woman on the dating site, and you age target will 50 to 60 years old men, because they want are looking to prey on younger women they quickly fall in love, then from there you can ask them for money. Some will give you because they want to sleep with you. Let me share this story with you, I had this client sometimes ago, he is man he who like to sleep with younger girls. Imagine this man told me he sleeps with his own daughter, and he has been doing it for years, then at some point he told me that he would like to sleep with my daughter that she is very seductive. So now imagine it if it was in real life that is what he will really do to my daughter, so I don't pity him at all" (Agba).

Supporting this avowal, these participant statements were captured:

"No job me self they do my brother, do you think it's easy for me to be on my laptop updating clients, making sure her day is okay, making sure that she is happy all the time? In reality, if her husband needs little money why she no go give him, so we are both benefiting, that is when they find out you are scamming them, they still want to hold on to the relationship. It's like an open market business or game, these clients are lonely and looking for love, happiness, and is money boys they find, so we are both helping each other" (Kadriz).

The above submissions reflect that human interaction has been revolutionised through communication technologies, which has given the rise to new forms of crime and deviances, in which romance scams are not excluded. The data suggests that the tenacious growth in

romance scams is something that cannot be impeded as users of social media and online dating sites continue to grow rapidly due to the conventional social means of interaction. The study of Duggan and Brenner (2013) notes that over half of the adults of ages 50 to 64 fall victim to this heinous crime which comes with huge financial and emotional implications. This age represents typical targets for 'yahoo boys' (cybercrime perpetrators) who, under a fictitious profile on dating network sites, 'cat-fish' for potential victims. Although there is a massive number of reported cases of romance scam victims across the world and the psychological damage it has brought on affected victims, it seems the number of victims is surging.

New statistics suggest that there is a nearly a 40 per cent increase in reported cases of romance scams since 2018 (FTC, 2020). Therefore, the findings from this study understand that people who have failed in their attempt to establish a relationship through conventional offline networks, or have chosen to pursue a relationship online, potentially fall victim to a romance scam. 'Yahoo boys' in this study submit that they benefit from innocent people who seek romantic relationships on various dating websites by presenting themselves to be potential spouses, a relationship that often begins with being friends on a dating website before developing into an intimate relationship that is based on trust. The accounts of the participants reveal that victims of romance scams are assumed to be driven by a quest for love and happiness but, as the relationship matures, these vulnerable people trust the cybercriminals after several convincing conversations and are ready to assist their imaginary partners, serving as evidence of commitment to the relationship. Also, the data deduces that some participants describe their relationship between them and their victims as beneficiary. Putting that into perspective, 'yahoo boys' have rationalised romance scams in a way that makes them free from moral guilt. This is in the sense that the unlawful act is being justified as rendering a pleasurable service to victims as their relationship with them progresses.

6.3 Conclusion

This chapter concludes the second part of the findings, in which four themes emerged. The themes represent the challenges confronting young people and the societal strains that influence youth into partaking in criminal activities, especially ‘yahoo-yahoo’. Also, the sociocultural and sociopsychological phenomena related to cybercrime and cybercriminals were examined.

The first theme demonstrated how poverty and unemployment encourages youth participation in cybercrime in Nigeria. The discussion from the theme reveals there is a link between unemployment, poverty, and crime. These two variables make the youth susceptible to both traditional crimes and cybercrimes.

The second theme reveals the transnational network and operational patterns of cybercriminals, while the third theme examined the relationship between spirituality and cybercrime. The findings reveal that ‘yahoo boys’ use spiritual and traditional elements to cast spell on their victims. Also, the themes show that many of the participants have, in one way or another, attempted the practise of cyber spirituality to support their crime enterprise. Lastly, the nascent trends of social networking and interactions were discussed. Many of the participants agreed to the fact that social media platforms have become a metaphorical pool of fish where they meet their next victims

CHAPTER SEVEN

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

7.1 Introduction

This study aimed to investigate the lived experiences of cybercrime perpetrators in South-West Nigeria. The study set out on the premise of fully addressing cybercrime in Nigeria, to achieve this it is important to have a comprehensive understanding of cybercriminals' experiences and the dynamics of cybercrime in Nigeria. This study brought to the fore some of the factors that influence the youth to participate in cybercrime within the study location. Unemployment, poverty, poor educational structures, and other socioeconomic elements were among the prevailing factors that lured young people towards criminal behaviours, particularly 'yahoo-yahoo'. To achieve the objectives of the study, secondary sources of data in the form of published literature, such as academic studies, journal articles, and newspapers, were examined. The data that were gathered directly from the fieldwork became a key source of information that was relevant to the study on 'yahoo-yahoo' (cybercrime) in Nigeria. From the findings of the study, addressing a phenomenon of this magnitude cannot be accomplished through a simple approach but rather it requires a conscious understanding of some fundamental issues. Finally, this chapter presents a general summary of the key findings from the study and then integrates them with the theoretical framework of this study.

7.2 Key Findings

7.2.1 Nexus Between Unemployment, Poverty, and Cybercrime in Nigeria

The idea that unemployment encourages criminal behaviour is intuitively appealing, this is based on the premise that individuals respond to incentives. Unemployment and poverty levels in Nigeria are one of the best indicators that the country's economy is in serious crisis. Youth unemployment has also remained high in the country for a long time. Unemployment and underemployment are some the factors often contribute to poverty. In simple terms, many people are poor today simply because they are jobless. Without a doubt, unemployment is

definitely a global trend with social economic, political, and psychological implications in developing countries worldwide. Thus, huge youth unemployment is a warning of far reaching, complex problems in any country. However, it became apparent in this study that the fear of unemployment and poverty has turned ‘yahoo-yahoo’ (cybercrime) into a habitual lifestyle for young people in Nigeria.

The findings of this study suggest that unemployment is a major problem confronting young people, with a massive number of unemployed youths becoming involved in social criminal activities, particularly ‘yahoo-yahoo’. This is all in relation to the relative deprivation of gainful employment for the youth in Nigeria. The most striking and clear relationship between unemployment, poverty, and cybercrime is that ‘yahoo-yahoo’ has become an innovative solution adopted by the youth as a means of survival, at the detriment of the social morals of the country. Interestingly, it arguable that ‘yahoo-yahoo’, as an illicit act, is deeply embedded in contemporary society.

7.2.2 ‘Yahoo-yahoo’ as Organised Crime: Organisational Structure and Apprenticeship

The internet has become one of the most significant elements defining the cultural space of contemporary society. As technology evolves, cybercrime becomes a part of the virtual world, thus, increasing the number of victims and perpetrators. This section describes some of the things involved in the learning process to becoming a cybercrime perpetuator. Also, peer influence emerged as a significant factor to consider in understanding how young people become introduced to cybercrime. This is not far-fetched because social interaction has become an essential aspect of society; through social interaction with peers, information is shared, and more knowledge is gained. In relation to the role of peer groups, the study found that interaction among peer groups who are involved in cybercrime activities brings about harmony and this leads to confirming strictly to these criminal tenets.

The findings in this study suggest that social networking is a fundamental factor sustaining the organisational structure of 'yahoo-yahoo boys' in Nigeria. They have built a state, regional, national, and even international network of hackers, spammers, and cybercrime perpetuators and through this approach they are able to increase the prospects of their enterprise. Hence, this study suggests that cybercrime perpetuators metamorphosised from individuals with intent to members of a collective and transnational cybercrime network. The findings indicate that collaborative practices are a common characteristic of cybercriminals, and their atrocities require a multilevel operation that involves hackers and informal networking among other cybercrime perpetrators and different institutions. Also, findings from the participants revealed that cybercriminals engage in different types of cybercrime, such as romance scams, lotto scams, and fake business proposals, and they even involve their clients in the criminal activities without their knowledge. It is noted that social media is a popular medium employed by cybercrime perpetuators for 'cat-fishing'; from the responses, dating experiences can be related to a real-life situation where relationship is built on love and trust, but in this context, there is an intent to defraud.

Furthermore, on the basis of the findings and the explanation above, a majority of cybercrime perpetrators start involving spiritual elements to quickly fast-track their financial success after learning their trade. This practice is a common behaviour among 'yahoo-yahoo boys', the common characteristic is that they are deemed to be motivated by the desperation to make fast money. Though, the participants blame their involvement in cybercrime and cyber spiritualism on the frustration of the socioeconomic problems in Nigeria. However, the practice of spirituality represents a wilder culture in Nigerian society since people deeply adhere to their religious beliefs. Therefore, the connection between cybercrime and spiritual practices may not be exclusive, thus, the application of spiritual elements in the cyberspace represents the sociocultural inclinations of subscribing to the supernatural for success and prosperity. The

findings reveal that the concept of cyber spiritualism and the strong belief in the effectiveness of these spiritual elements, and the role spiritual leaders' play in supporting this crime, cannot be understated. The application of spiritual elements on victims, and the sacrifices cybercrime perpetrators make for themselves, either for protection or to procure good luck and success, reflects the interconnectedness between the spirit world and human existence.

7.2.3 Perceptions of Government Initiatives and Strategies in Combating Cybercrime: A Bane or Solution

The rise in cybercrime is a major concern to the world, particularly with regards to e-commerce. This hideous trend has impacted virtually all sectors of society and is adversely affecting the image of Nigeria. Nigeria is considered one of the countries with the highest levels of cybercrime activity in the world. However, the fight against cybercrime, is confined within the legal structures that guide cybercrimes in Nigeria. To this date, the only strategy the government has introduced to pre-empt, and tackle cybercrime is the Cyber Crime Act of 2015. In this regard, the Economic and Financial Crime Commission and the Nigerian Police Force function within this framework. Regrettably, as was discovered from the findings that, this mechanism is ineffective to curbing and preventing youth from undertaking cybercrime related activities. This discovery indicates their underlying issues, such as unemployment, poverty, and poor youth development programmes that require urgent attention because the existing strategies are apparently not effective enough to deter and curb young people from desiring a life of cyber-criminality. It is sufficient to say, therefore, that addressing core socioeconomic factors predisposing young people to cybercrime will go a long way in reducing its spate and to curbing the menace rather than just focusing on punishment. From the findings it is evident that more needs to be done to address youth involvement in 'yahoo-yahoo'; combatting a crime of this magnitude requires a holistic approach in all ramifications. From the findings, it is notable that the government and its stakeholders should be more responsive and start adopting the latent initiatives that developed countries have used to control youth crime. For instance,

sport and youth development are common approaches to crime control in some European countries and in the United States. The desirability for an innovative idea like the involvement of the youth in sport and entertainment programmes which can easily captivate the interest of young people should not be negotiable in the fight against crime in Nigeria.

7.3 Theoretical Reflection of the Dynamics of Cybercrime in Nigeria

Robert K. Merton's (1938) strain theory and the rational choice theory were both adopted into the theoretical framework on which this study is premised. Merton proposes strain theory to suggest that social deprivation may prevent people from having access to the legitimate means of achieving culturally accepted goals under certain socio-economic circumstances, placing pressure on the citizenry to turn to the use of illicit means to accomplish culturally accepted goals. Merton's strain theory views crime as a result of a disjoint between cultural goals and the means to achieve them. In other words, social standards exist, and at the same time, the means of achieving these goals have been specified by society. However, individuals can deploy their own means to eschew the approved means whenever there is a disjoint between the goals and the means. The theory was beneficial to the study because it describes the growing trend of cybercrime among Nigeria youth, especially by highlighting the socioeconomic strain prevalent in the country as discussed thus far in this thesis. Examining the relevance of the theoretical perspectives to the responses of participants, it was discovered that the youth desire an improved livelihood for themselves, and they wish to enjoy a certain lifestyle of comfort that has become exceedingly difficult to achieve in Nigeria for reasons related to high levels of youth unemployment and poverty among other things. Many of them are driven by material success, thus, the societal means of achieving wealth and living flamboyantly are commonly achieved through illegitimate means rather than the legitimate means of hard work and educational attainment.

These findings enabled the researcher to conceptualise that social discomfort, infrastructure deficiencies, economic vulnerabilities, and an inability to meet one's needs are possible causation factors causing strain, which predisposes people to seek redemptive paths and conform to deviant practices. However, in this context, 'yahoo-yahoo boys' are young individuals within society who are experiencing social stressors and are exploring the opportunities available to them to achieve their goals, even when through illegal means. Also, the findings derived from the participants' narratives supports the aspect of Merton's theory which argues that most people have similar ambitions, but they never have equal opportunities. In the event that people fail to achieve society's expectations through approved means such as hard work, they may attempt to achieve success through criminal activities, specifically in this case 'yahoo- yahoo'.

In addition, the study found relevance in the rational choice theory. This theory suggests that people choose all their behaviours, including criminal behaviour, and that their choices are designed to bring them pleasure and mitigate their pain. Societal gaps have presented the youth with innovative opportunities, particularly 'yahoo-yahoo', which many participants considered better than traditional street crime. Participants' responses suggest that the youth consider cybercrime as the easiest means in which to attain success and reveals that act is a rational decision. Their accounts support the argument of rational choice, that the options available will influence an individual's sway in their economic pursuance.

Hence, if an initiative is set up to give the youth a sense economic worth and responsibility, it might control traditional and conventional crimes, to an extent. This study finds the theoretical framework germane because it complements the human dimensions and describes reasons as to why individuals commit crime. Although, strain theory concentrates on the society and the failure of law and order as a rationale for deviant behaviour., whereas rational choice theory focuses on the individual as a rational being. That is to say that people assess the cost

advantages of their choices before acting on their decision. These findings expose 'yahoo-yahoo boys' as conscious people who are rational in their decisions and people who understand the consequences of engaging in cybercrime but think the rewards of swindling people outweigh the punishment. This explains certain factors that were mentioned in the study, like peer influence, gaudy lifestyles, and the get rich quick syndrome. Many of these individuals see hard work as an impossible means to success and thus take the easy way out.

7.4 Poverty, Unemployment and Moral Decadence: A theory of intersecting disadvantages aiding cybercrime in Nigeria

Poverty has been regarded as a new form of concern in the modern world in recent years, particularly in the developing world. In either a personal or communal context, poverty is defined as the inability of a person to reach a specific level of the bare minimum of requirements for subsistence (Atkinson, 2019). In this context, poverty is a relative concept that is decided by the overall standard of living in a society. Individuals and families are put under additional stress when they live in poverty, which can sometimes lead to criminal activity in order to meet their immediate needs.

There is no doubt that there is a nuanced relationship between poverty and criminal activity, according to the findings of this study, poverty is the fundamental cause of many deprivations and frustrations and this result in social unrest, that cannot be overlooked. In this study, the researchers confirmed that there is a favourable co-integrating association between poverty and yahoo-yahoo (cybercrime) in Nigeria. It might be argued that the desire for economic liberation has finally resulted in many Nigerian youths becoming involved in yahoo-yahoo. Furthermore, it can be concluded from the findings of this study that the Nigerian government has not done much to address the socio-economic issues that have created a strain environment predisposing individuals most especially the youth to seek redress and solace through yahoo-yahoo and other deviant behaviors in the country. The issue of poverty in Nigeria is worrisome, and the

government and political elite should respond positively at this point by establishing and implementing rapid and sustained economic growth policies and programs in areas such as education, entrepreneurship, and productive resources. Also, impoverished individuals should be empowered by including them in the development and implementation programs aim to reduce and eradicate poverty. Their participation in such initiative program would give them a sense of inclusion, and guarantee such program represent their needs and interest. In relation to poverty, there is nothing inevitable about it. The government should take responsibility by re-examine the underlying causes that have contributed to persistence of poverty in the country, develop the political determination to implement policies to improve economic security and expand opportunities for young people.

Economic hardship and crime are perennially contentious issues in the fields of criminology and sociological literature. Several academics have proposed that unemployment can lead to a cascade of criminal activity. The statistics on crimes and other related offenses in many countries reveals the linkage between unemployment and crime. Although crimes are committed for different reasons and in variety of ways, however not all crimes can be traced back to lack of employment opportunities. Yahoo-yahoo (cybercrime) in Nigeria, according to recent studies, including this study, is highly associated with unemployment in the country. One of the primary arguments in this discourse is that Nigeria's growing poverty is exacerbated by the continuation of long-term trends in young unemployment and governmental corruption. Frustration, inability to earn a living, and unemployment are all factors that contribute to youth involvement in cybercrime, according to Adesina (2015).

The problem of unemployment has grown into a serious issue plaguing the lives of Nigerian youth, and as a result, the country's society is at risk of being undermined. The phenomenon of youth unemployment has far-reaching consequences for both the individual and society at large. This study also revealed that the high rate of unemployment in Nigeria is a significant

motivator for young people particularly undergraduates to engage in criminal activity. Many teenagers have been drawn into yahoo-yahoo because of a lack of job prospects. Several studies have also demonstrated that some graduates are eager and capable of working but have been unsuccessful in finding employment. According to the findings of this study, incessant unemployment frequently results in a sense of despondency, particularly among young people, and can trigger angry expressions that can lead to criminality, such as yahoo-yahoo (cybercrime) and other atrocities that can be perpetrated out of frustration. Additionally, unemployed cybercriminals who have been apprehended for their involvement in cybercrime are more likely to re-offend and return to their criminality after serving terms of incarceration. Thus, persistent unemployment can compound an individuals' involvement in cybercrime and other related offences.

Nigeria's high level of corruption has prevented the country from creating a thriving economic, even though the country has numerous natural resources to offer. Throughout the country, massive corruption is perpetuated in every sector and has permeated every aspect of Nigeria's societal structure. Thousands of dollars intended for development projects that could have created jobs have been misdirected, embezzled, misappropriated, or being held in foreign banks by politicians and other political stakeholders. Enduring corruption has deprived the country of the opportunity to use available resources to improve the quality of life for its citizens most especially youth the future of the country. In Nigeria, yahoo-yahoo (cybercrime) is a significant problem, as evidenced by the findings of this research. Some studies have also investigated cybercrime and the activities of yahoo-yahoo boys and have made categorical assumption that the growth of the phenomenon is as a result of the state neglect owing to corruption and the relative deprivation of large percentage of young people by the government (Titilayo, 2011;Tade 2013; Adesina, 2015).These data reveal that majority of yahoo boys (cybercrime perpetrators) are youth many of which are unemployed who are finding a way out of the trap

of poverty. The frequency of the criminal activities as recorded is a cause for serious concern. Therefore, it is imperative for the government to rise up to the occasion as address the issue of corruption that is deep rooted all government parastatals

The problem of moral decay among Nigerian youths is a contemporary issue that is pervasive and dominates everyday discussion, as well as making waves on social media periodically. It is astounding to learn that youth of nowadays are characterized by immorality. There is a significant deterioration in the moral, social, and educational aspects of our society that has taken place in recent years particularly among youths (Chima, 2010). However, moral decay in our present society has become a contentious subject since society appears to be oblivious to the difference between what is morally correct and wrong. As a matter of fact, moral decadence as a phenomenon began slowly and attracts little or no attention in the society, and it has led to a poor breed of youths in the society. Muraino and Ugwumba (2014), described moral decay as the process of acting in a way that demonstrates a lack of regard for moral principles, a progressive debasement of social standard. It is undeniable that moral degradation has totally supplanted fundamental moral value in contemporary society. This devastating phenomenon is at the root of some of the most serious difficulties that Nigeria is currently confronting as a nation. It is a phenomenon in which youth do not consider how the future will be better than present, or how to invent new things to automate processes that are involved in our everyday activities, but rather concentrate on how to enrich themselves by any means possible and control great riches at a young age (Afuye, 2013).

In fact, there are times when it becomes difficult to know where to begin when explaining the numerous immoral behaviors exhibited by some youth which have destroyed the image of the country. Due to lack of moral education, many Nigerian youths have come to see anti-social behaviors such as cybercrime as a means of enriching themselves. Thus, yahoo-yahoo (cybercrime) , student prostitution, political thuggery, kidnapping have in recent times, become

major sources of income in Nigeria, this unvalued lifestyle also includes drug abuse and money rituals etc. This study uncovered that relative deprivation and corruption among political elite is a powerful driving force for a number of anti-social behaviors that are frequent among Nigerian youths, such as indolence and not wanting to engage with conventional means of income. This explains why so many youths are engage money rituals, Yahoo-Yahoo, and Yahoo Plus. Conversely, Nigeria youths have misinterpreted and underappreciated the impact of the digital revolution they are caught in the web of different typologies of cybercrime.

The importance of youths in every society cannot be overstated, to the point where youths are used as a criterion for assessing the growth of any nation, including the development and productivity of its economy, as well as the development and productivity of its society. However, the government and the political elites have neglected the possibilities of empowering the youth neither are they being prepared for a brighter future. Based on this premise there are great deals of deviant behaviors from the youths in the society. Therefore, this study argues that there should be widespread shift in attitudes and motivations on the part of the government, and people of thoughts in the society towards meaningful mobilization of the youths for national development in Nigeria.

The government and political elites, on the other hand, have turned a blind eye to the potential for young empowerment and are failing to prepare them for a brighter future. There is a substantial amount of aberrant behavior among young people in our culture as a result of this concept. Consequently, the findings of this study suggest that there should be a widespread shift in attitudes and motivations on the part of government officials and individuals of influence in the society toward successful mobilization of young people for national development in Nigeria.

The global nature of the internet has resulted in enormously increased opportunities for cybercriminals. Computer crimes is increasing becoming one of the main threats to the wellbeing of the nations of the world. Therefore, there is a crucial need for a common understanding of such criminal activity internationally to deal with it effectively. It is likewise very important to delve into the lived experience of cybercrime victims, especially the victims of romans scam, this will understand the drive for their susceptibility to the crime of the nature.\

7.5 Policy recommendations

Policy recommendations are required for research of this nature, they are especially important for research that focuses on crimes including cybercrime (yahoo-yahoo). As a result, the policy recommendation enumerated in this study are consistent with the primary results presented in the previous chapters. Moreover, this study has demonstrated predisposing factors responsible for cybercrime and how intertwined these factors are within the local context of the young people and wider Nigerian context. Without no doubt Nigeria faces a critical challenge in curbing yahoo-yahoo menace, therefore there is need to project and execute useful, realistic, and transformative policy recommendation as well as preventative strategies that will deter younger generations from engaging cybercrime (yahoo-yahoo). This policy will support existing mechanism that aid to curb the menace. The following recommendation are offered in the light of the findings of this study.

7.5.1 Reflections on the Dominant Socioeconomic Challenges Predisposing Youths to Cybercrime and Ways Forward

This study identifies those socioeconomic challenges, and a dilapidated educational institution as some of the reasons why many youths engage in ‘yahoo-yahoo’ in Nigeria. Although there are other related factors, such as greed, contributing to the prevalence of the ‘yahoo-yahoo’ phenomenon, socioeconomic deprivation and a lack of education culture is foundational in the issue. In that regard, it is necessary that governments introduce and reinforce functional structures that will positively impact the lives of young people. The provision of basic goods

and services that meet the needs of the people should mainly include employment opportunities, an improved educational sector, and good health care services among other initiatives that could improve the livelihoods of all and sundry. Similarly, young people should be given opportunities to participate in politics and the economic planning of the nation. In doing so, the youth can influence the implementation of policies towards youth development and initiatives to boost the overall well-being of young people in society, thus, giving the political landscape of the country a different shape. Also, it is crucial to remember that cybercrime is inextricably linked to pervasive corruption, a difficult economic climate, and abject poverty on a global scale. For the Nigerian government to effectively combat cybercrime and other related offenses, it must first attack the root causes of the problem. In this context, attacking the root causes includes good governance, transparent electoral processes, and accountability in government, all of which translate into more improved opportunities, improved jobs, functional education structures, a more equitable investment climate, and ultimately a reduction in the tendency of our citizens to engage in cybercrime and other forms of criminal activity.

Finally, because of widespread corruption that appears to be embedded within the government system and which undermines the effectiveness of the legal framework responsible for curtailing Yahoo-yahoo, the government should begin to consider solutions from socioeconomic and political perspectives rather than relying solely on the EFCC and other law enforcement agencies in its efforts to eradicate cybercrime. In order to make this recommendation, it is necessary to consider the fact that the rise in yahoo-yahoo and other criminal offenses has been influenced by several factors, including monumental poverty, relative social deprivation, rampant corruption, excessive greed, and materialism, among others. By taking such constructive efforts, we hope to deter the next generation of young people from taking unfair advantage of others.

7.5.2 Empowerment programs for youth

In this case, it is about ensuring equal access to life possibilities for young people who possess the necessary competence and capacities to enable them to engage in important elements of the society. Empowerment programs should include strategies for making decisions in the political and economic spheres of social life, as well as the provision of vocational skills to unemployed youth. This study suggest that vocational education should be addressed with urgency, as describe by Wolf (2011), vocational education is any form of education that has its primary purpose as to prepare persons for employment in recognized occupations. It provides the skills, knowledge, and attitudes necessary for effective employment in specific occupation. This has to do with the provision of equitable opportunities for young men and women who possess competence and abilities to enable them to participate in key aspects of life. Therefore, the Federal government should lean towards improving existing vocational schools and if possible, create more across the geopolitical zones of Nigeria, particularly in the Southwest region where cybercrime is dominant and growing reprehensibly.

The improvement or establishment of these institutions will provide industrial, mechanical, technological training programs that will enhance the development of young people. For instance, a functioning institution like this will be an enabling platform for youths to be licensed or certified in various field such as auto mechanic, electrical engineering, farmers, and trade learning. But on the contrary it appears that the educational sector and stnow in Nigeria has embarked on deindustrialization of younger people because many youths focus more on going to tertiary institution and become unemployed after graduation, no wonder there many unemployed youths roaming on the street aimlessly, this inclination suggests that Nigeria is a certificate driven society, rather than skill empowerment society. As example, developed countries like USA, China, which Nigeria emulate does not emphatically prioritize college or

university education, through their vocational schools' young people are licensed and empowered with various skills.

Nevertheless, not to downgrade tertiary education, but the problem with tertiary education is that it only offers graduates competency of their degrees, intellectual knowledge-based capacity, whereas vocational education will offer practical based skills that can be applied immediately to assist young people make a living for themselves. The findings from this study reveals that most of what is taught in tertiary education is not economically relevant to contemporary settings, therefore this research urges the Federal government to implement policy that makes it mandatory for young people irrespective of gender to attend vocational schools after their secondary education to learn skills and trade school for two years, get certified in practical skills before proceeding to university. This policy will be effective in the sense that it will decolonize the mind of the younger generation and save them from the pipeline of yahoo-yahoo and other form of criminality. Further, government that utilise the money and resources apprehended from cybercrime perpetrators (yahoo-yahoo boys) to fund these vocational schools and create sustainable structures that will encourage this idea thrive and attain it aims and objectives.

7.5.3 Cooperate fight against Corruption

Corruption has in many ways emerged as the most concerning issue of the 21st century. The phenomenon in recent time has negative impact in several ways. Government and their ability to steer a country toward high economic growth and shared prosperity have been undermined by corruption, which erodes the credibility of the public set as well as trust in government. Corruption, on the political level, undermines the legitimacy of political systems by providing elites with alternatives to genuine democratic choice as a means of maintaining their positions of power. This study revealed that corruption is the number one public enemy in Nigeria; its presence is pervasive and detrimental to the advancement of the country, and it encourages the

continued participation of youth in cybercrime and other forms of criminal activity. To conquer the corruption cankerworm, government should opt for a collaborative approach to dealing by combining government efforts to combat corruption at all levels of government and by purging the Nigerian system of this insidious malfeasance. When it comes to addressing corruption, there is no one-size-fits-all solution. However, making settings less conducive to corrupt activities is an example of an open government reform that is useful in fostering openness, inclusion, and collaboration. Although their influence will always be subject to the availability of other critical enabling variables, such as political will, an independent media, and a vibrant civil society, a free and accountable media, and efficient sanctioning systems, are necessary prerequisites.

7.5.4 Youth Sport as a Key Factor in Changing Wealth Narratives Among Young People Leaning Towards 'Yahoo-Yahoo' as a Way to Attaining Success

The idea that sport is an interesting attraction and inspiration for young people around the world is consistent throughout modern history. In this regard, the beneficial impact of sport extends beyond the euphoria of sport itself. Sport has the power to address some of the social problems and global challenges confronting young people. Socioeconomic problems and crime, including cybercrime, are inextricably related in the Nigeria context. The primary objective of sport is not to reduce or prevent crime, but rather it can be an immensely beneficial tool to tackling socioeconomic issues. This study implores the government to look at a range of sporting events that could assist young people and guide them away from traditional and nonconventional crimes. There needs to be sport initiatives that enable young people to take part in developing their skills and programs that allow young people have a sense of belonging as this can definitely minimise situational crimes and develop other pro-social behaviours.

Combined with existing frameworks, youth sport and development programs can contribute to curbing the present and future menace of 'yahoo-yahoo'. Youth empowerment through sport activities is a strategy capable of controlling deviant behaviour by providing appropriate and

accessible social support. In other words, sport and the social fabric of Nigeria society must be related positively as this will improve sports-based intervention programmes and allow them to thrive; it will also provide an opportunity for international collaboration with sport organisations. Sporting activities, such as chess, scrabble, tennis, soccer, should be heavily invested in by the government. Interest in these sports should be encouraged right from primary school to improve the mental and academic capacity of children. Young people should be encouraged to take up sport as a career vocation. This will be discussed in the following subsection.

7.5.3.1 Developing a Grassroots Soccer Initiative

According to the Youth Empowerment and Development Initiative (YEDI), soccer at a grassroots level exemplifies how sports can enhance the effectiveness of health education and crime control. The best values of sports, integrity, inclusiveness, and empowerment, mutually reinforce other public health and youth empowerment objectives in this model. Soccer is a beloved game in Nigeria and a grassroots soccer initiative should be put in place which would concurrently engage the youth and communities to come together, strengthening community support, promoting public health awareness, and distracting vulnerable youths from crime. Designing and implementing the project through training youths builds their capacity and motivates them to succeed independently and also distracts them from anti-social behaviours. A well-structured grassroots soccer initiative would be a reasonable programme to engage youths in. Instead of loafing around, their time will be occupied with physical activities.

Studies conducted by The Population Council and Harvard School of Public Health, Stanford University's Children's Health Council, and the Children's Health Council have consistently and repeatedly evidenced the results of sports as a developmental tool and the programme's positive effects on children in the developing world. These studies have documented a grassroots soccer model's effectiveness in significantly improving students' knowledge,

attitudes, communication, and decision-making skills as well as reducing risky behaviours. There is a need for environmental development and a systematic infrastructure build up in communities to help make the pro-social choice more attractive for youths than the anti-social choice.

7.5.3.2 Youth Challenges

This initiative can be adopted in Nigeria to give youths from the 36 regions the opportunity to be involved in an interstate competition which would include widely acclaimed sports like football, basketball, and tennis to name a few. Participation will be restricted to unemployed graduates and perhaps uneducated youths. This competition should be highly incentivised and should be accompanied by positive media attention. Capital can be raised partially from sports fans and the federal government can supplement the programme. The initiative would be structured by each state and youths will be divided across sports based on their ability and interest. The untalented can take up roles like being water girls and boys, which are crucial to every sport. Youth who wish to be supporters can be taught to be politically correct in the appraisal of their individual teams.

7.5.3.3 Partnership

State government can identify a sports partner to develop a contextually appropriate intervention. These partners should be imbedded and trusted in their communities and have extensive youth networks that can be used to recruit participants in the project. Partnership with international sporting agencies can be agreed on so that they can scout potential players.

7.5.3.4 School Leagues

Universities should be tasked with investing in school leagues. There should be a systematic investment in sports and a relationship should be formed with schools in western countries to allow students to transfer based on sport scholarships. Universities can raise awareness on the soft skills gained through sports through increased cross-sector cooperation. The empowering and building capacities of sport and youth organisation allows educational institutions to

develop and impart sports-based employability for young people. The collection, classification, and promotion of African good practices in the field of skills development through sports and sports-based employability programs would be an imperative effect of this programme.

7.5.3.5 Adopt an Athlete

This initiative was initially adopted by the Nigeria ministry of sports to increase funding for the development of sport in the country in the build-up to next year's Olympic Games in Tokyo. Its model can, however, be extrapolated to fight domestic crime. The initiative should be run as a campaign where individuals and companies pick an athlete, athletes, or a team and sponsor them. By organising an annual athletic competition, companies and rich sport enthusiasts will be implored to scout for prospective athletes they can invest in. Adopted athletes will be provided with financial support that will boost their preparation for various sport competitions Through this adoption they will enjoy the best training, get the best coaches, and will be able to attend trials and pay any medical personnel needed.

7.5.3.6 Sport Marketing

The Nigerian government has been identified as being a major proprietor of sports in terms of funding and administration (Akarah, 2014). Policies have been formulated by the Nigerian government that aim at making the sports sector a contributory sector to its economy base. However, the policies which seek to use the Public-Private Partnership (PPP) model in the sector have not been implemented. Sports marketing in Nigeria pitches the marketing of sports products and services directly to consumers of sports and entails the marketing of other consumer and industrial products or services through sports promotions. It will bolster youths' interest in sport if they realise that sport can be used as a pedestal to showcase themselves to the world. It will also spark interest in other sport related endeavours like coaching, refereeing, and endeavours related to sport health. Sports marketing would be effective in Nigeria if sports activities were designed by the Nigeria sports sector to meet the sports needs and wants of

consumers through an exchange process that is aimed at generating revenue that would develop sports and boost the Nigerian economy. This will go a long way to curtailing internet crime.

The above actions if taken into consideration can become strategies to develop community sport and to encourage parents to allow their children to participate in sports. This will develop all kind of sports at a grassroot level across all regions of the country. The younger people are engaged with sport and physical activities, the more chances are of reducing their participation in criminal activities and creating the vision that their dreams and aspirations of success are valid and realisable through sport, irrespective of their social class, gender, or ethnicity. Ekholm (2013) argues that sports initiative programmes divert young people from youth crime. For instance, Canada has adopted various sports-based programs in a diversion-based approach to deterring young people from anti-social behaviours (Spruit, 2017). Therefore, the study recommends that the policy structure in Nigeria should acknowledge sport as an evidence-based crime prevention mechanism for young people. By implementing effective and organised sport programs across regions, government can deter vulnerable and disadvantaged young people from deviancy and criminal activities, particularly in a country where unemployment is predominantly high. Within this paradigm, sport will exist as a social development and preventive mechanism, it will create different shades of employment, education, generate improvement in the health sector, and offer a wide range life skills and international networks for young people

7.6 Conclusion

Cybercrime has become a subject of interest within the discipline of criminology and social science. This chapter summarised the major findings of the study, clarified its conclusion, and critically examined a list of recommendations which aim to curb the spate of cybercrime in Nigeria. The major findings, as discussed, include that there is a nexus between unemployment, poverty, and cybercrime in Nigeria. Because of this prevailing socioeconomic circumstance,

cybercrime, especially ‘yahoo-yahoo’ as it is popularly called, has grown into an organised crime with functional structures and a system of apprenticeship. As such, participants are of the opinion that the initiatives and strategies implemented to curb the popularity of the crime have been marred by corruption.

Following the succinct summary of findings was a critical and theoretical reflection on the dynamics of cybercrime in Nigeria. A critical, theoretical analysis was presented on how socioeconomic strain has influenced the growth of cybercrime in Nigeria. This was presented through Robert Merton’s strain theory. Also, cybercrime was described an act that is rationally committed by participants after examining the costs and results of the illicit act. A list of recommendations was discussed, and these include those sports be embraced as a part of the panacea to youth crime in Nigeria. This would be putting in place youth development initiatives that will empower young people in acquiring relevant skill and support. Also, developing a grassroots soccer programme, promoting youth sports challenges, creating partnerships with different social sectors for sport development, funding school leagues and competitions, developing sports mentorship programmes, and improving sports marketing. Incentivised supporter clubs for every sport team or athlete would go a long way to preventing youth indolence, hence, mitigating interest in internet crime (‘yahoo-yahoo’). The recommendations above are orientated towards achieving a less criminogenic society by providing sport, vocational education, and youth empowerment as a development initiative to engage with the youths that are most susceptible to crime. It is important to state that addressing the challenges of cybercrime in Nigeria will require a multi-phased approach that addresses the social, cultural, institutional, political, and economic factors that predispose young people to lives of crime.

REFERENCES

Abomhara, M. 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security and Mobility*. **4**(1), pp.65-88.

Act, B. 2014. *Nigeria Ranked Third in the World for Cybercrime*.

Adejoh, S.O., Alabi, T.A., Adisa, W.B., and Emezie, N.M. 2019. *"Yahoo boys" phenomenon in Lagos metropolis: A qualitative investigation*.

Adeniran, A.I. 2008. The Internet and Emergence of Yahooboys sub-Culture in Nigeria. *International Journal of Cyber Criminology*. **2**(2).

Adesina, O.S. 2017. Cybercrime and poverty in Nigeria. *Canadian social science*. **13**(4), pp.19-29.

Adomi E. E., and Igun, S. E. 2007. Combating Cyber Crime in Nigeria. Available at: www.emeraldinsight.com/0264-0473.html

Agnew, R. 1992. Foundation for a general strain theory of crime and delinquency. *Criminology*. **30**(1), pp.47-88.

Agnew, R. 1992. Foundation for a general strain theory of crime and delinquency. *Criminology*. **30**(1), pp.47-88.

Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G., Jackson, D., King, J., Lee, W., Naraine, R., Ollmann, G., and Ramsey, J. 2008. *Emerging cyber threats report for 2009*.

Ajayi, E.F.G. 2016. Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*. **6**(1), pp.1-12.

Ajayi, E.F.G. 2016. The impact of cybercrimes on global trade and commerce. *International Journal of Information Security and Cybercrime (IJISC)*. **5**(2), pp.31-50.

Akogwu, S. 2012. An assessment of the level of awareness on cybercrime among internet users in Nigeria

Akogwu, S., 2012. An assessment of the level of awareness on cybercrime among internet users in Ahmadu Bello University, Zaria (Unpublished B. Sc project). *Department of Sociology, Ahmadu Bello University, Zaria*.

Akpabio, I., 2005. Human agriculture: social themes in agricultural development. *Abaam Publication. Co. Uyo*.

Albanese, J.S. 2014. *Organized crime: From the mob to transnational organized crime*. Routledge.

Amankwaa, L. 2016. CREATING PROTOCOLS FOR TRUSTWORTHINESS IN QUALITATIVE RESEARCH. *Journal of Cultural Diversity*. **23**(3).

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T. and Vasek, M., 2019. Measuring the changing cost of cybercrime.

Aransiola, J.O. and Asindemade, S.O. 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behaviour, and Social Networking*. **14**(12), pp.759-763.

Attri, R. 2012. Spiritual Intelligence-A Model for Inspirational Leadership. *The International Journal's Research Journal of Social Science & Management*. **1**(9).

Awe, J. 2004. *Fighting Cybercrime in Nigeria*. Available at: www.nigeriavillagesquare.com/articles/Guest/2004/11/fighting-cybercrime-in nigeria.html (Accessed 31 May 2018).

Ayantokun, O. 2006. *Fighting cybercrime in Nigeria*. Available at: http://archives.neohapsis.com/archives/isn/2006.92/0298.html (accessed 31 May 2018).

Ayomide O. Tayo. 2018. *How to deal with Internet fraud in Nigeria Pulse tv*.

Bailey, R. 2005. Evaluating the Relationship between Physical Education, Sport and Social Inclusion. *Educational Review*. **57**(1), pp.71-90.

Balancing Act News Update. 2003. *Africa's policies forces begin to gear up to fight cyber-crime*. Available at: www.balancingact.africa.com/news/back/balancing_act_184.htmlforms

Bassiouni, M.C. 1999. *Crimes against humanity in international criminal law*. Martinus Nijhoff Publishers.

Bässmann, J. 2015. Perpetrators in the field of cyber-crime. *A literature analysis on part 1 "A phenomenological and offender typology-based analysis" and part II "Criminological explanations and scope for action".*

Beech, I. 1999. Bracketing in phenomenological research. *Nurse Researcher (through 2013)*. **6**(3), pp.35.

Bernard, H.R. 2002. Research Methods in Anthropology: Qualitative and quantitative methods. 3rd edition. AltaMira Press ,Walnut Creek, California

Bernik, I. and Mesko, G. 2011. Internet study of familiarity with cyber threats and fear of cybercrime. *Revija za kriminalistiko in kriminologijo*. **62**(3), pp.242-252.

Bernik, I., Dobovšek, B., and Markelj, B. 2013. To fear or not to fear on cybercrime. *Innovative Issues and Approaches in Social Sciences*. **6**(3), pp.1-17.

Bhardwaj, A., Avasthi, V., Sastry, H., and Subrahmanyam, G.V.B. 2016. Ransomware digital extortion: a rising new age threat. *Indian Journal of Science and Technology*. **9**(14), pp.1-5.

Bidgoli, M. and Grossklags, J. 2016. End user cybercrime reporting: what we know and what we can do to improve it. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF),* pp.1-6.

Blaxter, L., Hughes, C. and Tight, M. 1997. *How to Research*. London: Redwood Books.

Boyce, C. and Neale, P. 2006. *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input*.

Brenner, S., and Schwerha I.V. J. 2008. Cybercrime havens. *The Computer & Internet Lawyer*. **25**(9), pp.19–21.

Brenner, S.W. 2006 At light speed: Attribution and response to cybercrime/terrorism/warfare. *J. Crim. L. & Criminology*. **97**(1), pp.379.

Britz, M. 2009. *Computer forensics and cybercrime: An introduction, 2/e*. Pearson Education: India.

Broadhurst, R. 2006. Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. 2013. *Organizations and Cybercrime*. Available at SSRN 2345525.

Brown, B.B. 2004. Adolescents' relationships with peers. *Handbook of adolescent psychology* **2**(1), pp.363-394.

Brown, S. 2005. *Understanding youth and crime: Listening to youth?* McGraw-Hill Education: UK.

Bryman, A. 2012. *Social Research Methods*. 4th edition. New York: Oxford University Press.

Bryman, A. 2016. *Social research methods*. Oxford university press. Cambridge, UK: Royal Society of Chemistry.

Bulhan, H.A. 2015. *Stages of colonialism in Africa: From occupation of land to occupation of being*.

Cameron, M., and MacDougall, C.J. 2000. *Crime prevention through sport and physical activity.* Volume 165. Canberra: Australian institute of criminology.

Campbell, T.A. 2015. A phenomenological study on international doctoral students' acculturation experiences at a US university. *Journal of International Students*. **5**(3), pp.285-299.

Cassim, F., 2010. Addressing the challenges posed by cybercrime: a South African perspective. *J. Int'l Com. L. & Tech.*, *5*, p.118.

Castells, M., 2011. Network theory| A network theory of power. *International journal of communication*, *5*, p.15.

Catalano, R.F., Arthur, M.W., Hawkins, D.J., Berglund, L., and Olson, J.J. 1998. *Comprehensive community-and school-based interventions to prevent antisocial behaviour*.

Chang, W., Chung, W., Chen, H., and Chou, S. 2003. An international perspective on fighting cybercrime. In *International conference on intelligence and security informatics*, pp. 379-384. Springer: Berlin, Heidelberg.

Chaski, C.E. 2005. Who's at the keyboard? Authorship attribution in digital evidence investigations. *International journal of digital evidence*. **4**(1), pp.1-13.

Chawki, M. 2009. Nigeria tackles advance fee fraud. *Journal of information, Law and Technology*. ***1***(1), pp.1-20.

Chawki, M. 2010. Anonymity in cyberspace: Finding the balance between privacy and security. *International Journal of Technology Transfer and Commercialisation*. **9**(3), pp.183-199.

Chawki, M., Darwish, A., Khan, M.A., and Tyagi, S. 2015. 419 scams: An evaluation of cybercrime and criminal code in Nigeria. In *Cybercrime, digital forensics, and jurisdiction*, pp. 129-144. Springer, Cham.

Choo, K.K.R. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security*. **30**(8), pp.719-731.

Clarke, R.V.G. and Cornish, D.B. eds. 1986. *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.

Clement, J. 2019. *Number of internet users in Nigeria from 2017 to 2023*.

Coalter, F. 1996. *Sport and Anti-Social Behaviour: A Policy Related Review*. Edinburgh: Scottish Sports Council.

Collins, M., Henry, I., Houlihan, B. and Buller, J. 1999. Sport and social inclusion: A report to the Department of Culture, Media, and Sport. *Loughborough: Institute of Sport and Leisure Policy, Loughborough University*.

Cook, D. 1997. *Poverty, crime, and punishment*. London: CPAG.

Cook, M. 2005. Fraud and ID Theft–The Lowdown on Fraud Rings. *Collections and Credit Risk*, pp.10.

Cornish, D.B. and Clarke, R.V. 2014. *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

Council of Europe Treaty Office. 2015. *Convention on Cybercrime*. CETS No.: 185.R http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Council of Europe. 2001. Convention on Cybercrime. Available at: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (Accessed September 1, 2012).

Crabbe, T., 2008. Avoiding the numbers game: Social theory, policy and sport's role in the art. Sport and Social Capital. Oxford*: Elsevier Butterworth-Heinemann, pp.21-39.*

Creswell, J.W. 2014. The selection of a research approach. *Research design: Qualitative, quantitative, and mixed methods approach*, pp.3-24.

Crossman, Ashley. "Rational Choice Theory." ThoughtCo, Feb. 16, 2021,

Cullen, F.T. and Messner, S.F. 2007. The making of criminology revisited: An oral history of Merton's anomie paradigm. *Theoretical Criminology*. **11**(1), pp.5-37.

Cunningham, P. and Fröschl, F. 2013. *Electronic business revolution: opportunities and challenges in the 21st century*. Springer Science & Business Media.

Cyber Intelligence Company. 2018. Nigerian Confraternities Emerge as Business Email Compromise *Threat' internet fraudsters are run by organised crime syndicates. Crowd strike*

Czuck, A. 2017. *The Evolution of Ransomware on Mobile Devices*.

Debora, D. 2012. Finding high quality in social media. In *International Conference on Web Search and Data Mining.* Calabar: WSDM.

Diep, F. 2017. What Strategies Work Best in Policing. *Pacific Standard*.

Donalds, C. and Osei-Bryson, K.M., 2019. Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior, 92, pp.403-418.

Doppelmayr, A. 2013. *Its' All About Love: Organization, Knowledge Sharing and Innovation Among the Nigerian Yahoo Boys.* Master's thesis.

Dzomira, S. 2014. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*. **4**(2), pp.16-26.

Eboibi, F.E. 2017. A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer law & security review*. **33**(5), pp.700-717.

Ekholm, D. 2013. Research on sport as a means of crime prevention in a Swedish welfare context: A literature review. *Scandinavian Sport Studies Forum*. **4**(1), pp.91-120. Malmö University.

Emelie, c., 2019. Poverty and denial of environmental rights: a focus on the global legal framework. *International review of law and jurisprudence (irlj)*, *1*(1), pp.53-57.

Emerson, R.M., Fretz, R.I. and Shaw, L.L. 2011. *Writing ethnographic fieldnotes*. University of Chicago Press.

Etter, B. 2002, February. The challenges of policing cyberspace. In *Netsafe: Society, Safety, and the Internet Conference.* Auckland, New Zealand, pp. 10-12.

Fafinski, S. and Minassian, N. 2009. UK Cybercrime Report. Available at: http://www.garlik.com/file/cybercrime_report_attachement (Accessed March 29, 2019).

Featherstone, R. and Deflem, M. 2003. Anomie and strain: Context and consequences of Merton's two theories. *Sociological inquiry*. **73**(4), pp.471-489.

Featherstone, R. and Deflem, M. 2003. *Anomie and strain: Merton's two theories*. *Sociological inquiry, 73(4), pp.471-489.*

Federal Bureau of Investigation. 2014. *African Cybercriminal Enterprise Members Using School Impersonation to Defraud Retailers*. Available at: http://www.ic3.gov/media/2014/140904.aspx (accessed March 22, 2019).

Federal Bureau of Investigation. 2015. *Mission Statement*. Available at: https://www.ic3.gov/about/default.aspx (Accessed: March 17, 2019).

Fischer, P., Lea, S.E., and Evans, K.M. 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*. **43**(10), pp.2060-2072.

Florêncio, D. and Herley, C. 2013. Sex, lies, and cyber-crime surveys. In *Economics of information security and privacy III*, pp. 35-53. Springer: New York.

Fobosi, S.C. and Fobosi, S.C. 2019. Original Paper Experience of Negotiating Access in the "Field": Lessons for Future Research. *World*. **6**(4).

Friis, K. and Ringsmose, J. eds., 2016. Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives. Routledge.

Friis, k., Ringsmose, J. Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives. Abingdon: Routledge, 2016, p 225

Geddes, M. and Root, A. 2000. The Modernization and Improvement of Government and Public Services: Social Exclusion—New Language, New Challenges for Local Authorities. *Public Money and Management*. **20**(2), pp.55-60.

Gercke, M., 2012. *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*. International Telecommunication Union.

Giri, B.N., Jyoti, N. and Avert, M. 2006. The emergence of ransomware. *AVAR, Auckland*.

Given, L.M. ed. 2008. *The Sage encyclopedia of qualitative research methods*. Sage publications.

Gottfredson, M. R., & Hirschi, T. 1990. *A general theory of crime.* CA: Stanford University Press, Stanford.

Gottschalk, P. 2010. *Policing Cyber Crime*. Bookboon.

Gravetter, F.J. and Forzano, L.A.B. 2018. *Research methods for the behavioural sciences*. Cengage Learning.

Gravetter, F.J. and Forzano, L.A.B. 2018. *Research methods for the behavioural sciences*. Cengage Learning.

Groothuis, D. 1999. *The soul in cyberspace*. Wipf and Stock Publishers.

Hameed, T. 2007. ICT as an enabler of socio-economic development. (Retrieved June 24, 2007), pp.278-286.

Hancock, B., Ockleford, E. and Windridge, K. 2001. *An introduction to qualitative research*. Trent focuses group.

Haverkamp, B.E. 2005. Ethical perspectives on qualitative research in applied psychology. *Journal of counselling psychology*. **52**(2), pp.146.

Hawes, J. 2013. An epic year for data breaches with over 800 million records lost. *Naked Security*. **19**(1), pp.2014.

Heeks, R. 2017. *Information and communication technology for development (ICT4D)*. Routledge.

Hess, K.M. 2008. *Introduction to private security*. Nelson Education.

Hill, J.B. and Marion, N.E. 2016. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century: Computer Crimes, Laws, and Policing in the 21st Century*. ABC-CLIO.

Hodgson, G.M. 2012. On the limits of rational choice theory. *Economic Thought*. **1**(1).

Hoffman, D.L., Novak, T.P. and Schlosser, A. 2000. The evolution of the digital divide: How gaps in Internet access may impact electronic commerce. *Journal of computer-mediated communication, 5(3), p. JCMC534.*

Holt, T.J., Strumsky, D., Smirnova, O. and Kilger, M. 2012. Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*. **6**(1).

Homans, G.C. 1983. Steps to a theory of social behaviour: an autobiographical account. *Theory and Society*. **12**(1), pp.1-45.

Homans, G.C. 1986. Fifty years of sociology. *Annual Review of Sociology*. **12**(1), pp.xiii-xxx.

Homans, G.C. and Curtis, C.P.,1934. *An introduction to Pareto, his sociology*. Knopf.

Hoofnagle, C.J. 2007. Identity theft: Making the known unknowns known. *Harv. JL and Tech.* **21**(1), pp.97.

Hopkins, M. and Dehghantanha, A. 2015. November. Exploit Kits: The production line of the Cybercrime economy? In *2015 second international conference on Information Security and Cyber Forensics (InfoSec)*, pp. 23-27. IEEE.

How gaps in Internet access may impact electronic commerce. *Journal of computer-mediated communication*. **5**(3), pp.534. Available at: http://www.icnl.org/research/library/files/Nigeria/3_NigeriaCriminalCode1990.pdf (accessed August 2019).

https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html accessed on 20 October 2019.

https://techxplore.com/news/2019-09-fbi-nigeria-step-up-cyber-crime.html access May 2020

https://www.ftc.gov/news-events/press-releases/2020/02/new-ftc-data-show-consumers-reported-losing-more-200-million Accessed 09/07/2020

https://www.pulse.ng/news/metro/yahoo-boy-reportedly-runs-mad-after-using-his-dad-for-rituals-in-benin-video/9pf2vrw.

Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A.C. and McCoy, D., 2018, May. Tracking ransomware end-to-end. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 618-631). IEEE.

Hui, K.L., Kim, S.H. and Wang, Q.H. 2017. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*. **41**(2), pp.497.

Humphrey, J., Mansell, R., Paré, D. and Schmitz, H. 2003. *Reality of e-commerce with developing countries*.

Ibrahim, S. 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*. **47**(1), pp.44-57.

International Telecommunication Union. 2009. *Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Sector*. Available at: https://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-understanding-cybercrime- .pdf

Internet Crime Centre Complaint Centre. 2012. *Internet Crime Report*. Available at: https://pdf.ic3.gov/2012_IC3Report.pdf (Accessed March 29, 2019).

Internet Crime Centre Complaint Centre. 2013. *The Internet Crime Centre Report 2013*. Available at: https://pdf.ic3.gov/2013_IC3Report.pdf (accessed March 27, 2019.).

Internet Crime Centre Complaint Centre. 2014. *The Internet Crime Centre Report 2014*. Available at: https://pdf.ic3.gov/2014_IC3Report.pdf (Accessed April 14, 2019).

Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children, and Internet Chat Services*.

Internet World Stats. 2014. *World Internet Usage and Population Statistics – June 30, 2014 Mid- Year Update*. Available at: http://www.internetworldstats.com/stats.htm (Accessed February 5, 2015).

Ismail, N. 2018. *Global cybercrime economy generates $1.5Trillion*. Available at: https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/ (Accessed 14th September 2019).

Jackson, K.M., Hruska, J. and Parker, D.B. 1992. *Computer security reference book*. CRC Press, Inc.

Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M. and McNamara, J. 2007. December. Security usability principles for vulnerability analysis and risk assessment. In *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, pp. 269-278. IEEE.

Jude, U. 2011. *Nigerian Youths and Internet Exposure*. Onitsha: Sofie Publicity and Printing company.

Kanu, S.I. and Okorafor, E.O. 2013. The nature, extent, and economic impact of fraud on bank deposits in Nigeria. *Interdisciplinary Journal of Contemporary Research in Business*. **4**(9), pp.253-265.

Kaplan, A.M. and Haenlein, M. 2010. Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*. **53**(1), pp.59-68.

Kasali, M.A. and Odetola, R.G. 2016. Alternative Approach to Policing in Nigeria: Analysing the Need to Redefine Community Policing in Tackling the Nation's Security Challenges. *African Journal of Criminology and Justice Studies: AJCJS*. **9**(1), pp.98.

Katyal, N.K. 2001. Criminal law in cyberspace. *University of Pennsylvania Law Review*. **149**(4), pp.1003-1114.

Kaur, N. Prevention and Control of Cyber Crimes. Journal of Computer Science and Engineering, 2016, p 37

Kawulich, B.B. 2005, May. Participant observation as a data collection method. In *Forum qualitative sozialforschung/forum: Qualitative social research.* **6(**2).

Keel, R. 2005. Rational choice and deterrence theory: Sociology of deviant behaviour. *Sociology*, pp.111-118.

Khadam, N. 2012. Insight to Cybercrime. *Justice Yatindra Singh*.

Kiser, E. and Hechter, M. 1998. The debate on historical sociology: Rational choice theory and its critics. *American Journal of Sociology*. **104**(3), pp.785-816.

Kitchin, R. and Tate, N. 2013. *Conducting research in human geography: theory, methodology and practice*. Routledge.

Koops, B.J. and Leenes, R. 2006. Identity theft, identity fraud and/or identity-related crime. *Datenschutz und Datensicherheit-DuD*. **30**(9), pp.553-556.

KPMG. 2001. *Global e-fraud Survey, KPMG Forensic and Litigation Services*. Available at: https://home.kpmg.com/xx/en/home/services/advisory/riskconsulting/forensic.html

Kshetri, N. 2006. The simple economics of cybercrimes. *IEEE Security & Privacy*. **4**(1), pp.33-39.

Kshetri, N. 2010. The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures. In *The Global Cybercrime Industry*, pp. 1-34. Springer, Berlin, Heidelberg.

Kshetri, N. 2010. *The global cybercrime industry: economic, institutional, and strategic perspectives*. Springer Science & Business Media.

Kshetri, N. 2013. Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. *Crime, law, and social change*. **60**(1), pp.39-65.

Kshetri, N. 2013. *Cybercrime and cybersecurity in the global south*. Springer.

Kshetri, N. and Voas, J. 2017. Do crypto-currencies fuel ransomware? *IT professional*. **19**(5), pp.11-15.

Kumar, K. 2003. *Cyber laws, international property, and e-commerce security*.

Landoll, R.R., La Greca, A.M., Lai, B.S., Chan, S.F., and Herge, W.M. 2015. Cyber victimization by peers: Prospective associations with adolescent social anxiety and depressive symptoms. *Journal of adolescence*. **42**(1), pp.77-86.

Lawani, C. and Osagie-Obaz, G. 2019. Alarming Rate of "Yahoo plus" and Human Insecurity Dilemma in Nigeria: Implication for Counselling. *European Scientific Journal.* **15**(13).

Lee, B.X. 2016. Causes and cures V: The sociology and anthropology of violence. *Aggression and violent behaviour*. **27**(1), pp.158-163.

Lee, K.R. 2002. Impacts of Information Technology on Society in the new Century. *Konsbruck Robert Lee. Route de Chavannes C*, pp.*27*.

Levin, J. and Milgrom, P. 2004. Introduction to choose theory. Available at: http://web. stanford. edu/~ jdlevin/Econ, pp.*20202*.

Lewis, J. and Baker, S. 2013. *The economic impact of cybercrime and cyber espionage*. McAfee.

Lewis, J.L. & S.R.J. Sheppard. 2006. Culture and communication: can landscape visualization improve forest management consultation with indigenous communities? Landscape and Urban Planning 77:291–313.

Lewis, S. 2015. Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*. **16**(4), pp.473-475.

Li, X. 2008. *Cybercrime and deterrence: networking legal systems in the networked information society* (Doctoral dissertation, Turun yliopisto oikeustieteellinen tiedekunta).

Liamputtong, P. and Ezzy, D. 2005. *Qualitative research methods. Second*. Melbourne: Oxford university press.

Lincoln, Y. S. & Guba, E. G. 1985. *Naturalistic Inquiry*. Newbury Park, CA: Sage Publications.

Lincoln, Y.S. 2001. Varieties of validity: Quality in qualitative research. *HIGHER EDUCATION-NEW YORK-AGATHON PRESS INCORPORATED*. **16**(1), pp.25-72.

Lincoln, Y.S. and Denzin, N.K. 2003. *Turning points in qualitative research: Tying knots in a handkerchief,* Vol. 2. Rowman Altamira.

Lindseth, A. and Norberg, A. 2004. A phenomenological hermeneutical method for researching lived experience. *Scandinavian journal of caring sciences*. **18**(2), pp.145-153.

Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L. 2009. Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives. *Journal of Information Technology Impact*. **9**(3), pp.155-172.

Macionis, J. 2012. *"Sociology" Kenyon College*. Boston: Pearson, Print.

Maghaireh, A.M.S. 2009. Jordanian cybercrime investigations: *a comparative analysis of search for and seizure of digital evidence.*

Mason, G. and Wilson, P.R. 1988. *Sport, recreation, and juvenile crime: An assessment of the impact of sport and recreation upon Aboriginal and non-Aboriginal youth offenders*. Canberra: Australian Institute of Criminology.

Mason, M. 2010. August. Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research.* 11(3).

Mathew, A.R., Al Hajj, A. and Al Ruqeishi, K. 2010. Cybercrimes: Threats and protection. In *2010 International Conference on Networking and Information Technology,* pp. 16-18. IEEE.

Mathiesen, T. 1990. Prison on Trial: *A critical assessment.* London: Sage Publications.

Matusitz, J.A. 2006. *Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them* (Doctoral dissertation).

Mbiti, J.S. 1990. *African religions & philosophy*. Heinemann.

Mbiti, J.S. 1991. *African Religions and Philosophy*. New Hampshire.

McConnell International. 2000. *Cyber Crime… and Punishment? Archaic Laws Threaten Global Information*.

McFayden, E. 2010. *Global Implications of White-Collar Crime*. Available at: SSRN 1530685.

McGuire, M. 2018. Into the web of profit: Understanding the growth of the cybercrime economy. *Bromium Report*.

McGuire, M. and Dowling, S. 2013. *Cybercrime: A review of the evidence–Summary of key findings and implications– Home Office Research Report 75*. Available at: https://www.
gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary. Pdf (Accessed on November, 2014).

Melugbo, D.U., Ogbuakanne, M.U. and Jemisenia, J.O. 2020. Entrepreneurial potential self-assessment in times of COVID-19: Assessing readiness, engagement, motivations, and limitations among young adults in Nigeria. *Ianna Journal of Interdisciplinary Studies ISSN (Print) 2735-9883; ISSN (Online) 2735-9891*, **2**(1).

Merton, Robert K. 1938. Social Structure and Anomie, American Sociological Review. **3**(1), pp.672-682.

Miles, M.B. and Huberman, A.M. 1984. Drawing valid meaning from qualitative data: Toward a shared craft. *Educational researcher*. **13**(5), pp.20-30.

Miquelon-Weismann, M.F. 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process, 23 J. Marshall J. Computer & Info. L. 329 (2005). *The John Marshall Journal of Information Technology & Privacy Law*. **23**(2), pp.4.

Monsurat, I., 2020. African Insurance (Spiritualism) and the Success Rate of Cybercriminals in Nigeria: A Study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*. **14**(1), pp.300-315.

Mosco, V., 2005. *The digital sublime: Myth, power, and cyberspace*. Mit Press.

Msigwa, R. and Kipesha, E.F. 2013. *Determinants of youth unemployment in developing countries: Evidences from Tanzania*.

Muhammed, A and Tersur, M. 2013. Youth Empowerment And National Development in Nigeria. *International Journal of Business and Management Invention*. **10**(2), pp.785-797.

National youth Policy of Nigeria, Abuja. 2001. http://www.africanchildforum.org/clr/policy%20per%20country/nigeria/nigeria_youth_2002_en.pdf.

Nicholas CAMQC. 2008. *Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities, International Association of Prosecutors, Singapore*. Available at: http://www.odpp.nsw.gov.au/docs/defaultsource/speechesbynicholascowdery/emerging-trends-in-cyber-crime.pdf?sfvrsn=2

Nichols, G. and Taylor, P. 1996. *West Yorkshire Sports Counselling: Final Evaluation Report*. Halifax: West Yorkshire Sports Counselling Association.

Nkamnebe, A.D., 2014. Africa's retailing environment. *The Routledge companion to business in Africa*, p.70.

Nolte, I. 2007. Ethnic vigilantes and the state: the Oodua People's Congress in south-western Nigeria. *International Relations*, **21**(2), pp.217-235.

Nugroho, Y. 2008. Adopting Technology, Transforming Society: The Internet and the Reshaping of Civil Society Activism in Indonesia. *International Journal of Emerging Technologies & Society*. **6**(2).

O'Connor, B. 2018. *Cybercrime: $1.5 Trillion problem*. Retrieved from: https://www.experian.com/blogs/ask-experian/cybercrime-the-1-5-trillion-problem/ (accessed 14th September 2019).

Ogbuoshi, L.I. 2006. *Understanding Research Methods and Thesis Writing*. Enugu: Linco Enterprises.

O'Gorman, G. and McDonald, G., 2012. Ransomware: A growing menace. Arizona, AZ, USA: Symantec Corporation.

Ogwezzy, M.C. 2012. *Cybercrime and the proliferation of yahoo addicts in Nigeria*. AGORA International Journal of Juridical Science, 86e102.

Ojedokun, U.A. and Eraye, M.C. 2012. Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*. **6**(2), pp.1001.

Oke, O. 2015. *An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention Etc) Act, 2015*. Available at: SSRN 2655593.

Okeshola, F.B. and Adeta, A.K. 2013. The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*. **3**(9), pp.98-114.

Okeshola, F.B. and Adeta, A.K. 2013. The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*. **3**(9), pp.98-114.

Okochu, E**.** 2017. *Cybercrime: The World's New Social Problem.*

Olaide, J. and Adewole, O., 2004. *Cyber Crime Embarrassing for Victims*. Available at: http//www.heraldsun.com.au (Retrieved September 2011).

Olowu, D. 2009. Cyber-crimes and the boundaries of domestic legal responses: Case for an inclusionary framework for Africa. *Journal of Information, Law and Technology*. **1**(1), pp.1-18.

Olugbodi, K. 2010. *Fighting Cyber Crime in Nigeria*. (Accessed April 21, 2019).

Ormston, R., Spencer, L., Barnard, M. and Snape, D. 2014. The foundations of qualitative research. *Qualitative research practice: A guide for social science students and researchers*. **2**(1), pp.52-55.

Osalor, P. 2014. Breaking the Nigerian Poverty Cycle through Entrepreneurial Revolution Part I. *Vanguard Newspaper*. Monday, March 31, pp.18.

Osumah, O. and Aghedo, I. 2011. Who wants to be a millionaire? Nigerian youths and the commodification of kidnapping. *Review of African Political Economy*, **38**(128), pp.277-287.

Oxford Dictionary of Law. 2002. *Oxford Dictionary of Law*. 5th Edition, pp.132, 149. Available at: http://www.fd.unl.pt/docentes_docs/ma/wks_MA_21613.pdf

Oyewole and Obeta. 2002. *An Introduction to Cyber Crime*. Available at: http//www.crimeresearch.org/articules/cyber-crime (Retrieved September 2011).

Paganini, P. 2013. *InfoSec Institute 2013 Cost of cybercrimes.* Available at: http://resources.infosecinstitute.com/cybercrime-and-theunderground-market/

Paquet-Clouston, M., Haslhofer, B. and Dupont, B., 2019. Ransomware payments in the bitcoin ecosystem. Journal of Cybersecurity, 5(1), p.tyz003

Parker, D.B. 1976. The Future of Computer Abuse. *Proceedings of Man and the Computer S ymposium*, pp.59-68.

Parnaby, P.F. and Sacco, V.F. 2004. Fame and strain: the contributions of mertonian deviance theory to an understanding of the relationship between celebrity and deviant behavior. *Deviant Behavior*. **25**(1), pp.1-26.

PAT 10. 1999. *Policy Action Team 10: A Report to the Social Exclusion Unit: Arts and Sport*. London: DCMS.

Patton, M.Q. 2002. Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*. **1**(3), pp.261-283.

Petersen, R.D. and Valdez, A., 2005. Using snowball-based methods in hidden populations to generate a randomized community sample of gang-affiliated adolescents. Youth violence and juvenile justice, 3(2), pp.151-167.

Popli, N.K. and Girdhar, A. 2019. Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In *Computational Intelligence: Theories, Applications and Future Directions-Volume II*, pp. 65-80. Springer, Singapore.

Qu, S.Q. and Dumay, J. 2011. The qualitative research interviews. *Qualitative research in accounting and management*, Vol 8 (3)

Quarshie, H.O. and Martin-Odoom, A. 2012. Fighting cybercrime in Africa. *Computer Science and Engineering*. **2**(6), pp.98-100.

Radwan, I. and Pellegrini, G. 2010. *Knowledge, productivity, and innovation in Nigeria: Creating a new economy*. The World Bank.

Ramzan, Zulfikar 2010. Phishing attacks and countermeasures. In Stamp, M. and Stavroulakis, P., *Handbook of Information and Communication Security*. Springer. ISBN 978-3-642-04117-4.

Ribadu, E. 2007. *Cyber Crime and Commercial Fraud; A Nigerian Perspective*. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R. 2013. *Qualitative research practice: A guide for social science students and researchers*. Sage.

Robins, D. 1990. Sport as Prevention: The Role of Sport in Crime Prevention Programmes Aimed at Young People, Occasional paper 12. *Centre for Criminological Research. Oxford: University of Oxford.*

Rosewarne L. 2017. "Nothing crueler than high school students": The cyberbully in film and television. *International Journal of Technoethics*. **8**(1), pp.1-17.

Rubin, H.J. and Rubin, I.S., 2011. *Qualitative interviewing: The art of hearing data*. sage.

Rutger Leukfeldt (editor). 2017. *Research agenda the human factor in cybercrime and cyber security eleven international publishing.*

Ruwan, I.I.F., Garba, M.Y., Ishaya, D.S. and Godiya, A. 2020. An assessment of violent crimes: armed robbery and murder in Lagos State, Nigeria from 2015-2019. *KIU Journal of Humanities*. **5**(2), pp.169-176.

Sadler, G.R., Lee, H.C., Lim, R.S.H. and Fullerton, J. 2010. Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & health sciences*. ***12***(3), pp.369-374.

Satz, D. and Ferejohn, J. 1994. Rational choice and social theory. *The Journal of philosophy*. **91**(2), pp.71-87.

Saunders, M.N., Lewis, P., Thornhill, A. and Bristow, A. 2015. *Understanding research philosophy and approaches to theory development*.

Schmidt, E. and Cohen, J. 2013. *The new digital age: Reshaping the future of people, nations, and business*. Hachette UK.

Sekaran, U. and Bougie, R. 2016. *Research methods for business: A skill building approach*. John Wiley & Sons.

Seodotcom. 2011. *The History of Search (infographic)*. Available at: http://www./rb.co.uk/v33n24/steven-shapin/an-example-of-the-good-life (Retrieved May 13, 2013)

Shank, S. 2011. Cybersecurity: Domestic and legislative issues. *American University National Security Law Brief*. **1**(1), pp.8.

Shinder, D. 2011. *Online Anonymity: Balancing the Needs to Protect Privacy and Prevent Cybercrime*. Available at: http://www.techrepublic.com/blog/it-security/online-anonymity-balancing-the-needs-to-protect-privacy-and-prevent-cybercrime/

Shinder, D.L. 2002. *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Publishing Inc., USA.

Sieber, U. 1997. *Memorandum on a European Model Penal Code*. pp.2.

Simon, M. and Goes, J. 2016. *Reliability and validity in qualitative studies*. Accessed on dissertationrecipes.com .

Slater, J. 2018. *India is no longer home to the largest number of poor people in the world, Nigeria is*. Washington Post, pp.10.

Spitzberg, B. H., and Hoobler, G. 2002. *Cyberstalking and the technologies of interpersonal terrorism*. New Media & Society. **4**(1), pp.71-92.

Spruit, A. 2017. *Keeping youth in play: The effects of sports-based interventions in the prevention of juvenile delinquency*. Universiteit van Amsterdam.

Steve Morgan, Editor-in-Chief. 2017. *Cybercrime Report on Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021*. Herjavec Group CybersecurityVentures.

Sukarieh, M. and Tannock, S. 2014. *Youth rising? The politics of youth in the global economy*. Routledge.

Symantec Corporation. 2012. *Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually*. September 5, 2012. Symantec. Available at: http://www.symantec.com/about/news/release/article.jsp?prid= 20120905_02 (Accessed March 21, 2019).

Tade, O. 2013. A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*. **23**(4), pp.689-705.

Tade, O. and Aliyu, I. 2011. Social organization of internet fraud among university undergraduates in Nigeria. *Int. J. Cyber Criminol*. **5**(2), 860e875.

Tambe, E., Alain, C., and Mikko, S. 2014. *Toward a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective.*

Tan, Koontorm Center. 2006. "Phishing and Spamming via IM (SPIM)". (Retrieved December 5, 2006).

Tapsoba, K., 2018. *Ransomware: Offensive Warfare Using Cryptography as a Weapon* (Doctoral dissertation, Utica College).

Taylor, P., Crow, I., Nichols, G. and Irvine, D. 1999. *Demanding Physical activity Programmes for Young Offenders under Probation Supervision*. London: The Home Office.

Taylor, R., Caeti, T., Loper, K., Fritsch, E., & Liederbach, J. 2006. *Digital crime and digital terrorism: Chapter 3 - The Criminology of Computer Crime*. Pearson/Prentice Hall.

The conversation. 2016. *Social media and crime: the good, the bad and the ugly*. The Conversation Africa, Inc.

Times, P. 2019. *Nigeria's unemployment rate hits 33.5 per cent by 2020-minister*.

Transparency International. 2014. *The 2014 Corruption Perception Index*. Available at: http://www.transparency.org/cpi2014. accessed 30.12.15.

Treviño, A. Javier. 2009. '*George C. Homans, the human group and elementary social behaviour', the encyclopaedia of informal education*. Available at: www.infed.org/thinkers/george_homans.htm

Udeh, C.S. 2008. *Youth Unemployment and Poverty in Nigeria: implication for National Security*. A paper presented at the international conference on Nigeria youth political participation and national development organized by CDRT, Bayero University, Kano.

Umejiaku, N.O. and Anyaegbu, M.I. 2016. LEGAL FRAMEWORK FOR THE ENFORCEMENT OF CYBER LAW AND CYBER ETHICS IN NIGERIA. *International Journal of Computer & Technology*. **15**(1), pp.7130-7139.

United nation world youth report. 2007. Available at: http:www.un.org

United Nations Office on Drugs and Crime. 2013. *Comprehensive Study on Cybercrime*. Report prepared for the Open-Ended Intergovernmental Expert Group on Cybercrime. New York: United Nations. Available at: https://www.unodc.org/documents/organizedcrime/ UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. (Retrieved on 26th February 2015).

United Nations Office on Drugs and Crime. 2013. *Comprehensive Study on Cybercrime. Report prepared for the Open-Ended Intergovernmental Expert Group on Cybercrime*. New York: United Nations. Available at: https://www.unodc.org/documents/organizedcrime/ UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. (Retrieved on 26th February 2015)

United Nations Office on Drugs and Crime. 2014. *United Nations Convention Against Corruption*. Available at: https://www.unodc.org/documents/brussels/UN_Convention_Against _Corruption.pdf.

Uniterd Nation Human Right. 2005. *Ratification of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*. Available at: http://www.ohchr.org/en/hrbodies/cat/pages/catindex.aspx

Uniterd Nations Educational Scientific and Cultural Organization. 1954. *Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention 1954*. The Hague, 14 May 1954. Available at: http://portal.unesco.org/en/ev.phpURL_ID=13637&URL_DO=DO_TOPIC&URL_SECTION=201.html

Van de Weijer, S.G., Leukfeldt, R. and Bernasco, W. 2019. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*. **16**(4), pp.486-508.

Van der Merwe, A J, Loock, M, Dabrowski, M. 2005. *Characteristics and Responsibilities involved in a Phishing Attack*. Winter International Symposium on Information and Communication Technologies: Cape Town.

Van Manen, M., 2016. Phenomenology of practice: Meaning-giving methods in phenomenological research and writing. Routledge.

Vandebosch, H. and Van Cleemput, K. 2009. Cyberbullying among youngsters: Profiles of bullies and victims. *New media & society*. **11**(8), pp.1349-1371.

Viano, E.C. 2017. Cybercrime: Definition, Typology, and Criminalization. In *Cybercrime, Organized Crime, and Societal Responses*, pp. 3-22. Springer, Cham.

Von Lampe, K. 2015. *Organized crime: analysing illegal activities, criminal structures, and extra-legal governance*. Sage Publications.

Wall, D. 2007. Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police, Practice and Research: An International Journal*. **8**(2), pp.183- 205.

Wall, D. 2007. *Cybercrime: The transformation of crime in the information age*, Vol. 4. Polity.

Wall, D.S. 2011. Micro-frauds: virtual robberies, stings, and scams in the information age. In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 68-86). IGI Global.

Wall, David, S. 2009. The role of the media in generating insecurities and influencing perceptions of cybercrime. InMeško, G., Cockcroft, T., Crawford, A., and Lemaitre, A. (Eds.). *Crime, Media, and Fear of Crime*. Ljubljana: Tipografija.

Warner, J. 2011. Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*. **5**(1), pp.736.

Whitaker, R. 2013. *Proto-Spam: Spanish prisoners and confidence games*. Appendix **1**(4). Available at: http://theappendix.net/issues/2013/10/proto-spamspanish- prisoners-and-confidence-games (accessed April 12, 2019).

White, P. C. 2004. *Crime Scene to Court: The Essentials of Forensic Science*. 2nd Edition.

Whitty, M.T. and Buchanan, T. 2012. The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*. **15**(3), pp.181-183.

Whitty, M.T. and Ng, M. 2017. Literature Review for underware: Understanding West African culture to prevent cybercrimes. Report for the National Cyber Security Centre as part of a group of studies funded in the *Research Institute in Science of Cyber Security.*

Williams, P. and Fiddner, D. 2016. *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*. Army War College-Strategic Studies Institute: Carlisle, United States.

Willis, P., 2014. The scholarly and pathic cavalier: Max Van Manen's phenomenology of practice. Phenomenology & Practice, 8(2), pp.64-69.

Witt, P. and Crompton, J. 1996. *Recreation Programs that Work for At-risk Youth*. Pennsylvania: Venture Publishing.

World Bank. 2012. *Internet users*. Available at: http://data.worldbank.org/indicator/IT.NET.USER/countries.

Yar, M., Jewkes, Y. 2010. *Histories and Contexts. Handbook of Internet Crime*. Routledge Books, London.

Yazan, B. 2015. Three approaches to case study methods in education: Yin, Merriam, and Stake. *The qualitative report*. **20**(2), pp.134-152.

Yazdanifard, R., Oyegoke, T. and Seyedi, A.P., 2011. Cyber-crimes: Challenges of the millennium age. In *Advances in Electrical Engineering and Electrical Machines* (pp. 527-534). Springer, Berlin, Heidelberg.

Zakariyya A., 2018. How yahoo-yahoo boys scam their victims – Experts. Agency reports

Zebel, Z., de Vries, P., Giebels E., WouterStol, M. 2013. *Youthful offenders of cybercrime in the Netherlands: An empirical exploration, Research carried out for the WODC, Commissioning Research Division, Ministry of Security and Justice*. WODC, Ministry of Security and Justice, Copyright reserved.

Zembroski, D., 2011. Sociological theories of crime and delinquency. Journal of Human Behavior in the Social Environment, 21(3), pp.240-254.

Zero Tolerance. 2006. Retiree in Trouble over Internet Fraud. *Economic and Financial Crime Commission*. **1**(1).

APPENDIX 1- ETHICAL CLEARANCE LETTER

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

27 March 2019

Mr Tolulope L Ojolo 215080532
School of Applied Human Sciences
Howard Colledge Campus

Dear Mr Ojolo

Protocol reference number: HSS/1686/018D
Project title: A criminological investigation of the Lived experiences of Cybercrime Perpetrators in South West Nigeria.

Full Approval – Full Committee Reviewed Application

With regards to your response received on 28 February 2019 to our letter of 07 November 2019, the Humanities and Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. Please note: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereaf[redacted]n must be applied for on an annual basis.

I take th[redacted] wishing you everything of the best with your study.

Yours fa[redacted]

.....
Dr Shamila Naidoo (Deputy Chair)

/px

cc Supervisor: Dr Sazelo Mkhize
cc Academic Leader Research: Dr Maud Mthembu
cc School Administrator: Ms Ayanda Ntuli

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

APPENDIX 2- GATEKEEPERS LETTER ADO-EKITI

ADO-EKITI LOCAL GOVERNMENT

Ado-Ekiti Local Government

Your Ref No.....

Further communications should be addressed to the Chairman

Local Government Secretariat
P. M. B. 5313,
Ado-Ekiti,
Ekiti State.

Our Ref No. AELG/172/222/05

Date. 25th October, 2018

Mr. Tolulope Lembola Ojolo,
Department of Criminology,
University of Kwazulu-Natal,
Durban, South Africa.

Dear Mr. Ojolo,

RE: REQUEST FOR GATEKEEPER'S LETTER

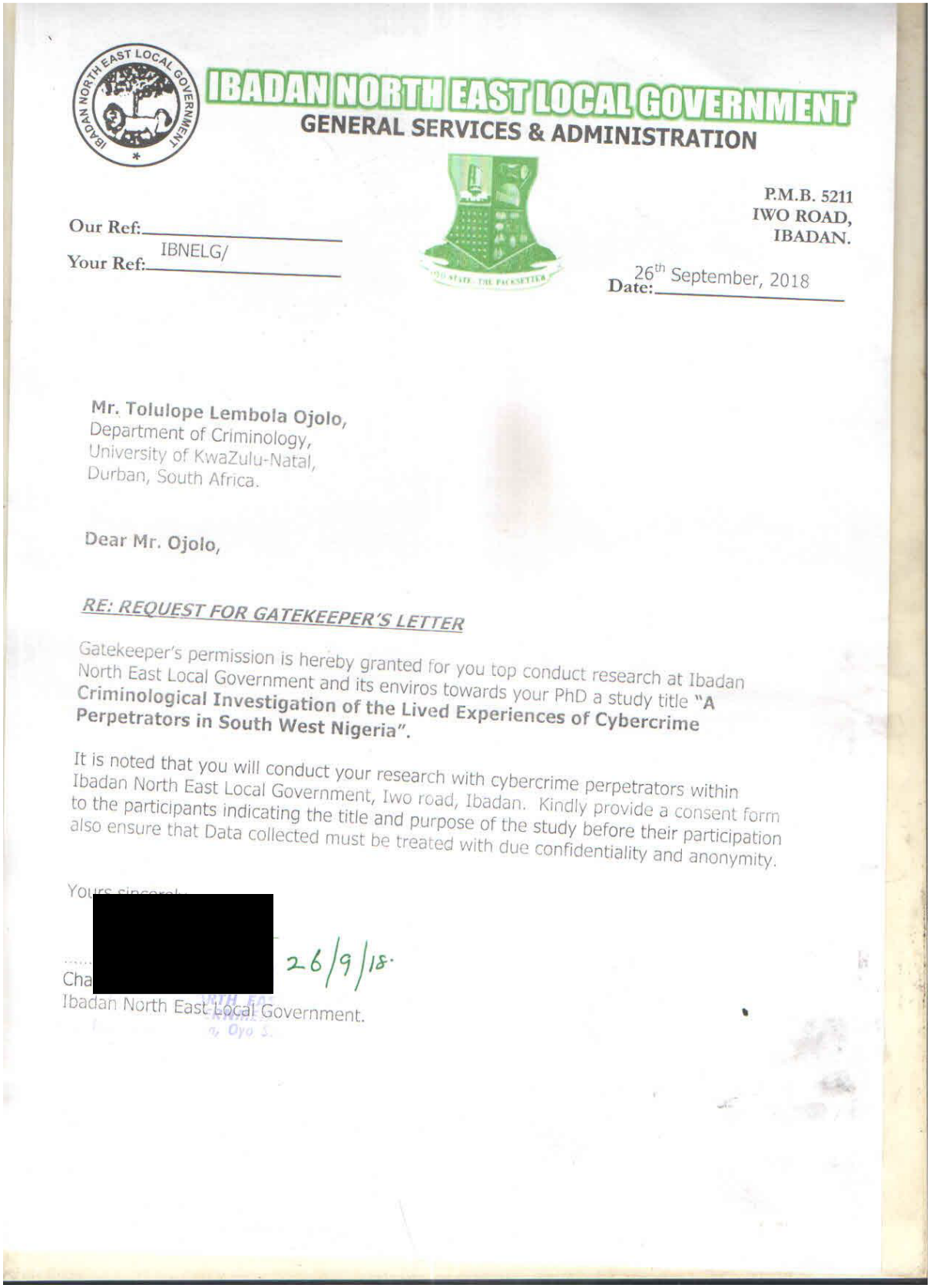
Gatekeeper's permission is hereby granted for you to conduct research at Ado-Ekiti Local Government and its enviros towards your PhD as study titled "A **Criminological of the Lived Experiences of Cybercrime Perpetrators in South West Nigeria".**

It is noted that you will conduct your research with cybercrime perpetrators. Kindly provide a consent form to the participants indicating the title and purpose of the study before their participation. Also ensure that Data collected must be treated with due confidentially and anonymity.

Yours Sincerely,

Ak
Fo

APPENDIX 3- GATEKEEPERS LETTER IBADAN



IBADAN NORTH EAST LOCAL GOVERNMENT
GENERAL SERVICES & ADMINISTRATION

P.M.B. 5211
IWO ROAD,
IBADAN.

Our Ref: _____
Your Ref: IBNELG/

Date: 26th September, 2018

Mr. Tolulope Lembola Ojolo,
Department of Criminology,
University of KwaZulu-Natal,
Durban, South Africa.

Dear Mr. Ojolo,

RE: REQUEST FOR GATEKEEPER'S LETTER

Gatekeeper's permission is hereby granted for you top conduct research at Ibadan North East Local Government and its enviros towards your PhD a study title **"A Criminological Investigation of the Lived Experiences of Cybercrime Perpetrators in South West Nigeria".**

It is noted that you will conduct your research with cybercrime perpetrators within Ibadan North East Local Government, Iwo road, Ibadan. Kindly provide a consent form to the participants indicating the title and purpose of the study before their participation also ensure that Data collected must be treated with due confidentiality and anonymity.

Yours sincerely,

[redacted] 26/9/18.

Cha
Ibadan North East Local Government.

APPENDIX 4- INFORM CONSENT FOR PARTICIPANTS

School of Applied Human Sciences,

University of KwaZulu-Natal,

Howard College Campus,

Dear Participant

INFORMED CONSENT LETTER

My name is Mr Tolulope Lembola Ojolo. I am a PhD candidate studying at the University of KwaZulu-Natal, Howard College campus, South Africa. I am currently conducting a research study titled: **"A Criminological Investigation of the Lived Experiences of Cybercrime Perpetrators in South West Nigeria"** This study examines the lived experiences of cybercrime perpetrators in South West Nigeria. The aim of the study is to engage with forty cybercrime perpetrators to unveil from their perspectives, in-depth information about the circumstances that has driven them into committing crime. To gather the information, I am interested in asking you some questions.

Please note that:

- Your confidentiality is guaranteed as your inputs will not be attributed to you in person, but reported only as a population member opinion.
- The interview may last for about 1 hour and may be split depending on your preference.
- Any information given by you cannot be used against you, and the collected data will be used for purposes of this research only.
- Data will be stored in secure storage and destroyed after 5 years.
- You have a choice to participate, not participate or stop participating in the research. You will not be penalized for taking such an action.
- Your involvement is purely for academic purposes only, and there are no financial benefits involved.
- If you are willing to be interviewed, please indicate (by ticking as applicable) whether or not you are willing to allow the interview to be recorded by the following equipment:

I can be contacted at:

Email: ojolotolulope@yahoo.com

Cell: +27631379699

My supervisor is Dr. S Mkhize who is located at the School of Applied Human Sciences, Criminology Department, Howard College campus of the University of KwaZulu-Natal.

Contact details: email: mkhizes1@ukzn.ac.za Phone number: 0312601773.

You may also contact the Research Office through:

P. Mohun HSSREC Research Office,

Tel: 031 260 4557 E-mail: mohunp@ukzn.ac.za

Thank you for your contribution to this research.

APPENDIX 5- INTERVIEW GUIDE

INTERVIEW SCHEDULE:

"A Criminological Investigation of the Lived Experiences of Cybercrime Perpetrators in South West Nigeria."

BIOGRAPHICAL INFORMATION

1. Name?
2. Recommended pseudo name?
3. Age?
4. Gender?
5. Marital status?

CYBERCRIME RELATED QUESTIONS

6 Can you please tell me more about you more you (Who are you are)? I want to get to know you generally

7 Can you narrate the circumstances that motivated your involvement in cybercrime?

8 How can you describe the learning process of cybercrime in Nigeria?

9 What type of cybercrime are you engaged with?

10 What has been your achievements since your involvement in cybercrime?

11 What is the general description of a typical cybercrime perpetrator in Nigeria?

12 How are you being perceive by your family members?

13 Do you think this act of cybercrime is at getting back at colonial masters?

14 Are you proud of being a cybercrime perpetrator? If yes or no, Why?

15 Will you consider cybercrime as a social problem in Nigeria?

16 What is your perception on the victims of romance scam?

17 What are your long term plans? Do you think of quitting at some point?

MECHANISMS PUT IN PLACE BY THE GOVERNMENT AND CYBERCRIME

18 Do you think there are effective mechanisms by the government to curb cybercrime? If yes, how have you navigated these mechanisms?

19 In your opinion what are the long-lasting mechanisms that can deter youth from yahoo-yahoo.

20 Have you had any encounter with the police?

21 How do you think high profile cybercrime cases in Nigeria has been treated and does it affect your continuous involvement?

THANK YOU

APPENDIX 6 -LETTER CONFIRMING EDITING

Barbara Dupont Language School

37A Hilltop Road
Hillcrest
3610
Cell No: 0846668351

19th December 2020

To Whom It May Concern

EDITING OF ACADEMIC DISSERTATION

I hereby confirm that I, Barbara Dupont, edited the thesis written by **Tolulope Lembola Ojolo** titled '**A Criminological Investigation into the Lived Experiences of Cybercrime Perpetrators in South West Nigeria**' and commented on the grammatical anomalies in MS Word Track Changes and review mode by the insertion of comment balloons prior to returning the document to the authors. Corrections were made in respect of grammar, punctuation, spelling, syntax, tense and language usage as well as to sense and flow. Reference guidelines and additional comments were provided to assist with corrections. No actual content was altered, suggestions for amendments were made where deemed necessary.

I have a been teaching English for the past 12 years and have a Cambridge CELTA diploma in teaching English as a foreign language. I am also employed by the British Council as an official IELTS examiner for Southern Africa. I have been editing academic and other documents for the past four years, regularly editing the research dissertations, articles and theses of the School of Nursing, Environmental Studies and various other schools and disciplines at the University of KwaZulu-Natal and other institutions, as well as editing for publishing firms and private individuals on a contract basis.

I trust that this document will prove acceptable in terms of editing criteria.

Yours faithfully
B Dupont
Barbara Dupont

Address: 37a Hilltop Road, Hillcrest, 3610
Contact Number: 0846668351