INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY

MUKTAR BELLO

Ph.D. Thesis **2018**

INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY

MUKTAR BELLO

Salford Business School
College of Business and Law
University of Salford, UK.

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE DEGREE OF DOCTOR OF PHILOSOPHY, JUNE, 2018

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENT

I owe my deepest gratitude to the Almighty Allah for His Infinite Wisdom and Mercy in allowing me to successfully finish my Ph.D. Programme. The project would not have been possible without the assistance, mentorship and guidance of my supervisor Dr. Marie Griffiths, I am most grateful for her support.

This thesis was made possible with the sponsorship and support of Petroleum Technology Development Fund (PTDF) throughout the duration of my studies.

I am indebted to my wife, Dr. Farida and our lovely daughters Iman and Anisa for their patience, love and understanding. I am grateful to my father, Dr. Bello Lafiaji (fwc) OFR and my mother Mrs. Maryam Bello for their continued love, dedication and prayers. To my father in law, Dr. Muazu Babangida Aliyu and my mother in law, Mrs. Jummai Aliyu I am forever grateful to your mentorship, support and prayers.

To my Aunt, Hajiya Larai Musa Abubakar, I am immensely grateful for your support. To my brothers and sisters I am grateful for your prayers and support. Also, gratitude to my Uncles; Alh. Alkassim Umar, Alh. Mohammad Aliyu (Ciroma) and Baba Bashir.

I would like to thank the Former President and Commander in Chief of the Armed Forces, General Ibrahim B. Babangida for his kind assistance, advice and mentorship over the years. I am most grateful sir. Also, I want to appreciate the kind gesture, prayers and encouragement from Mallam Ahmed Dasuki for his good heart and generous contribution.

Finally, I would like to thank all my friends that have over the years being patient with me and supported me one way or the other, I am indebted to you all.

DEDICATION

To My Parents

To My Wife

To My Daughters

DECLARATION

This project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet, etc) has been acknowledged within the main report to an entry in the References list.

ABBREVIATIONS

ABBREVIATION	FULL MEANING
ACPO	Association of Chief of Police Officers
AFF	Advance Fee Fraud
AU	African Union
ATCON	Association of Cyber Cafe and Telecentre Owners
ATM	Automated Teller Machine
BOFIA	Bank and Other Financial Malpractices in Bank Act
CAC	Cybercrime Advisory Council
CBN	Central Bank of Nigeria
CCB	Code of Conduct Bureau
CCT	Code of Conduct Tribunal
CD	Compact Disk
CERT	Computer Emergency Response Team
CFIN	Computer Forensic Institute, Nigeria
CI	Critical Infrastructure
CMA	Computer Misuse Act
COE	Council of Europe
CTR	Customer Transaction Records
DSS	Department of State Services
EC	European Council
ECOWAS	Economic Community of West African States
EU	European Union
EFCC	Economic and Financial Crimes Commission
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FGN	Federal Government of Nigeria
FHC	Federal High Court
FMoJ	Federal Ministry of Justice
GCFR	Grand Commander of the Federal Republic
GMP	Greater Manchester Police
GSM	Global System for Mobile Communications
HOR	House of Representative
IC3	Internet Crime Complaint Centre
ICPC	Independent Corrupt Practices and other Related Offences Commission
ICT	Information and Communication Technology
ISP	Internet Service Providers
ISPAN	Internet Service Providers' Association of Nige
INTERPOL	International Police
ITU	International Telecommunication Union
LEA	Law Enforcement Agencies
MDA	Ministries, Departments, and Agencies
MLA	Money Laundering Act
MLAT	Mutual Legal Agreement Treaty
MNO	Mobile Network Operator
MOJ	Ministry of Justice
MOU	Memorandum of Understanding
MPCCU	Metropolitan Police Cyber Crime Unit
NBS	National Bureau of Statistics
NCA	National Crime Agency
NCC	Nigerian Communications Commission
NCCU	National Cyber Crime Unit

ABBREVIATION	FULL MEANING
NCS	Nigerian Computer Society
NCSS	National Cyber Security Strategy
NCWG	Nigerian Cybercrime Working Group
NFIU	Nigerian Financial Intelligence Unit
NGCERT	Nigerian Computer Emergency Response Team
NIA	National Intelligence Agency
NIG	Nigerian Internet Group
NITDA	National Information Technology Development Agency
NPF	Nigerian Police Force
NSA	National Security Advisor
OBJ	Objective
ONSA	Office of the National Security Advisor
POS	Point of Sale
RCCU	Regional Cyber Crime Unit
RQ	Research Question
SBS	Salford Business School
SMART	Simple, Moral, Accountable, Responsive, Transparent
SMTP	Simple Mail Transfer Protocol
SOCA	Serious Organized Crime Agency
TCP	Transaction Clearing Platform
UK	United Kingdom
UNCAC	United Nations Convention Against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organised Crime
USA	United States of America
USSS	United States Secret Services
UoS	University of Salford
WITFOR	World Information Technology Forum
WYP	West Yorkshire Police

ABSTRACT

The evolution of the Internet amidst a rapidly growing global economy has created a completely new environment in which traditional crime prospers. Equally the convergence of computing and communication has changed the way we live, communicate and commit crime. Cybercriminals in Nigeria commonly known as "419 scammers"; a word coined from the Nigerian criminal code that penalises people from obtaining money under false pretense cost the Nigerian consumer $13.5 billion dollars in losses in 2012. (Clarke, 2004, Sesan et al., 2012; Grabosky, 2001;)

Previous studies have focused on the causes and effects of cybercrime in Nigeria (Hassan et al., 2012; Adesina, 2017); laws penalising against misuse of computer (Olusola et. al., 2013b; Saulawa & Abubakar, 2014) and have focused relatively on financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et. al., 2012). Even though some studies have tried to explore cybercrime from the perspective of law enforcement Agencies in the UAE and Jordan (Maghairah, 2009; Alkaabi, 2010), none has been done holistically from the view of law enforcement and members of the Cybercrime Advisory Council in Nigeria.

Adopting a classical criminological framework of Routine Activity Theory (RAT), this thesis examined particularly cyber-enabled crime of advance fee fraud in Nigeria within the scope of RAT which argued that for crime to take place, three requirements must be present namely; a motivated offender, a suitable target and an absence of a capable guardian. The thesis examined the factors that motivates an offender and what elements makes a target (i.e. victim or computer) suitable for a crime. In the process, it considers the suitability of a law enforcement officer and some members of the Cybercrime Advisory Council (CAC) as capable guardians and what factors limits their capabilities in mitigating the activities of cybercriminals.

The research has been framed on an interpretivist paradigm and relativist philosophical stance, with focus on an inductive qualitative approach involving semi-structured interviews and documentation. These involved policy makers, members of parliament, telecommunications and ICT regulators on one hand; and investigators, prosecutors, forensic analyst and media practitioners particularly from the Economic and Financial Crimes Commission (EFCC), which is a leading law enforcement agency in the fight against cybercrime. The multi-dimensional evidence explains the role played by each of the stakeholders, the measures and partnership deployed in tackling cybercrime, and the challenges and recommendations needed in the international effort to tackle cybercrime globally.

Findings suggests that the proliferation and lack of effective policing of the internet enabled by the greed of individuals and lack of enforcement and collaboration of relevant stakeholders has led to financial losses to victims. The findings further show how lack of proper education and awareness of individuals, and adequate training and provision of tools for law enforcement officers contributes to the high prevalence of cybercrime in Nigeria.

Evidence is provided that documents the way members of the Cybercrime Advisory Council and especially the EFCC have attempted to overcome these challenges through partnership, capacity building and enforcement of relevant laws and policies aimed at addressing the issue of cybercrime in Nigeria. The findings of this research could help in understanding the implication of technology in crime detection and prevention, and also contribute to adhering to policies and international conventions in limiting the negative impact of cybercrime. The findings equally extends the criminological understanding of online deviant behaviors and furthers the current discussion on the role of law enforcement in policing the Internet.

Keywords: Cybercrime, Policing, Nigeria, Routine Activity Theory

CHAPTER 1: INTRODUCTION

1.0 Introduction

This chapter presents a brief background of the phenomenon of cybercrime activities in Nigeria and the UK, the impact of such activities and the roles played by law enforcement agencies in addressing the issue. The chapter also defines the scope, states the research questions, lists the aims and objectives, identifies the problem statement and recommends contributions of the research.

1.1 Cybercrime Global Overview

According to the UNODC (2013), as the usage of the internet increases globally, especially in developing countries, the number of targets and offenders increases daily. Also, it is difficult to estimate how many users of the internet are using it for illegal activities. Cybercrime, according to Wall (2017) cannot be eradicated and there is no way to 'turn these technologies off'. He further argued that more laws to address the issue of cybercrime is not the answers as most existing computer misuse laws in all jurisdictions are not properly enforced. Alternatively, using technology as a counter-measure is not the appropriate response as it is sometimes used to restrict the freedom of others. However, cybercrime could only be managed in a way the risks and harm are reduced to the barest minimum. In order to tackle cybercrime, law enforcement, government and the private sector as the 'capable guardians' would need to collectively respond adequately to the ever-evolving nature of technology based crimes (Wall, 2017).

1.1.1 Background to the Research

Nigeria has a population of over 191 million and is ranked first in the number of internet users within Africa with 91 million active users. The country is multi-ethnic and culturally diverse and accounts for 47 percent of West Africa's population (Internet World Stats, 2017; World Bank, 2017). Policing crime in Nigeria has been the sole responsibility of the Nigerian police for decades (Nigerian Police Force, 2017b), however, maintaining of public security is one of the biggest challenges facing the country due an ineffective police force that has rendered the Nigerian government handicapped to function maximally (Owen, 2014; Nwachukwu, 2012). This problem is further compounded with the coming of the internet and smartphones which has made the internet more accessible and affordable even to criminals (Clough, 2010).

Due to the integration of digital technology and accessibility of the internet (Saulawa and Abubakar,2014), cybercrime has become a popular crime in Nigeria due to inadequate policing, and lack of enforcement of relevant laws and policies in the country (Adesina, 2017; Nkanga, 2011). The negative socio-economic impact of cybercrime in Nigeria, propelled the government to take drastic measures such as creating another agency, enacting cybercrime laws, and partnering with stakeholders in order to drastically reduce the activities of cybercriminals (Adesina, 2017; Adomi and Igun 2008). Thus, the Economic and Financial Crimes Commission (EFCC) was established through an act of parliament called the EFCC Act (2004) and Advance Fee Fraud and other Fraud Related Offences (AFF) Act (2006) in order to investigate financial crimes such as cybercrime (Chawki, M., Darwish, A., Khan, M.A., Tyagi, S., 2015; Obuah, 2010). However, over the years, the adequacies of the laws and policies in fighting cybercrime have been limited (Chawki et al., 2015), therefore, the Cybercrime Prohibition, Prevention Act (2015) was signed into law in order to sanitise the Nigerian cyberspace (Paul, 2015). Table 1.1 illustrating the population and internet users vis a vis the internet crime rate in Nigeria and other countries.

S/N	COUNTRY*	POPULATION (2017 EST)	INTERNET USERS (DEC 2000)	INTERNET USERS (JUNE 2017)	PENETRATION	INTERNET CRIME (VICTIMS)	FACEBOOK SUBSCRIBERS 30-JUN-2017
1	**Nigeria**	191 million	200,000	91 million	47.7%	18th	16 million
2	**Canada**	36 million	-	33 million	90%	1st	23 million
3	**India**	1.3 billion	47 million	462 million	34.4%	2nd	241 million
4	**UK**	65 million	-	62 million	94.8%	3rd	44 million
5	**Australia**	24 million	6 million	21 million	88.2%	4th	15 million
6	**France**	64 million	-	56 million	86.8%	5th	33 million
7	**Brazil**	211 million	-	139 million	65.9%	6th	139 million
8	**Mexico**	130 million	-	85 million	65.3%	7th	85 million
9	**China**	1.3 billion	22 million	738 million	53.2%	8th	1.8 million
10	**Japan**	126 million	47 million	118 million	94%	9th	26 million

(Adapted from Internet Crime Report 2016 & Internet World Stats 2017) ***excluding the USA**

Table 1.1: Showing Countries and Internet Stats vis a vis number of Internet Crime Victims

The Internet Crime Report (2016) ranked Nigeria 18th in the world in terms of victims loss, which is seen as a significant improvement to the Internet Crime Report (2010) that ranked the country 3rd after the United States and the United Kingdom with the highest prevalence of cybercrime in the world.

1.1.2 Problem Statement

Undeniably, the policing of crime using the traditional Nigerian police has many limitations (Owen, 2014), and the integrity of the Nigerian police force has been eroded by its failure to perform its constitutional responsibilities to the society (Nwachukwu, 2012). Due to that, cybercrime has had a negative impact to the economy and reputation of the country as a haven of criminals. Ribadu (2007) argued that, cybercrime transaction worth £300 million, €200 million, and $500 million were stopped between 2003 and 2007, and recently it cost Nigerian consumers approximately $13.5 billion dollars in 2012 (Sesan, G., Soremi, B., Oluwafemi, B.; 2013). The problem of cybercrime in Nigeria is further compounded by the increased usage of the internet for fraudulent activities (UNODC, 2013) and the lack of cyber user awareness, which makes internet users vulnerable to be exploited by criminals online (Kortjan and Solms, 2014). Even though, the Nigerian government have developed appropriate legal and institutional frameworks in securing the Nigerian cyberspace (Adomi and Igun, 2008), policing the cyberspace would require governments and legal systems to continuously adapt to new technologies and strategies in tackling cybercrime (Grabosky, 2001). Currently, there is a need for the Nigerian government to work together in strengthening the legal frameworks for cybersecurity, and also enforcing existing laws in order to reduce the impact of cybercrime in the society (Olusola, M., Samson, O., Semiu, A., Yinka, A. 2013b; Hassan, A.B., Lass, F.D., Makinde, J., 2012)

1.1.3 Scope

Previous studies have focused on the causes and effects of cybercrime in Nigeria (Hassan et al., 2012; Adesina, 2017); laws penalising against misuse of computer (Olusola et. al., 2013b; Saulawa & Abubakar, 2014) and have focused relatively on financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et. al., 2012). Even though some studies have explored cybercrime from the perspective of law enforcement Agencies in the UAE and Jordan (Maghairah, 2009; Alkaabi, 2010), none has been done holistically from the view of law enforcement and members of the Cybercrime Advisory Council in Nigeria. The research focuses on the activities of the activities EFCC in relation to other key stakeholders in the investigation of cybercrime. Embracing a classical criminological view of Routine Activity Theory (RAT), the research examined Advance Fee Fraud, a variant of cybercrime, in understanding the challenges and recommendations needed in the multi-national efforts to tackle cybercrime. Even though, the research is limited on activities of Nigerian law enforcement, it examined the role of selected UK law enforcement agencies in investigating

cybercrime. Therefore, the scope of the research is limited to activities of law enforcement agencies (LEAs) investigating cyber-enabled crimes in Nigeria, which is viewed from a theoretical lens of RAT. Figure 1.1 shows the research scope of this study.

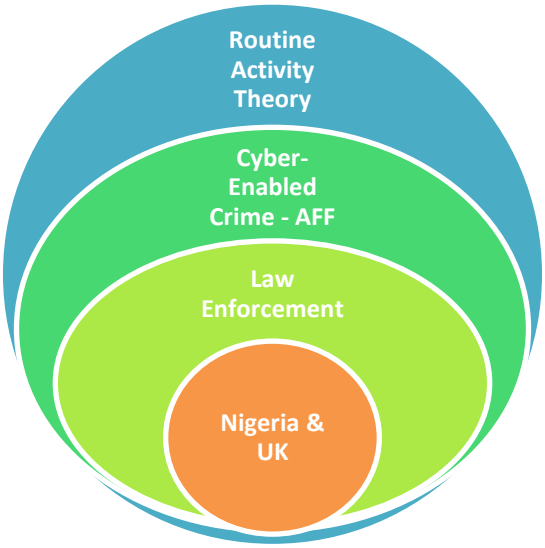


Figure 1.1: Scope of Research

Figure 1.1 showing the theoretical framework as RAT, the research context as Nigeria and the UK, the sector as law-enforcement agency, and the type of crime as cyber-enabled crime.

1.2 Definition of Terms

These terms were used throughout the research study and a detailed definition is provided below:

1.2.1 Cybercrime

Cybercrime is defined as the use of electronic devices or computers via information systems to facilitate illegal activities (McQuade 2006, p. 2). The Association of Chief of Police Organisation (2009) defines cybercrime as "the use of networked computers or internet technology to commit or facilitate the commission of crime" (ACPO 2009).

1.2.2 Cyber-Enabled Crime

Cyber-enabled crimes are 'traditional crimes, which can be increased in their scale or reach by the use of computers, computer networks or other form of ICT'. Two published forms of cyber-enabled crime relate to fraud and theft (McGuire and Dowling, 2013b)

1.2.3 Advance Fee Fraud

Advance Fee Fraud or '419' fraud; a name coined from a section of the Nigerian Criminal Code is a prevalent crime within the West African organised criminal networks. There are many variations of the scheme and scams which is designed to persuade recipients/victims to part with their money (Stevens 2006). The Criminal Code Act (1990) defines advance fee fraud through section 419 as:

> *Any person who by any false pretence, 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 is liable to imprisonment for three years.*

The EFCC Red Alert on Scam (2015) defines advance fee fraud as a form of confidence scam whereby there is intent to defraud through the false pretense of offering a service or reward that does not exist.

1.2.4 Law Enforcement Agency

Law enforcement agency (LEA) is a government agency that is responsible for the enforcement of the laws. The powers exercised by law enforcement agencies include; exemption from laws, arrest and prosecution, legal deception, use of force and constraint of liberty, and jurisdiction override amongst others (Oxford Dictionary, 2018; US Legal, 2016).

1.3 Rationale for Research

According to Rojon and Saunders (2012), after formulating a research question and objectives, it is important that these represent a convincing rationale for a research. They proposed the following checklist as a guide to researchers;

1. Does the research study add value through one of the following options: it addresses a new topic, provides new insights into an existing phenomenon, or replicates research to corroborate earlier findings?
2. Is the research concerned with the theory and practice of the research topic?
3. Does the research question show correlation between relevant theory and related literature?
4. Will the researcher draw meaningful conclusions and recommendations from the data collected to meet a research objective?

Therefore, adopting the argument by Rojon and Saunders (2012), the rationale for conducting this research is summarised into three factors. These factors are based on the knowledge gap of existing literature, practical and policy gaps, and few theoretical applications to the phenomenon of cybercrime within the scope of this research. The factors are as follows:

Knowledge Gap: Although, cybercrime is a 'vastly topical and newsworthy subject' (Wall, 2004), it continues to evolve due to technological advancements and reliance of digital technologies to communicate (Grabosky, 2001). Previous studies focused mainly on financial cost (Sesan et al., 2012; WITFOR, 2005), laws and legal frameworks (Olusola et at., 2013b, Saulawa and Abubakar, 2014), and causes and effects of cybercrime (Adesina, 2017; Hassan et al., 2012 & Adomi and Igun, 2008). There is a lack of sufficient research on policing cyber criminals in Nigeria, and this has created a gap between policy makers, the academia and law enforcement.

Practice and Policy Gap: Several practical and policy issues differ between nations and a certain degree in commonalities in practice and law is required in the international effort to tackle cybercrime (Longe, Ngwa, Wada and Mbarika, 2009; Grabosky, 2001). This lack of common operating procedures and standards between the stakeholders and countries hinders the successful investigation and prosecution of cyber criminals. Currently, the cybercrime laws in Nigeria are either inadequate (Olusola et al., 2013b;), or needs to be properly enforced (Hassan et al., 2012). Based on the researchers' professional experience, there is significant information sharing gap between the key stakeholders within the criminal justice system in Nigeria. Due to the training and knowledge gaps as argued by (Smith, 2003), many cybercrime cases have become dormant in the court system as most prosecutors and judges do not have the requisite knowledge to understand the dynamics of cybercrime.

Theoretical Application: There are few literatures discussing the theoretical application to cybercrime in Nigeria. Some attempts have been made by Marenin and Reisig (1995) in explaining patterns of crime, and Olayemi (2014), in discussing the socio-technological analysis of cybercrime. Therefore, the lack of existing literature on the application of routine activity theory was a rationale in conducting this research.

1.3.1 Rationale for Selection of UK and Nigeria

The researcher rationale for selection of the UK and Nigeria are based on the following commonalities between the countries. The rationales are as follows:

Commonwealth Members: Both the UK and Nigeria are members of the Commonwealth of Nations and share many similarities as most of the Nigerian Legal framework were derived from British common laws and practices (The Commonwealth, 2018).

Council of Europe Signatories: The UK and Nigeria are signatories to Convention on Cybercrime (Council of Europe, 2018). Nigeria is also a signatory of several treaties and conventions on international cooperation in criminal matters such as UNTOC, UNCAC etc.

Mutual Legal Agreement Treaty (MLAT): Both countries have a bilateral mutual legal agreement in the areas of arrest, confiscation or drug trafficking (UK Government, 2016b). The UK government is supporting the Nigerian government through capacity building and partnership in order to reduce the number of UK citizens and businesses falling victim to fraud and cybercrime originating in Nigeria (Elebeke, 2015).

Accessibility of Data: The accessibility of primary data through interviews and documentation from Nigeria is also a rationale for selection of Nigeria as a case study.

1.3.2 Rationale for Selection of Nigerian Stakeholders

This research study is examining the different roles played by members of the Cybercrime Advisory Council (CAC) in investigating cybercrime. The researcher selected the Economic and Financial Crimes Commission as the main case study and other relevant stakeholders such as the Office of the National Security Adviser (ONSA); Nigerian Information Technology Development Agency (NITDA); Nigerian Communications Commission (NCC); and the Nigerian Senate. Based on the research scope (Figure 1.1), the researcher rationale for the selection of these stakeholders are as follows:

Members of Cybercrime Advisory Council: Section 42 (1) of the Cybercrimes Act (2015) states the members of the council. Amongst the members are ONSA, EFCC, NITDA and NCC. Each of these members has specific roles, which is discussed further in Chapter 2 (Research Context). For example, investigations particularly of fraud-related cybercrime have been carried out by the EFCC (AFF Act 2006; EFCC Act, 2004) while the ONSA is the central authority in coordinating other members of CAC and the designated Nigerian Computer Emergency Response Team (Council of Europe, 2017).

Perception and Awareness: In a recent study, (UNODC, 2017) about corruption in Nigeria, the EFCC was ranked as the most effective anti-corruption organisation in Nigeria. The study showed that 64.9% of participants are aware of the EFCC, while 78.3% view the agency to be

very effective. Table 1.2 showing the awareness and perception of effectiveness of anti-corruption institutions in Nigeria.

S/N	Organisation	Perception of Effectiveness (%)	Awareness of Organisation (%)
1	**Economic & Financial Crimes Commission (EFCC)**	78.3%	64.9%
2	**Nigerian Police Force (NPF)**	39.7%	90.7%
3	**Federal High Court (FHC)**	64.1%	47.7%
4	**Code of Conduct Bureau (CCB)**	64.6%	20.1%
5	**Independent Corrupt Practices Commission (ICPC)**	64.7%	30.0%
6	**Federal Ministry of Justice (FMoJ)**	60.9%	34.9%
7	**Code of Conduct Tribunal (CCT)**	67.1%	23.4%

Table 1.2: Awareness and perception of effectiveness of anti-corruption institutions (UNODC, 2017)

Table 1.2 illustrates that, the traditional Nigerian police as the most visible organisation in Nigeria with 90.7% of participants aware of their existence, which is in contrast to 39.7% that view them as effective. Table 1.2 clearly illustrates that based on effectiveness; the EFCC was chosen as the main case study.

Accessibility: The researcher has professional and privileged access to the EFCC as he has worked with them previously before undertaking this study. Most studies about the EFCC are based on secondary data, however, this study has collected and analysed primary data for the purpose of adding to existing knowledge on cybercrime policing in Nigeria.

1.3.3 Rationale for Selection of Advance Fee Fraud

Advance Fee Fraud is confidence scams and despite the high number of incidences involving Nigerian criminals, it has now become a global crime (EFCC, 2014). Table 1.3 illustrates that majority of the crime investigated by the EFCC in Nigeria between the year 2011-2014 is advance fee fraud. AFF offences have recorded the highest number of cases investigated and convictions secured in Nigeria (EFCC, 2012, 2013, 2014).

Table 1.3 presents the major offences investigated by the EFCC.

S/N	Offence Category	2014	2013	2012	2011
1	**Advance Fee Fraud (AFF)**	1910	2379	1585	1386
2	**Bank/Securities Fraud**	594	621	331	492
3	**Public Sector Corruption/Money Laundering**	506	878	700	872
4	**Pipeline Vandalism/Oil Bunkering**	21	25	53	45
5	**Procurement Fraud**	21	44	20	64
6	**Cyber Crime***	147	96	-	-
7	**Real Estate Fraud**	15	11	13	-

***prior to 2013, Cybercrime offences were reported under AFF cases**

Table 1.3: Major Offences Investigated by the EFCC (2011-2014) (EFCC, 2014)

Table 1.3 illustrates that prior to 2013, cybercrime cases were reported as AFF cases, and AFF cases recorded the highest numbers in terms of petitions received and investigations conducted. This study corroborates an earlier study done by the NBS (2007) that showed, 82.9% of participants that participated were aware about the EFCC because of its investigation of advance fee fraud cases. Therefore, the high prevalence of advance fee fraud in Nigeria and the high conviction rate of AFF cases makes it a suitable crime to be selected for this research.

1.3.4 Rationale for Selection of UK Stakeholders

The two UK stakeholders selected for this research are the National Crime Agency (NCA) and the West Yorkshire Police (WYP). The selection was based on their existing international cooperation with Nigerian law enforcement agencies and their willingness to participate in the research.

International Cooperation: The National Crime Agency has been investigating cybercrime jointly with the Nigerian EFCC for the past five years in identifying a West African organised crime group involved in fraudulent activities such as advance fee fraud, bank and credit card fraud (Council of Europe, 2017).

Partnership: Both agencies (i.e. NCA and WYP) were willing to partner and participate in the research. The researcher was invited to a high level Cyber Technical Meeting at the West Yorkshire Police Force headquarters to present his research and discuss some of the findings with the aim of finding solutions to tackling cybercrime.

1.4 Aims and Objectives of the Research

The main aim of the study is to identify any improvements required in international efforts to tackle cybercrime within the scope of law enforcement agencies in the UK and Nigeria. To fulfil this aim, the researcher seeks to achieve the following objectives:

1. To examine the different roles played by members of the Cybercrime Advisory Council (CAC) in tackling cybercrime in Nigeria through review of relevant literature and interviews.
2. To examine the different definitions and categorizations of cybercrime through review of relevant literature.
3. To explore the different forms of cybercrime that is prevalent in Nigeria through review of relevant literature and interviews.
4. To understand the different reasons cybercrime is committed in Nigeria through review of relevant literature and interviews.
5. To explore the benefits of partnerships in investigating cybercrime in Nigeria through review of relevant literature and interviews.
6. To examine the current measures used by LEAs in Nigeria and the UK in tackling cybercrime through review of relevant literature and interview of members of the CAC.
7. To explore the current laws used in investigating cybercriminals in Nigeria through review of relevant laws and policies.
8. To explore the challenges and limitations in investigating cybercrime in Nigeria through review of relevant literature and interview of members of the CAC.
9. To examine the recommendations and improvement required to tackle cybercrime in Nigeria and the UK through review of relevant literature and interview of members of the CAC.

1.5 Overview of Research Questions

A number of research questions were developed based on the aim and objectives above and the literature review. The research questions are as follow, however, their design is further discussed in Chapter 5 – Research Methodology

1. How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?

2. Are Law Enforcement Agencies in Nigeria capable guardians in tackling cybercrime and explored in relation to Routine Activity Theory?
3. To what extent are the current laws adequate in investigating cybercrime in Nigeria?
4. How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?
5. What improvements are needed in the International efforts in tackling cybercrime globally?

1.6 Research Correlation Map

Table 1.4 gives a graphical view into the different components of this research. The table illustrates the relationship between the research objectives, research questions, literature themes, interview question and the theoretical framework. The research correlation map guided the researcher throughout the research process. The research objectives and questions are discussed in detail in Chapter 1 (Introduction) and Chapter 8 (Discussion). The literature themes were reviewed in Chapter 2 (Literature Review) and analysed in Chapter 7 (Analysis). A sample of the interview question is available in Appendix H (Interview Question & Transcript - Investigator), while the theoretical framework was reviewed extensively in Chapter 4 (Theoretical Framework) and discussed in Chapter 8 (Discussion). Table 1.4 presents how all the components of the research are linked with each other.

TITLE	INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY				
AIM	To identify any improvements required in international efforts to tackle cybercrime within the scope of LEAs in the UK and Nigeria				
S/N	**RESEARCH OBJECTIVES**	**RESEARCH QUESTIONS**	**LITERATURE THEMES**	**INTERVIEW QUESTIONS**	**THEORETICAL FRAMEWORK**
1	To examine the different roles played by members of the Cybercrime Advisory Council (CAC) in tackling cybercrime in Nigeria through review of relevant literature and interviews.		**T1: FUNCTION OF OFFICE** **T2: ROLE IN FIGHTING CYBERCRIME**	QUESTION 1, 2, 3	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
2	To examine the different definitions and categorizations of cybercrime through review of relevant literature.	**RQ4:** How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?	**T3: DEFINITION OF CYBERCRIME**	QUESTION 4	
3	To explore the different forms of cybercrime that is prevalent in Nigeria through review of relevant literature and interviews.		**T4: FORMS OF CYBERCRIME**	QUESTION 5	**RAT:** SUITABLE TARGET
4	To understand the different reasons cybercrime is committed in Nigeria through review of relevant literature and interviews.	**RQ1:** How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?	**T5: CAUSES OF CYBERCRIME**	QUESTION 6	**RAT:** MOTIVATED OFFENDER
5	To explore the benefits of partnerships in investigating cybercrime in Nigeria through review of relevant literature and interviews.		**T6: PARTNERSHIP** **T7: BENEFITS OF PARTNERSHIP**	QUESTION 7, 8, 9, 10	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
6	To examine the current measures used by LEAs in Nigeria and the UK in tackling cybercrime through review of relevant literature and interview of members of the CAC.	**RQ2:** Are LEA in Nigeria capable guardians in tackling cybercrime and explored in relation to RAT?	**T8: MEASURES & COUNTER - MEASURES**	QUESTION 11 & 12	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
7	To explore the current laws used in investigating cybercriminals in Nigeria through review of relevant laws and policies.	**RQ3:** To what extent are the current laws adequate in investigating cybercrime in Nigeria?	**T9: LAWS**	QUESTION 13	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
8	To explore the challenges and limitations in investigating cybercrime in Nigeria through review of relevant literature and interview of members of the CAC.	**RQ2:** Are LEA in Nigeria capable guardians in tackling cybercrime and explored in relation to RAT?	**T10: CHALLENGES**	QUESTION 14	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
9	To examine the recommendations and improvement required to tackle cybercrime in Nigeria and the UK through review of relevant literature and interview of members of the CAC	**RQ5** What improvements are needed in the International efforts in tackling cybercrime globally?	**T11: RECOMMENDATIONS**	QUESTION 15 & 16	

Table 1.4: Correlation between the Research Objectives, Research Questions, Themes, Interview Question and Theoretical Framework

1.7 Research Structure

The research structure is a synopsis of what each chapter entails. It is further categorised into nine chapters namely:

CHAPTER 1 (INTRODUCTION): This chapter introduces the research topic and identifies the problem statement by narrowing down the scope of the research investigation. It defines some key terms such as 'cybercrime' and 'advance fee fraud' that are frequently used in the study. The chapter also enumerates the researcher's rationale for selecting the UK and Nigeria and also the rationale for the selection of the three law enforcement agencies for this study. Furthermore, the chapter gives an overview of the aims, objectives and research questions of the research. Finally, the expected research contributions are categorized and explained further.

CHAPTER 2 (RESEARCH CONTEXT): The research context chapter gives an in-depth overview of the research phenomenon of cybercrime within the country of Nigeria. The chapter further explores the policing of crime in Nigeria and discusses the structural problems associated with the traditional Nigerian Police in investigating and tackling crime. A brief overview of cybercrime in the UK and Nigeria is presented with an emphasis on policing cybercrime. The research participants overview is elaborated and defined within the scope of the Cybercrime Advisory Council.

CHAPTER 3 (LITERATURE REVIEW): This chapter gives an overview of the main topics of the research by defining 'crime' and 'cybercrime' from different perspectives. It also gives an overview of cybercrime in Nigeria by highlighting the statistics and socio-economic cost of cybercrime to Nigeria. It goes further to narrow down the scope of the literature to 'advance fee fraud,' a variant of cybercrime and gives a detailed overview of the Nigerian government efforts in combating cyber criminals. The chapter emphasizes the role of the EFCC in tackling cybercrime in Nigeria as well as the UK and international responses to cybercrime. Furthermore, it mentions the limitations to tackling cybercrime Finally, it presents the cybercrime investigation timeline as a framework and guide for the research investigation and process.

CHAPTER 4 (THEORETICAL FRAMEWORK): The theoretical framework chapter lays the foundation for the theoretical component of the research topic. It guides the formulation of the research objectives and questions and guides the researcher in narrowing down the scope of the

research within various theoretical arguments in understanding crime and policing cybercrime. The chapter gives an overview of multiple theoretical arguments that fit into the research paradigm and justifies the selection of the theoretical argument that guides the researcher in exploring cybercrime in Nigeria within the scope of law enforcement activities.

CHAPTER 5 (METHODOLOGY): The methodology chapter is an integral component of the research process. The chapter introduces the researcher's model, philosophy, and paradigm underlying the study. It also classifies the research; state the methodology; enumerates the approach as well as the choices of methods and approaches that the researcher has made along with justifications. The chapter further explains the researcher's data collection methods and analysis for these choices. Furthermore, the chapter states what methods the researcher is using to validate the research findings. Finally, the chapter enumerates the researcher's ethical considerations throughout the research process.

CHAPTER 6 (PILOT INVESTIGATION): This chapter introduces the pilot study conducted and the justifications for conducting such a pilot study. It discusses some observations of the pilot study and lists all the stakeholders interviewed for the pilot and main study.

CHAPTER 7 (DATA ANALYSIS): The data analysis chapter introduces the various research participants and how the research interview questions were designed and developed. The chapter also examines the function of the interviewer and how the interview was administered to the participants. An overview of the interview transcription and coding of the data is further elaborated with an emphasis on thematic analysis of the data. The chapter further presents the analysis of the findings and the interpretation of the themes. Finally, a summary of the findings and conclusion are discussed and elaborated.

CHAPTER 8 (DISCUSSIONS): The discussions chapter of the research discusses the various findings from the analysis of the data in relation to the research questions of the study. Furthermore, an overall theme conclusion and summary of discussion is adequately examined.

CHAPTER 9 (CONCLUSION): This is the final chapter of the research that summarizes the overall objectives of the research. The contributions of the research are categorised in terms of theory, knowledge, pratice and police respectively. The limitations of the research are identified and discussed and an overview of possible future research in this area is elaborated on and

examined. Finally, a graphical milestone is discussed with an overall conclusion of the complete research study.

1.8 Research Contributions

The research contributes to the field of cybercrime and policing in several ways. Whilst these contributions emerged throughout the research process and are discussed in detail in Chapter 9 (Conclusion), a summary of the contribution are as follows:

Knowledge: The identification of eleven themes related to cybercrime investigation in Nigeria and development of fifty-one emerging outcomes contributes to existing literature on cybercrime especially in Nigeria. The study is also specific to LEAs in Nigeria and the UK and some members of the Cybercrime Advisory Council. It is hoped the findings of the research contributes to the current discussion on the role of LEAs in policing the internet.

Theory: The study addresses the gap in the application of Routine Activity Theory to cybercrime in Nigeria by extending the criminological understanding of a motivated offender, the suitability of a target and the capability of guardianship within the context of LEAs.

Practice and Policy: The findings of the research enumerates some measures and policies to be adhered to proferring solution in tackling cybercrime in Nigeria. It is hoped the study's recommendations would be an added value to policy makers decisions in allocating more resources to LEAs and relevant stakeholders to tackle cybercrime. The research would be valuable to investigators and prosecutors in Nigeria as it extends application of some best practices in the UK in curtailing cybercrime.

1.9 Conclusion

The chapter introduces the research topic by identifying the problem and narrowing down the scope of the research. The rationale for the research as well as the aims, objectives and the research questions are enumerated. Finally, the chapter summarises each chapter of the research and lists the expected research contributions of the study.

Table 1.5 enumerates the research contributions and their respective references within the thesis.

S/N	Contribution	Summary	Reference
1	**Theoretical contribution**	Extends the RAT understanding of suitable target, motivated offender and capable guardianship within the Nigerian and law enforcement context.	**Chapter: 9** **Page. 237**
2	**Knowledge contribution**	• Themes & emergent themes • Cybercrime Investigation Timeline • Nigerian context (LEA & CAC) • Specific roles in investigating cybercrime • Novel recommendations	**Chapter: 9** **Page. 238**
3	**Practice and policy contribution**	• Review and misapplication of laws • Central coordination of efforts • Autonomous and upgraded forensic lab • Training for judges & Investigators	**Chapter: 9** **Page. 239**

Table 1.5: Summary of research contributions

CHAPTER 2: RESEARCH CONTEXT

2.1 Introduction

The research context chapter gives an in-depth overview of the research phenomenon of cybercrime within the country of Nigeria. The chapter further explores the policing crime in Nigeria and discusses the structural problems associated with the traditional Nigerian Police Force in investigating and tackling crime. A brief overview of cybercrime in the UK and Nigeria is presented with an emphasis on policing cybercrime. The research participant overview is elaborated on and defined within the scope of the Cybercrime Advisory Council.

2.2 Country Profile

Nigeria is situated in the West African Region with a population of approximately 184 million inhabitants. The country accounts for 47 percent of West Africa's population and has one of the largest population of youth in the world. It has 36 autonomous states and practices a federal system of government. Nigeria is a multi-ethnic and culturally diverse nation with abundance of mineral resources, thus, making it Africa's largest oil exporter and it also has the largest natural gas reserves on the continent (World Bank, 2017).

2.3 Policing Crime in Nigeria

The Nigerian Police is the principal law enforcement agency in Nigeria with a staff strength of about 371,800. The Nigerian Police is a very large organization consisting of 36 State commands grouped into 12 zones and 7 administrative organs. The agency is currently headed by an Inspector General of Police (Nigerian Police Force, 2017b). The Vision of the Nigerian Police Force is 'to make Nigeria safer and more secure for economic development and growth; to create a safe and secure environment for everyone living in Nigeria'. The Mission Statement of the Nigerian Police includes:

a) To partner with other relevant security agencies and the public in gathering, collating and sharing information and intelligence with the intention of ensuring the safety and security of the country.
b) To participate in efforts aimed at addressing the root causes of crime while ensuring that any criminal act is investigated so as to bring the criminals to justice in a fair and professional manner.

c) To engender an efficient, effective, well-trained and highly motivated workforce, with deliberate efforts aimed at improving the capacity and welfare of all officers and men of the Force.
d) To build a people's friendly Police Force that will respect and uphold the fundamental rights of all citizens.
e) To build a gender sensitive and gender friendly Police Force that will give equal opportunity to female Police Officers, while at the same time respecting their differences (Nigerian Police Force, 2017a)

According to Alemika and Chukwuma (2003), successive Nigerian Constitutions since 1979 have provided for the existence of the Nigeria Police Force alone. The 1999 Constitution had provisions relevant to Nigerina Police Force, Police Council and the Police Service Commission (National Assembly of Nigeria, 2017b).

> *Section 214(1) of the 1999 Constitution provided that: There shall be a Police Force for Nigeria, which shall be known as the Nigeria Police Force, and subject to the provisions of this section, no other police force shall be established for the Federation or any part thereof.*

The 1999 Constitution re-established the Police Council, which was in the 1963 Constitution but absent from the 1979 Constitution. The Third Schedule of the 1999 Constitution created the Nigeria Police Council and the Police Service Commission. The Police Council consists of:

(a) President who shall be the Chairman;
(b) Governor of each State of the Federation;
(c) Chairman of the Police Service Commission; and
(d) Inspector-General of Police (National Assembly of Nigeria, 2017b).

2.3.1 Problems of Nigerian Police

Owen (2014) argues that the maintaining of public security is perhaps the biggest challenge to Nigeria's consolidating democracy. Since 1999, the Nigeria Police Force has been central in managing and responding to those challenges. The integrity of the Nigeria police has been eroded by the ineffectiveness and inefficiency of their constitutional responsibilities to the society (Nwachukwu, 2012). Due to lack of an effective police force, the Nigerian Government, society and economy will find it difficult to function effectively and maximally. Some of the challenges to policing Nigeria include rapid urbanisation, population growth, unemployment,

mass migration, breakdown of social order and the opening of new economic arenas, which give rise to a huge range of criminal challenges including armed robbery, kidnap, corruption, fraud, terrorism, sexual assault, domestic violence, communal strife, and criminality in politics (Owen, 2014). Owen (2014) argues that the challenge is to keep the NPF at the centre of law, order and security management, in the face of five main limiting factors:

a) New challenges to peace and security, across many regions and states of the country, of which persistent problems in many states of the Niger Delta, Middle-Belt, South-East, and North-East, are only the most high-profile. Terrorism, communal conflicts, political conflicts, and new types of crime are also reshaping the policing landscape.
b) Limited human resource, skills and motivation problems are rampant within the force
c) Limited resources to achieve mandated tasks due to the Federal Government inability to fund the Nigeria Police Force adequately to achieve all tasks before it.
d) Multiple overlapping agencies taking on specialist policing duties, including the National Security and Civil Defence Corps, Army, State Security Service, and others.
e) Structural constraints as the Nigeria Police remains a centralised force operating in a federalised polity and the tension between these two arrangements is still unresolved. Its structures of accountability also render it vulnerable to interference by a political class who limit police effectiveness in enforcing the law.

In a recent study, UNODC (2017) about corruption in Nigeria, the Nigerian Police was ranked as the most ineffective law enforcement agency in Nigeria. Even though the study showed that 90.7% of the participants knew the Nigerian Police, only 39.7% thought they were effective. Table 2.1 showing the awareness and perception of effectiveness of anti-corruption institutions and other organisations in Nigeria.

S/N	Organisation	Perception of Effectiveness	Awareness of Organisation
1	**Economic & Financial Crimes Commission (EFCC)**	78.3%	64.9%
2	**Nigerian Police Force (NPF)**	39.7%	90.7%
3	**Federal High Court (FHC)**	64.1%	47.7%
4	**Code of Conduct Bureau (CCB)**	64.6%	20.1%
5	**Independent Corrupt Practices Commission (ICPC)**	64.7%	30.0%
6	**Federal Ministry of Justice (FMoJ)**	60.9%	34.9%
7	**Code of Conduct Tribunal (CCT)**	67.1%	23.4%

Table 2.1: Awareness and perception of effectiveness of anti-corruption institutions (UNODC, 2017)

The study corroborates an earlier study by the NBS (2007) on crime and corruption that rated some national organisations in Nigeria. The study found out that 52.9% of participants thought the Nigerian Police to be 'dishonest' compared to like the EFCC in which only 6.9% viewed them to be dishonest. Table 2.2 illustrates the rating of integrity of some institutions in Nigeria.

S/N	Organisation	Very Dishonest	Somewhat Dishonest	Neither Honest or Dishonest	Somewhat Honest	Very Honest	Don't Know
1	ICPC	2.1%	5.9%	15.7%	37.2%	18.4%	19.4%
2	EFCC	1.9%	5%	8.8%	40.9%	37.2%	4.8%
3	Code of Conduct Bureau	2.9%	4.9%	18.3%	36.4%	14.8%	21.3%
4	Police Force	31.8%	21.1%	18.3%	19%	4.1%	4.4%
5	Traffic Police	19.8%	21.8%	19.3%	25.9%	6.4%	5.2%

Table 2.2: Rating of Integrity of some National Institution (NBS 2007)

2.4 Cybercrime in Nigeria

The arrival of the internet and computers has opened many opportunities for the young and old in the global community to have access to the world from their homes, offices and cyber cafes. The coming of smartphones has made internet access easier and faster (Saulawa and Abubakar, 2014; Clough, 2010). Unlike in the past when the ability to commit computer related crimes was largely limited to those with the access and skill sets; nowadays, technology is easily accessible, thus, making it available to both offenders and victims (Clough, 2010). Clough (2010) suggested that, with the proliferation of information technology and the convergence of digital and communication devices, the internet has transformed the way in which we interact and conduct businesses across the globe. Even though this has been largely a positive development, there has also been a darker side to this development because virtually every advance made in the digital domain has been accompanied by a 'corresponding niche to be exploited for criminal purposes'.

Sub-Saharan African (SSA) is the last continent to embrace the internet and mobile technologies. Internet penetration in Sub-Saharan Africa has been on the increase with most countries depending on privately owned internet acess points such as cybercafés' for their daily internet activities (Longe, Ngwa, Wada and Mbarika, 2009).

Ajayi (2003) states that the ICT revolution in Nigeria began after the return of democratic rule in 1999. After coming out of a long period of military dictatorship which had been apathetic towards the development of ICT in the country as it was perceived as posing a security threat to

the military junta, the new democratic government of Nigeria realised that the digital divide in the country would continue to widen unless the issue of developing ICT in the country was given the priority it deserved.

Cybercrime has been one of the eluding issues in the online global transactions in Nigeria because of the endemic nature of computer related frauds and crimes. Due to the integration of digital technology across the globe, the economy of most nations across the globe is accessible through the use of information and communication technology (Abubakar and Saulawa, 2014). According to Adesina (2017), Cybercrime is a very popular crime in Nigeria as criminals are widely known for luring people across the planet into various fraudulent scams such as spam mails and 'cleverly designed but cash-laundering partnership' scams.

Nigeria has a population of about 186 million and with about 97 million Internet users which represents an internet penetration of approximately 52% (Internet World Stats, 2016). Nigeria is currently ranked 24th in the world in terms of complainant reporting of cybercrime and ranked 12th in terms of complainant loss (Internet Crime Complaint Centre, 2014). This is seen as a significant improvement to an Internet Crime Report (2010) report that ranked Nigeria third with 5.8% just behind United State of America with the highest prevalence of cybercrime activities in the world.

2.4.1 Policing Cybercrime in Nigeria

Adesina (2017) stated that having a robust legislation in place to tackle cybercrime was one of the major steps taken by the Nigerian Government to tackle crime. Due to the negative financial and economic consequences of cybercrime in Nigeria, the government pursued these drastic measures in order to curtail the activities of cybercriminals. The measures were:

a. Creation of a central agency to enforce crime laws
b. Regulation of cybercafés
c. Enactment of Cyber laws
d. Government partnership with Microsoft (Adomi and Igun, 2008)

The Nigerian Government in 2004 established the Nigerian Cybercrime Working Group compromising representatives from the government and the private sector to develop a legislation on cybercrime. The Government in 2007 established the Directorate of Cyber Security under the Office of the National Security Advisor as responsible for responding to

security issues associated with the growing usage of ICT in the country (Adesina, 2017). Adesina (2017) further states that apart from these initiatives, some new laws were created such as the Economic and Financial Crimes Act 2004 and the Advance Fee Fraud and Other Fraud Related Offences Act 2006. However, due to the ineffectiveness of the laws in curbing the activities of cybercrime, the Cybercrime Bill was signed into law in May 2015, thus, properly defining the act of cybercrime as unlawful with penalties attached to any infringement of the law.

The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 was passed to promote cybersecurity and cybercrime prevention. It provides for the obligation of the ISPs, telecommunication operators and financial institutions to report and cooperate with law enforcement authorities and the Nigerian Computer Emergency Response Team (ng-CERT). Furthermore, it requires the National Security Adviser and the Attorney General to coordinate and empower the institutional and legal framework whilst establishing a Cybercrime Advisory Council to facilitate for an effective implementation, inter-agency/international cooperation, capacity building and multi-stakeholder engagement (Council of Europe, 2017).

Cybercrime has been a key agenda for the Nigerian Government for many decades. Investigations that are fraud related have been carried out by the Economic and Financial Crimes Commission (EFCC). Though the admissibility of electronic evidence was amended in the Evidence Act 2011 through the parliament, the lack of a proper legal framework on cybercrime has made criminal justice measures ineffective until 2015 when the Government adopted the National Cybersecurity Policy and Strategy through an inter-ministerial committee headed by the Office of the National Security Adviser (Council of Europe, 2017).

2.5 Cybercrime in the UK

In 2017, fraud became the most common UK crime as con artists exploited the digital world to wreak havoc on businesses and individuals. More than five million cyber offences are committed every year, accounting for over half of all UK crime, with nearly one in 10 Britons falling victim. The cyber-criminals can steal funds from bank accounts, spend using individuals' credit card details, steal identities or drain pension funds of individuals to enrich themselves at others' expense (Jones, 2017). According to Hunton (2012), the internet has provided motivated cybercriminals with a vast array of simplified, cost-effective and almost anonymous illicit opportunities.

2.6 Cybercrime Advisory Council

The Cybercrime Act (2015) establishes the Cybercrime Advisory Council which is referred to as the 'Council'. The Council shall consist of a representative each of the ministries and agencies listed under the First Schedule of this Act'.

2.6.1 Functions and Powers of the Council

The functions and powers of the Cybercrimes Advisory Council is contained in Section 43 (1) of the Cybercrimes Act (2015). The functions are as follows:

a) To create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and promotion of cyber security in Nigeria;
b) To formulate and provide general policy guidelines for the implementation of the provision of this Act;
c) To advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
d) To establish a program to award grants to institutions of higher education to establish cyber security research centres to support the development of new cyber security defence, techniques and processes in the real-world environment and;
e) To promote Graduate Traineeships in cyber security and computer and network security research and development (Cybercrimes Act, 2015).

2.6.2 Members of the Cybercrime Advisory Council

Section 42 (1) of the First Schedule of the Cybercrimes Act (2015) states that the members of the Cybercrime Advisory Council shall consist of a representative each of the following Ministries, Departments and Agencies. The members are as follows: Federal Ministry of Justice; Federal Ministry of Finance; Ministry of Foreign Affairs; Federal Ministry of Trade and Investment; Central Bank of Nigeria; Office of the National Security Advisor; Department of State Service; Nigeria Police Force; Economic and Financial Crimes Commission; Independence Corrupt Practices Commission; National Intelligence Agency; Defense Intelligence Agency; Defense Headquarters; National Agency for the Prohibition of Traffic in Persons; Nigeria Customs Service; Nigerian Immigration Service; National Space Management Agency; Nigerian

Information Technology Development Agency; Nigerian Communications Commission; Galaxy Backbone; National Identity Management Commission; Nigeria Prisons Service; One representative each from the following: Association of Telecommunications Companies of Nigeria; Internet Service Providers Association of Nigeria; ; Nigeria Bankers Committee; Nigeria Insurance Association; Nigerian Stock Exchange and NGO with focus on Cyber Security.

2.7 Overview of Research Case Studies

This research study is limited to activities of law enforcement agencies (i.e. EFCC) and other key stakeholders in Nigeria in investigating cybercriminals. These stakeholders which includes the Office of the National Security Advisor and ICT and Telecommunications Regulator are key in understanding the roles played by these agencies and the challenges impeding them in performing their respective mandates in successfully investigating cybercrime in Nigeria. The research study explores the roles played by International Stakeholders such as the National Crime Agency, which is the coordinator and operates the National Cyber Crime Unit in the UK. The research further examines the roles of a regional police namely West Yorkshire Police Force which has an innovative method of investigating cybercrime in the UK. Figure 2.1 showing the stakeholders involved in the research study.

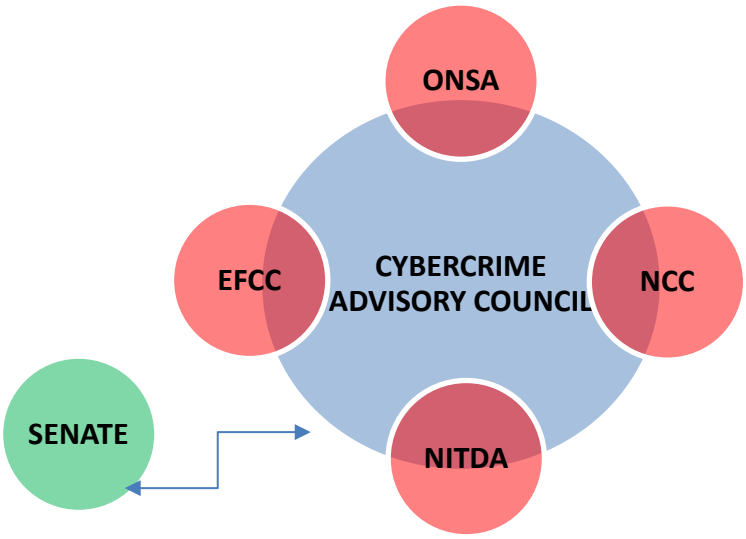


Figure 2.1: Members of the Cybercrime Advisory Council considered in Research

Table 2.3 gives an overview of each of the research case studies including their sector and country of jurisdiction respectively.

S/N	CASE STUDY	SECTOR	COUNTRY
1	Economic and Financial Crimes Commission	Law Enforcement	NIGERIA
2	Office of the National Security Advisor	Coordinator	NIGERIA
3	National Information Technology Development Agency	ICT Regulator	NIGERIA
4	Nigerian Communications Commission	Telecoms Regulator	NIGERIA
5	Senate Committee on ICT & Cybercrime	Parliament	NIGERIA
6	National Crimes Agency	Law Enforcement	UK
7	West Yorkshire Police Force	Law Enforcement	UK

Table 2.3: Showing Research Participants, Sector and Country of Jurisdiction

2.7.1 Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC) is a leading Nigerian law enforcement agency that investigates economic and financial crimes such as advance fee fraud (419 fraud) and money laundering. The EFCC was established in 2003, partially in response to pressure from the Financial Action Task Force on Money Laundering (FATF), which named Nigeria as one of 23 countries which were non-cooperative in the international community's efforts to fight money laundering (EFCC, 2017). The EFCC was established by an Act of Parliament known as the Economic and Financial Crimes Commission (Establishment) Act, 2004 which mandates the Commission with the responsibility for the enforcement of all economic and financial crimes laws, among other things (EFCC, 2004). The EFCC was established due to the Nigerian Government's determination to combat fraudulent activities of some Nigerians and foreigners, mismanagement of the economy, corruption by public officials and lack of accountability and transparency that led to Nigeria being known as the haven for money laundering and financial crimes. Thus, the EFCC was established with a mandate to cleanse the system (EFCC, 2016).

The EFCC by virtue of Section7(2) of the Establishment Act 2004 is charged with the responsibility of enforcing the provisions of laws relating to economic and financial crimes, including:

a) Money Laundering (Amendment) Act 2004 and 2013 as amended
b) Advance Fee Fraud and other Fraud Related Offences Act, 2006
c) The FailedBanks (Recovery of Debts) and Financial Malpractices in Bank Act, 1994
d) The Bank and other Financial Institutions Act, 1991

e) Miscellaneous Offences Act, 1985
f) Terrorism Act, 2011 and
g) Cybercrimes (Prohibition and Prevention) Act 2015 (EFCC 2004; EFCC 2016; Cybercrimes Act 2015)

Under the EFCC, participants were selected from five departments and units. These departments play a significant role in tackling cybercrime in Nigeria. An overview of the departments is given as follows:

Operations Department: The department is responsible for the prevention and detection of offences in violation of the EFCC Act; the arrest of economic and financial crime perpetrators; amongst others (EFCC, 2004)

Legal and Prosecution Department: The department is responsible for prosecuting offenders that have committed any form of economic and financial crimes, supporting the investigation unit by providing the unit legal advice and assistance and conducting proceedings necessary towards the recovery of assets or property forfeited under the EFCC Act (EFCC, 2004).

ICT Unit: The unit is responsible for the 'conceptualisation, operations, management and maintenance of the EFCC's ICT infrastructure' (EFCC, 2014).

Public Affairs Department: The department informs and enlightens the public on the activities of the EFCC. It also mobilises the public against economic and financial crimes.

Forensic Unit: The unit aids the investigation and prosecution of crimes through the scientific examination of evidence (EFCC, 2014).

Figure 2.2 illustrates some of the function of the departments and units involved in the research

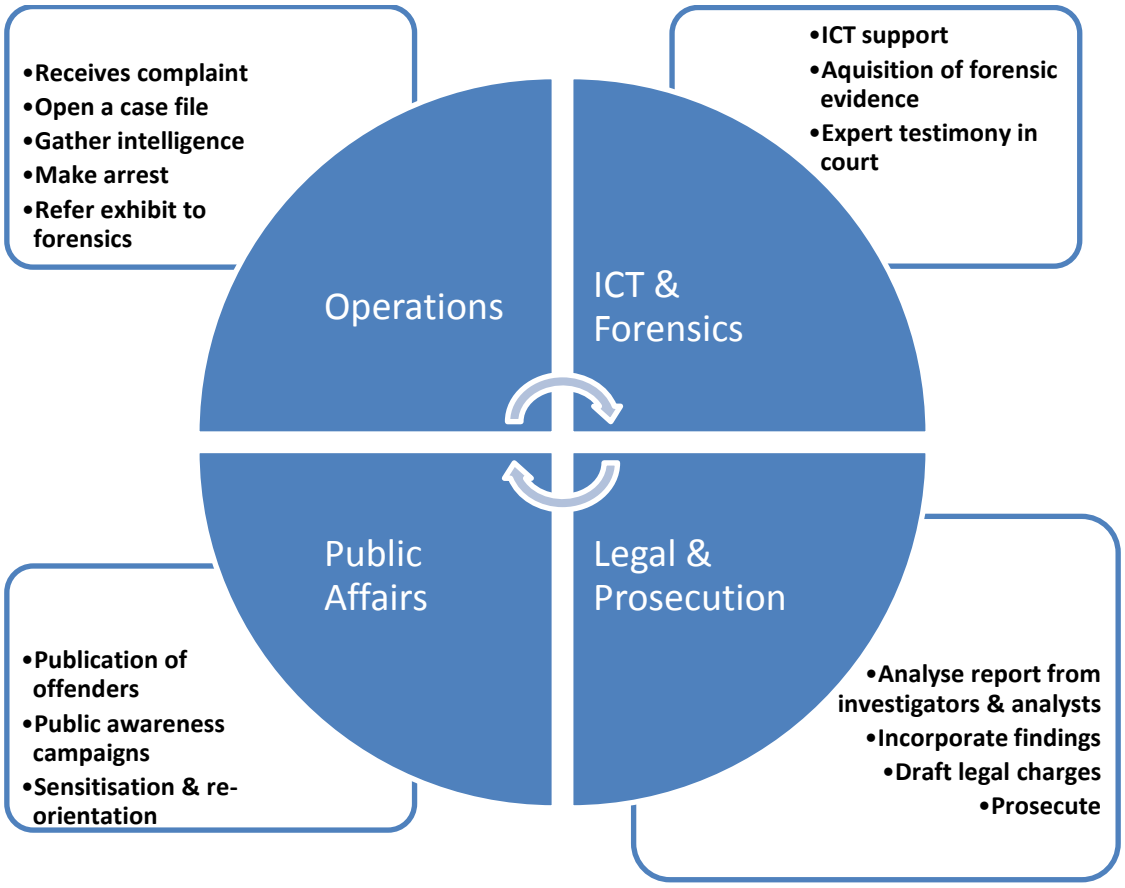


Figure 2.2: Relevant stakeholder with the EFCC and specific cybercrime roles (EFCC 2012, 2013, 2014)

2.7.2 Office of the National Security Advisor (ONSA)

The National Security Advisor is a one of the most senior aides in the cabinet of the President of Nigeria who serves as the chief advisor to the President on national security issues. The NSA participates in the meetings of the National Security Council and other deliberations on security matters. The National Security Advisor is often appointed by the President of Nigeria and serves a tenure of not more than 4 years (National Security Advisor – Nigeria, 2017).

The Office of the National Security Advisor under the National Security Advisor is the overall coordinator of the Cybercrime Advisory Council. Some of the functions of the Council include:

a) Creating an enabling environment for the sharing of information and experience

b) Formulating policy guidelines regarding implementation of provisions of the Cybercrimes Act 2015
c) Promoting training, education and research
d) Advice on preventive and other measures regarding cybercrime and cybersecurity. (Council of Europe, 2017; Cybercrime Act, 2015)

2.7.3 National Information Technology Development Agency (NITDA)

The National Information Technology Development Agency (NITDA) was created in April 2001 to implement the Nigerian information technology policy and co-ordinate general IT development in the country. It was mandated by the NITDA Act (2007) to create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria (Ajayi, 2003; NITDA, 2017a). NITDA's mandate is quite diverse and vast but mainly focusing on the responsibilities of the Agency for fostering the development and growth of IT in Nigeria. Some of the mandates of NITDA are:

a) To operate and implement the National IT policy and to give effect to provisions of the National Information Technology Development Agency Act (NITDA Act) of 2007;
b) To ensure that the entire citizenry is empowered with Information Technologies through the development of a critical mass of IT proficient and globally competitive manpower;
c) To enter into strategic alliance with the private sector as well as international organizations for the actualization of the IT vision;
d) To develop and regulate the Information Technology Sector in Nigeria;
e) To ensure that Information Technology resources are readily available to promote efficient national development;
f) To enhance the national security and law enforcement;
g) To ensure Simple, Moral, Accountable, Responsive and Transparent (SMART) governance, using the instrument of Information Technology; (NITDA, 2017b).

2.7.4 Nigerian Communications Commission (NCC)

The Nigerian Communications Act 2003, which was signed into law by the President, Chief Olusegun Obasanjo (GCFR) on the 8th of July 2003 after being passed by both Houses of the

National Assembly established the Nigerian Communications Commission and provides the NCC with the capacity to properly carry out its Regulatory functions and activities (NCC, 2017b). Some of the Objectives of the NCC are as follows:

a) To promote the implementation of the national communications or telecommunications policy as may from time to time be modified and amended.
b) To establish a regulatory framework for the Nigerian communications industry and for this purpose to create an effective, impartial and independent regulatory authority.
c) To promote the provision of modern, universal, efficient, reliable, affordable and easily accessible communications services and the widest range thereof throughout Nigeria.
d) To encourage local and foreign investments in the Nigerian communications industry and the introduction of innovative services and practices in the industry in accordance with international best practices and trends.
e) To ensure fair competition in all sectors of the Nigerian communications industry and also encourage participation of Nigerians in the ownership, control and management of communications companies and organisations.
f) To encourage the development of a communications manufacturing and supply sector within the Nigerian economy and also encourage effective research and development efforts by all communications industry practitioners.
g) To protect the rights and interest of service providers and consumers within Nigeria.
h) To ensure that the needs of disabled and elderly persons are taken into consideration in the provision of communications services.
i) To ensure an efficient management including planning, coordination, allocation, assignment, registration, monitoring and use of scarce national resources in the communications sub-sector, including but not limited to frequency spectrum, numbers and electronic addresses, and also promote and safeguard national interests, safety and security in the use of the said scarce national resources. (NCC, 2017b).

2.7.5 National Assembly – Senate Committee on ICT & Cybercrime

The National Assembly Senate Committee on ICT and Cybercrime is charged with legislative oversight responsibility over ICT development and cyber-crime control in Nigeria (Cyber

Sphere, 2017). The National Assembly was created by section 47-49 of the 1999 Constitution of the Federal Republic of Nigeria which states that (National Assembly, 2017b):

> *S47 - There shall be a National Assembly for the Federation which shall consist of a Senate and a House of Representatives.*
>
> *S48 - The Senate shall consist of three Senators from each State and one from the Federal Capital Territory, Abuja.*
>
> *S49 - Subject to the provisions of this Constitution, the House of Representatives shall consist of three hundred and sixty members representing constituencies of nearly equal population as far as possible, provided that no constituency shall fall within more than one State.*

The Senate is one of the chambers in Nigeria's bicameral legislature, the National Assembly. The National Assembly (NASS) is the nation's highest legislature, whose power to make laws is summarised in the 1999 Nigerian Constitution (National Assembly, 2017a).

According to Adebusiyi (2008), the legislative arm of the Nigerian government is saddled primarily with the responsibility of law making and must be committed enough to adopt appropriate legislation against the misuse of ICT for criminal purposes and activities which have a negative impact on integrity of national critical infrastructure. Abdulfatai (2017) argues that there exists a connection between the extent to which cybercrimes can be prevented in a country with adequate and effective cybercrime legislation. According to McConnell (2000), National Government remains the key authority for regulating criminal behaviour in most places in the world. The National Assembly of Nigeria has a vital role to play in preventing the threat posed by cybercrime, therefore, it is required of the National Assembly of Nigeria to legislate upon illegal interception, illegal access, computer related forgery, misuse of devices, offences related to child pornography and all other offences related to cybercrime (Abdulfatai, 2017).

2.7.6 National Crimes Agency (NCA)

The National Crime Agency, also known as the NCA, is a law enforcement agency responsible for leading the UK's fight to cut serious and organised crime (UK Government, 2017). The National Crime Agency of the UK tackles serious and organised crime, protects the UK border, fight fraud and cybercrime, and protect children and young people from sexual abuse and exploitation (NCA, 2017b).

The National Cyber Crime Unit (NCCU) of the NCA leads the UK's response to cybercrime, supports partners with specialist capabilities and coordinates the national response to the most serious of cybercrime threats. The NCCU works closely with the Regional Organised Crime Units (ROCUs), the MPCCU (Metropolitan Police Cyber Crime Unit), partners within Industry, Government and International Law Enforcement. Some of the Functions of the NCCU are as follows:

a) Providing a powerful and highly visible investigative response to the most serious incidents of cybercrime by pursuing cyber criminals at a national and international level.
b) Working proactively to target criminal vulnerabilities and prevent criminal opportunities.
c) Assisting the NCA and wider law enforcement to pursue those who use the internet or ICT for criminal purposes.
d) Directing a step-change in the UK's overall capability to tackle cybercrime, supporting partners in industry and law enforcement to better protect themselves against cybercrime (NCA, 2017a).

2.7.7 West Yorkshire Police Force

West Yorkshire Police is the territorial police force responsible for policing West Yorkshire in England. It is the fourth largest force in England and Wales by number of officers, with 5,671 officers (West Yorkshire Police, 2017c). West Yorkshire Police serve approximately 2.2 million people living in one of the five metropolitan districts of Bradford, Calderdale, Kirklees, Leeds and Wakefield. The physical area, of some 780 square miles, contains the West Yorkshire conurbation and a network of motorway and trunk roads which allow easy access to and from other population centres (West Yorkshire Police Force, 2017a). West Yorkshire Police is one of the few police forces across the UK that has a dedicated cyber unit (West Yorkshire Police, 2017b)

2.8 Critical Assessment

The stakeholders selected all play a major role in investigating and policing cybercriminals in Nigeria. The researcher narrowed down the selection of the stakeholders based on the following sampling as detailed in section 5.12.4.5.1. Furthermore, based on the researchers' previous professional experience, there is a lack of information sharing mechanism between the key stakeholders within the criminal justice system in Nigeria. Also, within organisations that are engaged in the investigation of cybercrime in Nigeria, there is lack of synergy between the investigative, legal and forensics department in conducting a thorough and scientific—based investigation. These factors amongst others have made investigating cybercrime cumbersome.

2.9 Conclusion

In conclusion, the chapter gave an overview of policing crime and cybercrime in Nigeria. It also enumerates the roles of the selected participants in the research, while giving a detailed overview of the various departments and units of the EFCC.

Table 2.4 showing the research objective that was achieved by the researcher.

S/N	RESEARCH OBJECTIVE	ID	OBJECTIVE ACHIEVED
1	To examine the different roles played by members of the Cybercrime Advisory Council (CAC) in tackling cybercrime in Nigeria through review of relevant literature and interviews.	**OBJ1**	**YES**

Table 2.4: Chapter 2 achievement of research objective

CHAPTER 3: LITERATURE REVIEW

3.1 Introduction

The literature review includes a comprehensive review of the different definitions of cybercrime, explores the Nigerian cybercrime phenomenon and the role law enforcement agencies are playing in curtailing the activities of cybercriminals. It also compares current laws, legislation and policies governing cybercrime in the UK with those in place in Nigeria.

3.2 Crime and Cybercrime

Pati (2003) argues that 'cybercrime' is a misnomer and the concept of cybercrime is not different from the concept of conventional crime as both include an act or omission which causes a violation of law.

3.2.1 Definition

Crime is a legal wrongdoing that can subsequently be followed by criminal proceedings which may eventually lead to punishment (Williams 2001 cited in Pati 2007).Cybercrime is defined as the use of electronic devices or computers via information systems to facilitate illegal activities (McQuade 2006, p. 2). The Association of Chief of Police Organization (2009) defines cybercrime as "the use of networked computers or internet technology to commit or facilitate the commission of crime" (ACPO 2009).The absence of a consistent current definition amongst law enforcement agencies mandated to tackling the cybercriminals is one of the major problems of cybercrime (NHTCU/NOP 2002:3). Wall (2002:2) argued that the term 'has no specific referent in law', still it has dominated the political, criminal justice, public and academic discourse of many nations.

3.2.2 Scope and Framework

The Council of Europe (2001) Convention on Cybercrime is the first international agreement on crimes committed through the use of the Internet and other computer networks. It includes infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains series of powers and procedures such as the search of computer networks and interception. The Council of Europe Convention on Cybercrime differentiates between four types of offences, namely:

1. Offences against the confidentiality, integrity and availability of computer data and systems

2. Computer – related offences
3. Content-related offences; and
4. Copyright-related offences

This categorisation is not based on any predefined concept of cybercrime; however, it does serve to demonstrate how different organisations and conventions categorise the activities of cybercrime. Pati (2007) categorises cybercrime by focusing on entities that are victims of activities of cybercriminals.

S/N	GROUPS TARGETED	TYPE OF CRIME
1	**AGAINST INDIVIDUAL**	Harassment via emails, cyber-stalking, dissemination of obscene material, defamation, hacking/cracking and indecent exposure.
2	**AGAINST INDIVIDUAL PROPERTY**	Computer vandalism, transmitting virus, netrespass, unauthorized control over computer system and hacking/cracking.
3	**AGAINST ORGANIZATIONS**	Hacking/cracking, possession of unauthorized information, cyber terrorism against the government organization and distribution of pirated software, etc.
4	**AGAINST SOCIETY**	Pornography (basically child pornography), corrupting the youth through indecent exposure; and trafficking

Table 3.1: Groups Targeted by Cybercrime Activities (Pati 2007)

Alternatively, McGuire & Dowling (2013a, 2013b) differentiates cybercrime as either cyber-enabled or cyber-dependent crime. They define cyber-enabled crime as traditional crimes which can be increased in their scale by use of computers or other form of ICT; while cyber-dependent crimes are offences that are solely committed using a computer, network or other form of ICT. However, Wall (2005) argues that the impact of the internet on crime is varied and requires further understanding whilst admitting that many so called cybercrimes appear as traditional crimes which already fall within the penal code of many criminal justice systems. However, he further argues that, in order to fully understand cybercrime, he puts forward a matrix of deviant behaviours that fall under 'the rubric of cybercrime'.

Table 3.2 shows the matrix developed by Wall (2003) in understanding the impact of the internet on criminal opportunities and behaviors.

OPPORTUNITIES	CRIME TYPES		
	CRIME AGAINST MACHINE	**CRIME USING MACHINES**	**CRIMES IN THE MACHINE**
	Harmful; Trespass	**Acquisition/Theft/Deception**	**Obscenity/Violence**
CYBER-ASSISTED – Traditional crime using computers. More opportunities for traditional crime	1. Phreaking; 2. Chipping	3. Frauds 4. Pyramid Schemes	1. Trading sexual materials 2. Stalking 3. Harassment (personal)
CYBER-ENABLED – Hybrid cybercrimes. New opportunities for traditional crime (e.g., organisation across boundaries)	1. Cracking/Hacking; 2. Viruses; 3. Hacktivism	1. Multiple large-scale frauds 2. 419 type fraud 3. Trade secret theft 4. ID Theft	1. Online sex trade 2. Camgirl sites 3. General hate speech 4. Organized pedophile rings (Child abuse)
CYBER-DEPENDENT – True Cybercrime. New opportunities for new types of crime (Sui Generis)	1. Spams; 2. Denial of service; 3. Information warfare, 4. Parasitic computing	1. Intellectual property 2. Piracy distribution 3. E-auction scams 4. Phishing, smishing, vishing	1. Cyber-sex 2. Cyber-pimping 3. Online grooming 4. Organised bomb talk/Drug talk 5. Targeted hate speech 6. Social network media crimes

Table 3.2: Mapping out Cybercrimes in a cyber-spatial surveillant assemblage (Wall, 2003)

Wall's (2003) mapping of cybercrime is applicable to understanding cybercrime in Nigeria. Most cybercrimes committed in Nigeria are cyber-enabled crimes either using a machine to commit a traditional crime (i.e. 419) or against a machine such as hacking. The map also aligns with the research scope of cyber-enabled crime of advance fee fraud commonly known as '419'.

However, the UK Government National Cyber Security Strategy (2016) deals with cybercrime in the context of two interrelated forms of criminal activity namely cyber-dependent and cyber-enabled crimes. Cyber-dependent crimes are committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime while cyber-enabled crimes are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

3.3 Overview of Cybercrime in Nigeria

Cybercrime in Nigeria can be defined as computer-enabled crime originating from Nigeria and is classified into three categories (WITFOR 2005):

1. Computer-aided crime perpetrated by Nigerians locally and internationally
2. Crimes perpetrated against Nigerian information and telecommunication resources.
3. Computer-aided crime committed by Non-Nigerians giving the similarities of a "Nigerian" origin (WITFOR, 2005).

Longe and Chiemeke (2008) argue that the first category is crimes committed daily with the aid of the internet through sending fraudulent and fictitious financial proposals around the world. This set of criminal activity is tagged as "419 scammers". Ribadu (2007) further argues that the second category which is crime perpetrated against Nigerian Information and telecommunications is related to mail scam, credit card fraud and insurance fraud. The third category are cybercrime activities committed by Non-Nigerians but made to look like '419' crimes. Amongst them are cybercrime activities originating from Cameroun which seems to have a high prevalence of cybercrime in Central Africa (Akuta, Ong'oa & Jones, 2011).

3.3.1 Statistics of Cybercrime in Nigeria

According to the Internet Crime Complaint Center (2016) annual report on internet crime, Nigeria is currently ranked 18th in the world in terms of complainant reporting of cybercrime and ranked 12th in terms of complainant loss. This is seen as an improvement to an earlier Internet Crime Report (2010) that ranked Nigeria third at 5.8% just behind United State of America with the highest prevalence of cybercrime activities in the world. According to the Internet World Stats (2016) report, Nigeria has a population of 185 million of which 97 million are Internet users representing 52% internet penetration.

Figure 3.1 shows an overview of digital statistics in Nigeria.

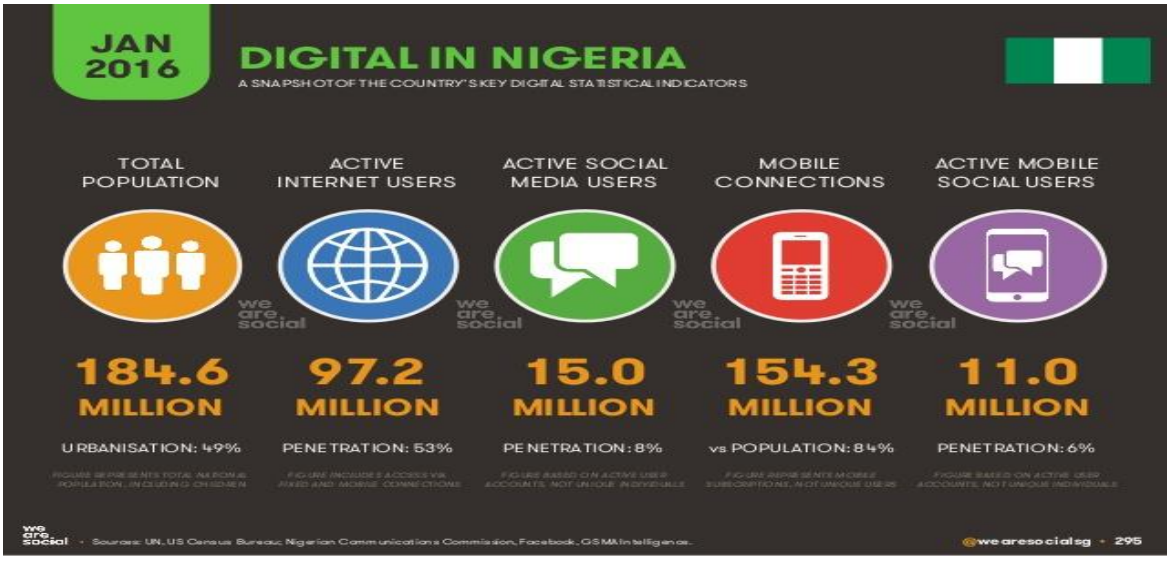


Figure 3.1: Overview of Digital Statistics Indicators in Nigeria (We Are Social, 2016)

Figure 3.1 shows the following digital indicators in Nigeria. Such indicators are: total population of 184.6 million; active internet users of 97.2 million; active social media users of 15 million; mobile connections of 154.3 million; and active mobile social media users of 11 million (We Are Social, 2016).

3.3.2 Socio-Economic Effects of Cybercrime

Cybercrime has had a negative impact on the Nigerian economy; it has the potential to adversely impact on technological growth within the country which is intended to be a stepping stone to improving productivity and socio-economic growth for the following reasons:

a. International financial institutions consider paper-based Nigerian financial instruments with suspicion making Nigerian bank drafts and checks not viable international financial instruments.
b. Nigerian Internet Service Providers (ISPs) are regularly being black-listed in e-mail blocking blacklist systems across the cyberspace.
c. Some companies and businesses are blocking entire Internet network segments and traffic that originates from Nigeria,
d. Newer and more sophisticated technologies are gradually emerging and that makes it convenient to isolate Nigerian e-mail traffic.
e. Key national infrastructure and information security assets are more prone to be compromised or damaged by unauthorized users. (WITFOR 2005)

3.3.3 Financial Costs

Sesan et al. (2012) in a survey conducted and titled 'Economic Cost of Cybercrime in Nigeria', stated that cybercrime cost the Nigerian consumers approximately $13.5 billion dollars in 2012.

Ribadu (2007) argued that cybercrime had a monumental impact on the Nigerian economy. Between 2003 and 2007, the Nigerian government, through the Economic and Financial Crimes Commission (EFCC), stopped cybercrime transactions worth £300 million, €200 million, and $500 million respectively. According to WITFOR (2005), Nigerian Cybercrime can be understood by considering the following statistics:

a. Annual global loss of $1.5 billion in 2002
b. 6% of global Internet spam in 2004
c. 15.5% of total reported FBI fraud in 2001
d. Highest median loss of all FBI Internet fraud of $5,575
e. VeriSign, Inc., ranked Nigeria 3rd in total number of Internet fraud transactions accounting for 4.81% of global internet fraud.
f. American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up 900% in 2001
g. American National Fraud Information Centre also ranked Nigeria money offer as 3rd largest fraud in 2002; at 4%, Nigerian Cybercrime impact per capita is exceptionally high.

3.4 Advance Fee Fraud (AFF)

Advance Fee Fraud or '419' fraud (a name coined from a section of the Nigerian Criminal Code) is a prevalent crime within the West African organized criminal networks. There are many variations of the scheme and scams which are designed to get recipients/victims to part with their money (Stevens 2006). The Criminal Code Act (1990) defines advance fee fraud through section 419 as:

> *Any person who by any false pretence, 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 is liable to imprisonment for three years.*

3.4.1 Historical Background

AFF letters and faxes are confidence trick schemes and mostly come as proposals from purported Nigerian government 'officials', companies or contractors. AFF letters first gained prominence in the mid-1980s around the time of the collapse of world oil prices, which is the main foreign exchange earner for the Nigerian government (US Department of States, 1997). However, according to Ultrascan AGI (2014), Nigerian 419 advance fee fraud came to the attention of the general public and regulators during the 1970s in relation to letters mostly aimed at small businesses claiming to come from two Nigerian government offices, namely the Central Bank of Nigeria and the Nigerian National Petroleum Corporation.

During the 1980s and 1990s, 419 scammers moved away from letters to fax messaging and following the explosion of the Internet in Nigeria in 2003, emails became the preferred method of communication for cybercriminals (Ultrascan, 2014).

3.4.2 Variations of AFF Scams

Tive (2006) argued that advance fee fraud (AFF) was the most common type of transnational '419' scam. AFF comes in various forms but the similarity between all variants is the demand of an advance fee. There are six major ways by which AFF operates and, in each case, the victim is asked to pay some advance fee for the transfer of money.

a. Families (widows, sons, brothers) of former West African Presidents, military generals and politicians looking for assistance to transfer money inherited by them.
b. Heads of government agencies (Central Bank of Nigeria, Debt Management Office, Nigerian Mining Corporation, Nigerian National Petroleum Corporation etc.) that have over-invoiced contracts and need assistance from a foreign partner to move the money out of Nigeria.
c. Bank accounts abandoned by wealthy businessmen who died in an accident and the need for someone to pose as the relative of the deceased to claim the money.
d. Stolen assets deposited in a security company that need to be transferred out of the country immediately.
e. Donations made to charitable or religious organisations where the beneficiary needs the service of an attorney to claim their money.

f. Deceased religious leader or philanthropist who has bequeathed his/her wealth to a church in America or Europe (Tive, 2006).

However, Stevens (2006) argues that there are other variants of AFF such as counterfeit cheques, contract fraud, auto scams, magic money, fake lottery wins and phishing amongst others.

3.4.3 Limitations to AFF Investigation

Tive (2006) pointed out that, prior to the establishment of the Economic and Financial Crimes Commission (EFCC), the Nigerian Police Force (NPF) was the government agency mandated to investigate and prosecute 419 offenders. Some of the limitations encountered by law enforcement when investigating advance fee fraud include:

a. Lack of admission by victims that they have been defrauded.
b. Victims do not want to travel to Nigeria to serve as prosecution witness against offenders.
c. Generally, victims do to want to pursue the suspected fraud legally in a court system.
d. Investigation of advance fee fraud cases requires expert knowledge on the use of modern computers. The fraudsters are aware of the low computer literacy level of the police; therefore, they know they cannot be caught.

3.5 Causes of Cybercrime in Nigeria

Technological advances in the global telecommunication infrastructure, including computers, mobile devices and the internet, have brought about significant transformation in the world of communication. In Nigeria, people of different ages and economic demographics have used the internet to communicate and access information easier and faster. However, one of the fall-outs of this unlimited access is the issue of cybercrime (Adesina, 2017). Africa has seen a phenomenal growth in Internet connectivity in recent years and also a high potential for cybercrime which is greater in that continent than elsewhere. In trying to understand why cybercrime is more prevalent in Africa, Oluwu (2009) argued that many African countries were contending with high unemployment rates and the problem of cybercrime was, thus, expected to continue unabated unless the issue of unemployment was comprehensively addressed. Oluwu (2009) further argued that information security awareness was lacking among internet users of private and public organisations, thus, making it rather difficult to combat cybercrime in many African countries. Another issue that contributed to the high prevalence of cybercrime in Nigeria

was greed and the uncontrollable desire for massive wealth (Olusola, Samson, Semiu and Yinka, 2013b). Weak implementation of cybercrime laws and inadequately equipped law enforcement agencies has made cybercrime a regular occurrence within the Nigerian cyberspace (Hassan, Lass and Makinde, 2012).

3.5.1 Unemployment and Poverty

Cybercrime in Nigeria can be associated with the high rate of unemployment, harsh economic situations and an ineffective educational system (Hassan, Lass and Makinde, 2012). The issue of poverty in Nigeria is a paradox because the country is a leading oil-producing nation and rich in various natural resources, yet most of the citizens are economically poor. About one third of Nigerians (35%) live in extreme poverty while about 54% are relatively poor, which means more than half of the Nigerian population lives on less than a dollar a day (Adesina, 2017). Statistics have further shown that unemployment is very high among youths, most of whom are university graduates with computer and internet competency (Olowu, 2009). These unemployed youths, according to Adesina (2017), have time on their hands and have easy access to the internet to commit cybercrime. Even when they do not have access to the internet at home, cybercafés are readily available throughout the country at relatively low rates for internet access.

3.5.2 Greed and Financial Gain

Another major cause of cybercrime in Nigeria is the quest for ill-gotten wealth that is exacerbated by an existing large gap between the rich and the poor. With high unemployment rate, many youths are looking for means of making money easily with minimal risk and cybercrime offers them that avenue (Hassan, Lass and Makinde, 2012). Adesulu (2017) has described cyber criminality and cyber victimization as crimes tied to the exploitation of human frailties such as greed, gullibility and the untamed quest for getting rich syndrome and not crimes that are necessarily influenced by social factors such as poverty and unemployment. Most people that are involved in cybercrime is not because they do not have what it takes to live a normal life but because they are never contented with what they have and desire to have quick money without going through the right process of acquiring wealth (Jacinta, 2017).

3.5.3 Lack of Awareness

The lack of cybersecurity awareness in Nigeria is one of the major causes of cybercrime because it has made it easy for fraudsters to operate leading to huge financial losses and a negative impact on the credibility and reputation of the country (Odumesi, 2015). Oluwu (2009) further argues that information security awareness is crucial to tackling cybercrimes and that, in contrast to Europe and the US, there is a significant lack of security awareness among users in Africa. This lack of awareness is also a major problem for ICT companies operating in Africa as most decision makers in Africa are not aware of the cybercrime problem.

3.5.4 Regulation and Enforcement

According to Odumesi (2006), the problems faced by law enforcement agencies in tackling the activities of cybercriminals in Nigeria are as follows:

a) The lack of a national internet gateway for Nigeria has made it difficult to identify and isolate the real activities of cybercriminals attributable to Nigeria on the internet.
b) Nigerian law enforcement agencies do not have a centralized government body that collects and publishes cybercrime statistical reports.
c) The lack of adequate data on the level and extent of cybercrime damages in the country.
d) The Nigerian law enforcement agencies are not computer literate and lack a basic computer forensic laboratory within any branch of the Nigerian Police or other law enforcement agencies to investigate and analyse cyber related offences.

Therefore, the lack of regulation invariably means the lack of law enforcement training, tools and techniques to investigate cybercrimes. Also, most African countries, including Nigeria, do not have specific laws for cyber-based intellectual property violations (Olowu, 2009). The lack of enforcement of some fragile laws regarding cybercrime is prevalent in Nigeria and most law enforcement agencies lack the sophisticated hardware tools to track down an online criminal (Hassan, Lass and Makinde, 2012).

3.5.5 Reliance on ICTs

The interaction of people and business relies on ICTs and internet-based services for communication. Growing reliance on ICT platforms makes systems and services more prone to attack against critical infrastructure (ITU, 2012). As the web has become important to our daily

transactions, it has also negatively attracted criminals to perpetuate their activities. The web offers these criminals a power platform to compromise ICT systems and 'monetize the resulting computing resources as well as any information that can be stolen from them' (Provos, Rajab & Mavrommatis, 2009). This compromise of systems even for a short interruption to services could cause huge financial loss to mostly e-commerce businesses. Also, existing ICT infrastructure has a number of known weaknesses which an offender can use to attack and cause damages. Also, with the growing number of people connected to the internet, the number of targets and offenders increase, thus, making it difficult for law enforcement agencies to investigate (ITU, 2012).

3.6 Limitations to Tackling Cybercrime

Cybercrime has evolved over the years with recent development in ICT resulting in newer cybercrime methods. However, advances in ICT have greatly expanded the capabilities of law enforcement agencies in adopting new methods of investigating cybercrime. Even though criminals may use new tools to prevent LEAs from conducting their work, it is important for police to expand their technical capabilities (ITU, 2012).

3.6.1 Internet Usage and Population

According to the Internet World Stats (2016), as of June 2016, the world internet population is more than 7.3 billion users with about 1.6 billion users actively using Facebook, the popular social media site. As the usage of the internet increases, especially in developing countries, the number of targets and offenders increases daily. It is difficult to estimate how many users of the internet do so for illegal activities (UNODC, 2013). In Nigeria, according to the Nigerian Communications Commission (2016) subscriber statistics, about 153 million mobile lines are connected with about 93 million actively using the Internet. Despite the internet's potential to drive growth and the global economy, it has continued to provide criminals with an avenue for damaging Nigeria's reputation. Advance Fee Fraud and cybercrime continue to dominate the crime scene in the war against economic and financial crimes in Nigeria.

3.6.2 Technology and Training

Chukkol (cited in Barnard, 2014) states that Nigeria has seen a transition in how crimes are evolving at a greater speed with criminals embracing ICT to commit crimes. Smith (2003) argues

that the investigation of cross-border cybercrime requires the adequate technical and forensic skills and knowledge. Other areas enumerated by Smith (2003) that need improving include:

a. Formulation of training programs and the development of investigative software tools
b. International training programmes should be developed and expertise shared between different nations.
c. The level of funding required for training and up-grading Equipments is inadequate.
d. Need for greater information sharing between investigators both within the public and private sectors.

3.6.3 Laws and Jurisdiction

Adequate and proper legislation is the bedrock for the investigation and prosecution of cybercrime. However, law-makers must continuously respond to ICT and internet development so as to measure the effectiveness of existing laws and provisions (ITU, 2012). With the exception of Europe and America that have sufficient investigative powers to prosecute cybercrime, the rest of the world has insufficient investigative powers (UNODC, 2013).

According to the ITU Report (2012), challenges in drafting national criminal laws to prosecute new forms of cybercrime takes time and some countries are yet to make the necessary adjustments. The report proposes the following three steps in the adjustment process:

a. Adjustments to national law must start with the recognition of an abuse of new technology
b. Identification of gaps in the penal code
c. Drafting of new laws and legislation.

Smith (2003) states that the harmonization of laws and the adoption of international conventions on cybercrime will make prosecution easier and will greatly improve the mutual assistance and extradition of criminals between countries.

3.6.4 Education and Awareness

Dix (2017) argued it is important for all digital users to practice basic cybersecurity hygiene to improve their own protection. He states that, about 80 percent of exploitable vulnerabilities online are due to ‘poor or non-existent cyber hygiene. Odumesi (2015) maintains, cyber risk

increases without the proper precautions to protect personally identifiable information on the cyberspace. He further stated that, Nigerian online users are highly vulnerable to cyberattacks because the lack of cybersecurity awareness had made it easy for cybercriminals to operate. However, according to Kortjan and Solms (2014), most users lack awareness and knowledge, therefore, they are ignorant of properly protecting their personal and confidential information. Also, they argued that the user's insecure online behaviours make them vulnerable to be exploited by the cybercriminal.

3.7 Nigerian Government Efforts in Combating Cybercriminals

According to Adomi and Igun (2008), the Nigerian Government had to take drastic measures in order to curtail the activities of cybercriminals. Due to the negative financial and economic consequences of cybercrime in Nigeria, the government pursued the following efforts:

e. Creation of a central agency to enforce criminal laws
f. Regulation of cybercafés
g. Enactment of Cyber laws
h. Government partnership with Microsoft

The WITFOR Report (2005) shows that the Nigerian government set up a Presidential Committee on cybercrime to examine the root causes and proffer solutions in order to tackle the problem. The committee report recommended the creation of a legal and institutional framework to tackle cybercrime in Nigeria. The creation of a central agency to enforce cybercrime laws in the country was the main theme of the report which subsequently led to the creation of the Nigerian Cybercrime Working Group (NCWG) in 2004 (WITFOR 2005).

3.7.1 Nigerian Cybercrime Working Group (NCWG)

The main aim of the NCWG was to develop appropriate legal and institutional frameworks in securing the Nigerian cyberspace (Adomi and Igun, 2008). The NCWG is an inter-agency consisting of most relevant law enforcement, security, intelligence, ICT Agencies of government and major private organizations in the ICT sector. Some of these agencies include the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), the National Security Advisor (NSA), Nigerian Communication Agency (NCC), Internet Service Providers' Association of Nigeria (ISPAN), Nigeria Computer Society (NCS), Department of State Services

(DSS), National Intelligence Agency (NIA), Nigeria Internet Group (NIG), National Information Technology Development Agency (NITDA) and individual citizens representing public interest. The duties of the NCWG include:

1. Engaging in public enlightenment programme
2. Building institutional consensus amongst existing agencies
3. Providing technical assistance to the National Assembly on cybercrime and the drafting of cybercrime act
4. Creating the framework for a cybercrime agency that will eventually emerge to take charge in tackling cybercrime in Nigeria
5. Collaborating with global cybercrime enforcement agencies in the USA, UK and other countries who are at the forefront of fighting cybercrime (WITFOR 2005).

3.7.2 Regulation of Cybercafés

Eyitemi (2011) argues that cybercafés have become an integral part of the business and social environment in Nigeria. Cybercafés are places where internet services are readily available for a fee and are the most popular place for people to access the internet in Nigeria. Adomi and Igun (2008) state that cybercafés in Nigeria facilitate overnight browsing that allows internet users to use the cafes from 10:00pm to 6:00am.

However, the Economic and Financial Crimes Commission (EFCC) and the Association of Cyber Café and Telecentre Owners (ATCON) banned night browsing in all the internet cafes in Nigeria (Nkanga, 2006). This was due to the daily embarrassment caused to the Nigerian government by certain activities of cybercriminals in the cybercafés. Nkanga (2006) argued that Nigerian cybercriminals had perfected the art of using the cybercafés as a platform to defraud unsuspecting people across the globe.

The ban according to the ATCON President was in compliance with the Telecommunication Act (2006) which transferred the policing of cyber-crimes to telecommunication operators and empowered the EFCC to enforce its provision. Other decisions of EFCC and ATCON to combat cybercrime included:

a. All Cybercafés must be registered with the Corporate Affairs Commission, Nigerian Communication Commission (NCC) and EFCC.

b. All the telecommunications companies, namely the global system for mobile communication operators, private telecommunication operators and cybercafés should ensure that they come up with a due diligence document that would be a standard guide and proffer measures for the effectively checkmating cybercrime in Nigeria.
c. Cybercafés will now be run on a membership basis instead of on a pay-as-you-go basis.
d. Cybercafés must install acceptable hardware surveillance to monitor fraudulent activities.
e. The physical architecture of cybercafés must be framed in such a way that all computers are visible at all times.
f. ATCON members must subscribe to registered and licensed Internet Service Providers (ISP) in the country, and
g. All cybercafés are expected to be a watchdog to others, as they have been given direct access to EFCC (Nkanga 2006).

3.7.3 Enactment of Cyber Laws

McQuade (2006, p. 273) maintains that 'laws and regulations are extremely important' because it affects most areas in criminal justice administration and assist in the effective management of data, information systems and critical infrastructures of any nation.

Ehimen and Bola (2010) argued that, as of the year 2010, the Nigerian government did not have a specific law to tackle the menace of cybercriminals. Therefore, the government has relied on existing laws that could be used to deal with the issue of cybercrime.

However, over the years, the Nigerian government enacted various laws and policies for the sole purpose of curtailing the activities of organised criminals and prosecuting the offenders of these laws. Such laws included the Criminal Code Act, Economic and Financial Crimes Commission Act (2004), Advance Fee Fraud and other Fraud Related Offences Act (2006) (Chawki, Darwish, Khan and Tyagi 2015).

In 2015, the Cybercrime Prohibition, Prevention (2015) Act was signed into law. Paul (2015) argues that the Act was passed into law to bring about sanity in the cyberspace of Nigeria.

3.7.3.1 The Criminal Code Act

The Nigerian Criminal Code is one of the laws inherited from the British during the colonial rule and it predates the advent of the internet and cyber era making it inadequate for addressing complex issues related to cybercrime (Oriola 2005). Cybercriminals in Nigeria are known as '419 scammers'; a word coined from the Criminal code that penalises people for obtaining money under false pretences (Sesan et al. 2013)

The Criminal Code Act (1990) defines 'false pretence' under section 418 as follows:

> *Any representation made by words, writings, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.*

Chawki et al. (2015) argues that under the Nigerian Criminal Code, Advance Fee Fraud qualifies as false pretence while an internet scam would amount to a crime under section 419 of the Criminal Code. Section 419 of the Criminal Code states that:

> *Any person who by any false pretence, 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 is liable to imprisonment for three years*

Due to the inadequacies of the Criminal code to tackle activities of the cybercriminals, Oriola (2005) argued that the Act had many limitations. He further categorised the limitations as follows:

1. The Act mentions that a suspect cannot be arrested without a warrant, unless found committing the offence. This provision makes it difficult for law enforcement agencies to effectively monitor and arrest a suspect when the offence is being committed because most of the fraudulent emails are sent from internet cafes.
2. The second drawback in the Act is the lack of harsh penalties to serve as deterrence to crime. An offender found guilty, is liable to just three or seven years imprisonment. Considering the huge amount of money fraudulently obtained from victims, the punishment is minor in comparison with the magnitude of the crime.
3. The third limitation of the Act is the lack of restitution for the victim of the crime. This is because in a Nigerian court, the government is the complainant and any compensation to the victim is difficult to be prosecuted in a criminal code unless the victim goes through the civil courts.

3.7.3.2 Economic and Financial Crimes Commission (Establishment) Act 2004

The Economic and Financial Crimes Commission (2004) Act was a renewed effort by the Nigerian government to tackle the embarrassment caused by fraudulent email scams that have emanated from the country (Oriola 2005).

The Economic and Financial Crimes Commission (Establishment) Act 2004 was adopted in 2004, thus repealing the EFCC Act of 2002. The EFCC was established with the responsibility for the enforcement of all economic and financial crimes (Chawki et al. 2015).

Obuah (2010) states that, the EFCC also serves as Nigeria's designated Financial Intelligence Unit (NFIU) and is charged with 'preventing, investigating, prosecuting, and penalising financial and economic crimes such as illegal oil bunkering, terrorism, capital market fraud, cybercrime, advance fee fraud (419 or obtaining through different fraudulent schemes), banking fraud and economic governance fraud'.

Amongst the functions of the EFCC as stated in Section 6b Part 2 under the Functions of the Commission states are as follows:

> *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, contract scam, etc.* (EFCC Act 2004)

The Commission also has special powers as enshrined under Section 7 of the EFCC Act (2004), which states that it can:

> *Cause investigations to be conducted as to whether any person, corporate body or organization has committed any offence under this Act or other law relating to economic and financial crimes.*

Section 46 of the EFCC Act (2004) defines economic and financial crimes as follows:

> *The non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug, trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labor, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc.*

Section 7 subsection 2 (f) also makes the EFCC the coordinating agency for the enforcement of many provisions such as the Criminal Code and the Penal Code (EFCC Act 2004).

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

The Advance Fee Fraud Act 2006 was a deliberate and concerted effort by the Nigerian government to tackle effectively the menace of advance fee scams. Due to the inadequacies of the Criminal Code Act to govern the cyber space, the government needed a law to plug any loopholes in the previous laws (Oriola 2005).

Section 20 of the AFF Act (2006) defines false pretence as:

> *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.*

According to Chawki et al. (2015), the AFF Act mandates not only government to carry out surveillance of alleged criminal behaviors but also gives critical stakeholders within the industry such as ISP and cybercafé operators some responsibilities.

Section 13 of the AFF Act (2006) clearly outlines the duties of telecommunication, ISPs and internet cafes in relation to the enforcement of the AFF Act. It states that any person or entity that provides telecommunication services or internet services must be registered with the EFCC and maintain an updated record of all fixed lines and GSM records. This record should be made readily available to EFCC on demand.

Furthermore, Section 1 through to Section 10 highlights the various offences and their penalties under the AFF Act. While Section 1 of the AFF Act (2006) penalises any person that 'obtains property' through false pretence to an imprisonment of not more than 20 years but not less than 7 years without an option of fine; Section 2 of the Act broadens the scope of the offences to cover people that claim to print fake currency, or have special powers of doubling money or claims to the 'Central Bank of Nigeria' and capable of printing currency notes are all liable upon conviction to a term of not more than 15 years and not less than 5 years without the option of a fine. Table 3.3 summarises the offences and their relevant penalties under the AFF Act 2006

S/N	ACT	SUMMARY OF ACT		
1	**AFF ACT 2006**	The Act to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences. Offences such as Advance Fee Fraud, cybercrime, 419 scams, securities and monetary scams etc.		
	PART 1: OFFENCES			
	SECTIONS	**TITLE OF SECTIONS**	**SUMMARY**	**PENALTIES**
	Section 1	Obtaining Property Under False Pretence Etc.	Any person who by false pretence & intend to defraud: obtains, induces any person in Nigeria or abroad in order to confer benefit has committed an offence.	Sec 1 (3): Person is liable on conviction to imprisonment of not ≥ 20yrs & not ≤7yrs without option of fine
	Section 2	Other Fraud Related Offences	Any person that (a) falsely misrepresent, (b) claims to possess special powers, make s or (c) not been CBN issues currency note commits an offence.	Sec 2 (c):Person is liable on conviction to imprisonment for a term not ≥ 15yrs & not ≤ 5yrs without option of fine
	Section 3	Use of Premises	Any person that knowingly allows his/her property to be used to commit a crime under this Act has committed an offence.	Sec 3: Person is liable on conviction to imprisonment for a term not ≤ 15yrs & not ≥ 5yrs without option of fine
	Section 4	Fraudulent Invitation	Any person with intention to commit fraud invites any person to Nigeria has committed an offence.	Sec 4: Person is liable on conviction to imprisonment of not ≥ 20yrs & not ≤7yrs without option of fine
	Section 5	Receipt of Fraudulent Document by Victim to Constitute Attempt	Where a false pretence is contained in a document, it is enough to charge an individual for attempt to commit an offence.	Not Applicable
	Section 6	Possession of Fraudulent Document to Constitute Attempt.	A person in possession of a document containing false pretence has equally committed an offence under the Act.	Not Applicable
	Section 7	Laundering of Funds Obtained through Unlawful Activities, etc.	Specifies the diff. categories of what constitutes laundering of funds though illegal activities, transportation of illegal funds and lack of adherence to BOFIA and MLA Act among others	Imprisonment varies from 3 years to 10 years and fine varies from N100K to N1 million Naira depending on individual or corporate body
	Section 8	Conspiracy, Aiding, etc.	A person who conspires, abets, aids or incites, procures any person has committed an offence as prescribed under the Act	Not Applicable
	Section 9	Conviction for alternative offence	A person can be convicted solely on attempted to commit an offence if the evidence is established against him/her.	Not Applicable
	Section 10	Offences by Corporate Bodies.	A corporate body either through neglect of a director, manager or secretary is proved to have committed an offence under this Act shall be punished accordingly and if convicted in a High Court, all its assets and properties forfeited to the FGN.	Not Applicable

(Adopted from Advance Fee Fraud and other Fraud Related Offences ACT 2006)

Table 3.3: Offences and Penalties under the Advance Fee Fraud Act (AFF Act 2006)

3.7.3.4 Evidence Act 2011 (As Amended)

The Evidence Act (2011) was amended and passed into law by the President of the Government of Nigeria in order to address the inadequacies of the previous Act (Ajayi 2011). The most significant improvement of the new Act, as Oremewe (2011) argued, was the provision on the admissibility of electronically generated evidence. The repealed Evidence Act did not take into consideration the rapid development in the sector of information and communications technology, therefore, making it difficult to contemplate the admission of other evidence other than paper documents.

The Act defines a 'computer' under Section 258 as:

> *Any device for storing and processing information and any reference to information being derived from other information is a reference to its derived from it by calculation, comparison or any other process' (Evidence Act 2011).*

The Evidence Act (2011) under Section 84 provides for the admissibility of statements in documents provided by computers. Section 84 (1) states 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.*

In order for an evidence to be admissible under Section 84(1), it must satisfy the provisions of Section 84(2) which states as follows: the information must be derived from a computer; the computer must be working properly, amongst other conditions.

Section 258 of the Act has broadened the scope and definition of 'document' to make provision for modern technology. Oremewe (2011) argues that the definition was expanded in an attempt to legitimise the status of 'tapes, CDs, memory cards and other electronic storage media' to be recognised as documents. The definition covers four paragraphs in order to properly capture all the forms of documents admissible. The Act under Section 258 expands the definition of documents to include:

> *Any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it (Evidence Act 2011)*

3.7.3.5 Money Laundering (Prohibition) Act 2012 (As Amended)

The Money Laundering (Prohibition) Act 2012 amends the Money Laundering (Prohibition) Act 2011 to expand the scope of money laundering offences and to enhance customer due diligence measures. The Act seeks to make comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of crime or an illegal act. The Act also provides appropriate penalties and expands the scope of supervisory and regulatory authorities in order to curtail the challenges faced in the implementation of the various anti-money laundering regimes in Nigeria (Money Laundering (Prohibition) Act 2011).

Section 1 of the MLA Act 2011 provides for the limitation to make or accept cash payment. It states that:

> *No person or body shall, except in the transaction through a financial institution, make or accept cash payment of a sum exceeding – (a) N5, 000,000.00 or its equivalent, in the case of an individual; or (b) N10, 000,000.00 or its equivalent in the case if a body corporate.*

3.7.3.6 Cybercrimes (Prohibition, Prevention etc.) Act 2015.

The Cybercrime Act 2015 was signed into law to not only curtail the abuse of ICT for criminal purposes but to further checkmate the nefarious activities on telecommunication assets by vandals (Paul 2015).

Oke (2015) maintains that, prior to the enactment of the Cybercrimes Act 2015, the Economic and Financial Crimes Act 2004, Advance Fee Fraud and Other Fraud Related Offences Act 2006 and the Money Laundering (Prohibition) Act 2012 regulated cybercrime and activities of fraudsters in Nigeria. Due to the inadequacies of the provisions of the previous laws to regulate cybercrime, there was an urgent need to harmonize all the laws which produced the Cybercrimes Act 2015.

The Cybercrimes Act (2015) provides an 'effective, unified and comprehensive' regulatory, legal and institutional framework for the detection, prevention, prohibition and prosecution of cybercrimes in Nigeria. The Act further provides protection to critical infrastructure and promotes cybersecurity in order to protect computer systems and networks, electronic communications, intellectual property, and privacy rights amongst others.

The Cybercrime Act is categorized into 59 sections and 8 parts. It contains two schedules. The provision of the first schedule provides for members of the cybercrime advisory council. It mentions various Ministries, Departments, and Agencies (MDA) that constitute representatives to form the advisory council. The second schedule provides for the 'Establishment of National security fund' and how it should be operated (Oke 2015).

In terms of structure and content, Part 1 is on the objectives and application of the Act. Part 2 provides for the protection of critical national infrastructure. Part 3 deals with various cyber offences and penalties. Part 4 enumerates on the duties of financial institutions. Part 5 deals with the overall administration, enforcement and establishment of Cybercrime Advisory Council. Part 6 handles issues of arrest, seizure, search and prosecution. Part 7 highlights provisions for jurisdiction and international cooperation while Part 8 state miscellaneous provisions relating to regulations, interpretation and the citation (Cybercrimes Acts 2015). These sections are presented in Table 3.4

S/N	PART NO.	NAME	ITEMS
1	***PART 1***	**OBJECTIVES AND APPLICATION**	Objectives and Application of Act.
2	***PART 2***	**PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE**	Designation of computers as critical infrastructure (CI), audit and inspection of CI.
3	***PART 3***	**OFFENCE AND PENALTIES**	Computer fraud, cyber terrorism, cyber stalking, phishing, child pornography etc.
4	***PART 4***	**DUTIES OF FINANCIAL INSTITUTIONS**	Duties of Financial Institutions, Record retention, Interception etc.
5	***PART 5***	**ADMINISTRATION AND ENFORCEMENT**	Cybercrime Advisory Council, enforcement and powers of Council etc.
6	***PART 6***	**ARREST, SEARCH, SEIZURE AND PROSECUTION**	Power to arrest, search and seizure and forfeiture etc.
7	***PART 7***	**JURISDICTION AND INTERNATIONAL COOPERATION**	Jurisdiction, Extradition, Mutual Assistance, Contact point etc.
8	***PART 8***	**MISCELLANEOUS**	Resignations, Interpretation, Citation.

(Adopted from the Cybercrimes (Prohibition, Prevention Etc.) Act 2015)

Table 3.4: Selected sections of the Cybercrime Act 2015

PART 1: OBJECTIVES AND APPLICATION

Part one of the Cybercrimes Act (2015), presents the objective of the Act which provides for an effective and harmonized legal and regulatory institutional framework for the purpose of detecting, prohibiting, preventing and prosecuting cybercrime and cybercriminals in Nigeria. It also seeks to promote cybersecurity and protect critical national information infrastructure against vandals.

Oke (2015) argues that the provision of the Act provides for the Act to be applicable throughout the Federal Republic of Nigeria, thus, making it impossible for states to enact cybercrime laws as Section 4(5) of the Constitution of the Federal Republic of Nigeria, 1999 provides that where a law enacted by a state government through the State House of Assembly is inconsistent with any law enacted by the National Assembly; the law enacted by the National Assembly shall prevail over the State Assembly.

PART 2: PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Section 3 and 4 of the Act provides for the protection of critical national infrastructure. Section 58 of the Cybercrimes Act (2015) defines 'Critical Infrastructure' as 'systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country'. Paul (2015) argues that Nigeria has suffered frequently from the activities of vandals on its public infrastructure. Physical Infrastructure belonging to telecoms operators, Internet Service Providers (ISP) and power infrastructures have been vandalized over the years, therefore, Part two of the Act seeks to protect the assets by stating that the President of the Federal Republic of Nigeria may prescribe minimum standards and rules in relation to protection of critical infrastructure. The President may prescribe the general management of critical information infrastructure and access to the transfer and control of data in any critical information infrastructure. The overall aim of this Part is to protect Critical National Information Infrastructure from tampering and vandalism by cybercriminals (Cybercrime Act, 2015).

PART 3: OFFENCES AND PENALTIES

The Act in Part three gives provisions for various offences and their penalties. Offences under the Act as enumerated by Ladan (2015) are: offences against critical national infrastructure; unlawful access to a computer system or network; system interference; intercepting electronic messages; cyberterrorism and identity theft and impersonation. Other offences mentioned in the Cybercrimes Act (2015) are racist and xenophobic offences; cyberstalking; cybersquatting; computer related fraud; computer related forgery; and theft of electronic signature amongst others. These offences are summarised in Table 3.5

	ACT	SUMMARY OF ACT		
	CYBERCRIMS ACT 2015	This Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.		
	PART 3: OFFENCES AND PENALTIES			
S/N	**SECTIONS**	**TITLE OF SECTIONS**	**SUMMARY**	**PENALTIES**
1	***Section 5***	Offences Against Critical National Information Infrastructure	Critical National Information Infrastructures are designated computer systems, programs and networks that have impact on the security and economy of Nigeria Amongst others.	A person found guilty is liable on conviction to imprisonment of term not ≥ 10years without option of fine. When offences involves bodily harm the penalty is ≥ 15 years and when it death = life imprisonment.
2	***Section 6***	Unlawful Access to a Computer	Unlawful access of computer or network for fraudulent purposes to obtain data	A person found guilty is liable on conviction to imprisonment of term not ≥ 7 years or a fine of ≥ N7 Million Naira
3	***Section 13***	Computer Related Forgery	Access of computer to delete or alter data	3 years in prison or N7 million or both
4	***Section 14***	Computer Related Fraud	Access of computer to commit fraud	3 years in prison or N7 million or both
5	***Section 16***	Unauthorized modification of Computer systems, network data and system interference.	Without lawful authority modifies or causes modification of any data held on a computer.	Not more than 7 years imprisonment or N10 Million or both
6	***Section 18***	Cyber Terrorism	Access computer for purpose of terrorism	Life imprisonment on conviction
7	***Section 22***	Identity theft and impersonation	Identity theft in financial institution or impersonation	7 years imprisonment or N5 Million Naira or both.
8	***Section 23***	Child pornography and related offences	Produces, offers, distributes or possess child porn	5-15 years in prison and N10 - N25 million in fines
9	***Section 24***	Cyber Stalking	A course of conducted directed at a specific person that would cause a reasonable person to feel fear.	3 – 10 years imprisonment and/or N7 – N25 Million Naira in Fines
10	***Section 30***	Manipulation of ATM/POS Terminals	Manipulation of ATM/POS with intention to defraud	5 years in Prison or N5 million or both
11	***Section 32***	Phishing, Spamming, Spreading of Computer Viruses	Sending of spam emails and spreading of computer viruses	3 years imprisonment or N1 Million or both
12	***Section 36***	Use of fraudulent device or attached e-mail and websites	Use of any devices, email or website with an intention to defraud.	3 years imprisonment or N1 Million or both

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

Table 3.5: Various Offences and Penalties under the Cybercrimes Act 2015

PART 4: DUTIES OF FINANCIAL INSTITUTIONS

Part four of the Act provides for duties of financial institutions and service providers. Duties of financial institutions under the Act include: verifying the identity of its customers carrying out electronic financial transactions, applying the principle of know your customer by documenting customers, and avoiding the making of unauthorized transactions on customer accounts (Cybercrimes Act 2015).

The Act further requires Service Providers as provided in Section 38(1) to retain all traffic data and subscriber information as may be requested by relevant authority for a period of two years (Cybercrimes Act, 2015).

PART 5: ADMINISTRATION AND ENFORCEMENT

Section 41 (1) of the Cybercrimes Act (2015) designates the Office of the National Security Advisor (ONSA) as the coordinating body for the administration and enforcement of all law enforcement and security agencies under the Act. The duties of the ONSA as a coordinating body are to provide support to relevant agencies to combat cybercrime, establish and maintain the National Computer Emergency Response Team (CERT), establish appropriate platforms for public private partnership (PPP), and establish and maintain a National Computer Forensic Laboratory amongst others.

A pragmatic provision of the Act requires that all LEAs should organize training programmes for officers in charge of prohibition, detection, prevention, investigation and prosecution of cybercrimes. Oke (2015) argues that this provision makes LEAs more effective in detecting and preventing cybercrimes in Nigeria.

Section 42 of the Act also establishes the Cybersecurity Advisory Council which comprises representatives of each of the Ministries and Agencies listed in the First schedule of the Cybercrimes Act (Cybercrimes Act, 2015).

Table 3.6 summarises of all the Acts and policies.

	NIGERIAN ACTS & POLICIES	SUMMARY OF ACT	OFFENCES COVERED	ENFORCEMENT AGENCY
1	**Criminal Code Act**	Act empowering criminal proceedings.	Armed robbery, advance fee fraud, treason, murder etc.	*****Various Law Enforcement Agencies
2	**Economic & Financial Crimes Commission Act 2004**	The Act provides for the establishment of the Economic and Financial Commission charged with the responsibility for the enforcement of all economic and financial crimes, among other things.	Economic and Financial Crimes such as fraud, narcotic drug trafficking, tax evasion, piracy, oil bunkering, illegal arms deal etc.	Economic and Financial Crimes Commission (EFCC).
3	**Money Laundering Act 2012 (as amended)**	This makes comprehensive provisions to prohibit the laundering of the proceeds of a crime or an illegal act and provides appropriate penalties and expands the interpretation of financial institutions and scope of supervision of regulatory authorities on money laundering activities, among other things.	Laundering of illegal gotten money or proceeds derived from Economic and Financial Crimes.	*National Drug Law Enforcement Agency (NDLEA) *Central Bank of Nigeria (CBN) *EFCC
4	**Advance Fee Fraud and other Fraud Related Offence Act 2006**	An Act to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences.	Advance Fee fraud, cybercrime, 419 scams, securities and monetary scams etc.	*****EFCC
5	**Evidence Act (as amended 2011)**	The Evidence Act applies to all judicial proceedings in or before any court established in the Federal Republic of Nigeria. It provides definitions of documentary evidence receivable before Courts in the country	Hearsay, Opinion and Character evidence, Documentary evidence, Oral evidence, Computer and Electronic Evidence etc.	***** Minister of Justice and Attorney General of the Federation through law enforcement agencies.
6	**Cybercrimes (Prohibition, Prevention Etc.) Act 2015**	This Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes.	Identity Theft, Phishing, Spamming, Cyber Squatting, Cyber Stalking, Cyber Terrorism and Child Pornography etc.	29 Stakeholders including the ONSA as the coordinating agency.
7	**National Cybersecurity Policy**	Strategic intent of the government in reducing the country's risk exposure; curtailing cyber threats that are inimical to national security.	Cybercrime, Cyber Espionage, Cyber Conflict, Cyber Terrorism & Child Porn.	All MDAs and Government Agencies
8	**National Cybersecurity Strategy**	Strategy to provide comprehensive measures and strategic actions towards assuring security and protection of the nation's presence in the cyberspace, protecting critical information infrastructure, building and a trusted cyber-community	NA	All MDAs and Government Agencies

(Adopted from Criminal Code Act, AFF Act 2006, EFCC Act 2004, MLA Act 2012, Cybercrimes Act 2015)

Table 3.6: Acts and Policies Dealing with Cybercrime and Advance Fee Fraud in Nigeria

3.7.4 Government Partnership

Yahaya (2009) stated that the Nigerian government through the EFCC signed a memorandum of understanding (MoU) with Microsoft with the aim of tackling cybercrime and software piracy in Nigeria. Some of the benefits of the MoU included:

1. Increasing the scope of the partnership to cover the fight against software piracy across Nigeria and to involve the Advance Fee Coalition (Microsoft, Yahoo, Money gram and African Development Bank)
2. Partnering with Advance Fee Coalition designed to curb internet scams, identity theft, financial scams and spams as well as software piracy.
3. Allowing the EFCC to host the first ever West African Internet Fraud Summit in 2009 sponsored by Microsoft.
4. Developing collaborative efforts between Microsoft and EFCC to develop and implement programmes to educate the public on the consequences associated with the infringement of software copyrights.
5. Implementing capacity building for institutions and stakeholders involved in software piracy
6. Strengthening awareness within the general public and stakeholders on the importance of intellectual property rights.
7. Collaborating in efforts to identify, investigate and prosecute suspected software pirates and ensure public awareness of the benefits of genuine software for local businesses (EFCC, 2009).

3.7.5 National Cybersecurity Policy

The National Cybersecurity Policy spells out the strategic intent of the Nigerian government in reducing the country's risk exposure, curtailing cyber threats that are inimical to national security and the Nigerian economic wellbeing (Ladan, 2015). The policy identified five key cyber threats as posing significant challenges to Nigeria. These challenges are: Cybercrime; Cyber-Espionage; Cyber conflict; Cyber-Terrorism; and Child Online Abuse and Exploitation (NgCERT, 2014). The National Cybersecurity Policy (NgCERT, 2014a) culminated in the establishment of the Cyber Security Focal Point at the Office of the National Security Advisor (ONSA).

The main objectives of the National Cybersecurity Policy as enumerated by Ladan (2015) are:

a. To facilitate the establishment of an effective legal framework and governance mechanism for Nigeria's presence in cyberspace and the cybersecurity ecosystem.
b. To develop an information security and control mechanism for the protection and safety of Nigeria's national critical information infrastructure and its associated economic infrastructures in the cyberspace.
c. To develop a national cybersecurity assurance framework, compliance and enforcement mechanism.
d. To develop a centralised national emergency readiness and incident management coordination capability.
e. To develop a framework for inter-agency collaboration on combating cybercrime and cybersecurity.

3.7.6 National Cybersecurity Strategy

The National Cybersecurity Strategy (NCSS) is Nigeria's readiness strategy to provide comprehensive measures and strategic actions towards assuring security and protection of the nation's presence in cyberspace, protecting critical information infrastructure, and building and nurturing trusted cyber-community (NgCERT, 2014b). Ladan (2015) states that the main aim of the NCSS is to provide a cohesive roadmap, initiatives and implementation mechanisms in order to achieve the national vision on cybersecurity. The objectives of the NCSS are:

a. A comprehensive cybercrime legislation and cyber threat counter measures that is in line with international laws and best practices.
b. To provide measures that protect critical information infrastructure.
c. The articulation of an effective computer emergency response capability.
d. The protection of the government from all forms of cyber-attacks.
e. The coordination of cybersecurity initiatives at all levels of government in the country, amongst others (NgCERT, 2014a; Ladan, 2015).

3.7.7 Nigerian CERT (ngCERT)

Section 41 subsections 1(c) of the Cybercrimes Act (2015) states that the Office of the National Security Adviser shall 'establish and maintain a National Computer Emergency Response Team (CERT) Coordination Center responsible for managing cyber incidences in Nigeria'. The

Nigerian Computer Emergency Response Team (ngCERT) was established with the mission: 'to manage the risk of cyber threats in the Nigeria's cyberspace and effectively coordinate incident response and mitigation strategies to proactively prevent cyber-attacks against Nigeria'. The main functions of ngCERT are:

a) To establish a shared situation awareness platform and coordinate information sharing at the national level.
b) To effectively manage and coordinate management of incident of national interest
c) To support the National Cybersecurity policy (Council of Europe, 2017).

3.8 Role of other Stakeholders

Apart from law enforcement agencies, there are other key stakeholders that are vital in tackling cybercrime and other computer-related offences in Nigeria. Their functions varies from making laws to regulating the telecommunications and ICT sector respectively. The stakeholders are the National Assembly, Office of the National Security Advisor, Nigerian Communications Commission and National Information Technology Development Agency.

3.8.1 National Assembly

The National Assembly of Nigeria is the Legislative arm of the Federal Government of Nigeria. It is made up of the upper chamber, Senate and the lower chamber, House of Representatives. The National Assembly is the nation's highest legislature, whose power to make laws is summarised in chapter one, section four of the 1999 Nigerian Constitution. The Senate is one of the Chambers in Nigeria's bicameral legislature, the National Assembly. Sections 47-49 of the 1999 Constitution state inter alia that "There shall be a National Assembly (NASS) for the federation which shall consist of two chambers: the Senate and the House of Representatives". The Senate is headed by the President assisted by the Deputy President of the Senate. These Presiding officers serve as political heads. There are 109 members in the Senate corresponding to the 109 senatorial districts in the country (National Assembly of Nigeria, 2017a).

Senatorial Districts are evenly distributed among the thirty six states. Each state has three senatorial districts while the Federal Capital Territory (FCT), Abuja has just one senatorial district (National Assembly of Nigeria, 2017a, 2017b, 2017c).

According to the 1999 Constitution of the Federal Republic of Nigeria, (National Assembly of Nigeria, 2017b), the House of Representatives is the 2nd Chamber in Nigeria's bicameral legislature, the National Assembly. The House of Representatives is headed by the Speaker assisted by the Deputy Speaker. These Presiding officers serve as political heads. There are 360 members in the House of Representatives representing the 360 Federal Constituencies the country is divided into based on population.

3.8.2 Office of the National Security Advisor – ONSA

The Office of the National Security Adviser was created to coordinate national security in Nigeria. The National Security Agencies Act (1986) states that the coordinator on national security shall be charged with the following duties:

a) Advising the President on matters concerning the intelligence activities of the agencies;
b) Making recommendations in relation to the activities of the agencies to the President, as contingencies may warrant;
c) Correlating and evaluating intelligence reports relating to the national security and providing the appropriate dissemination of such intelligence within Government, using existing facilities as the President may direct;

The Office of the National Security Advisor under the National Security Advisor is the overall coordinator of the Cybercrime Advisory Council. (Council of Europe, 2017; Cybercrimes Act, 2015)

3.8.3 Telecommunications Regulator – NCC

The Nigerian Communications Commission (NCC) is the independent national regulatory authority for the telecommunications sector in Nigeria. The Commission is responsible for creating an enabling environment for competition among operators in the industry as well as ensuring the provision of qualitative and efficient telecommunications services throughout the country (Nigerian Communications Commission, 2017a).

Some of the functions of the Commission are:

a. The facilitation of investments into the Nigerian market for provision and supply of communications services, equipment and facilities.

b. The protection and promotion of the interests of consumers against unfair practices including but not limited to matters relating to tariffs and charges for and the availability and quality of communications services, equipment and facilities.

c. Ensuring that licensees implement and operate at all times the most efficient and accurate billing system.

d. The promotion of fair competition in the communications industry and protection of communications services and facilities providers from misuse of market power or anti-competitive and unfair practices by other service or facilities providers or equipment suppliers.

e. The granting and renewing communications licences whether or not the licences themselves provide for renewal in accordance with the provisions of this Act and monitoring and enforcing compliance with licence terms and conditions by licensees.

f. The proposing and effecting of amendments to licence conditions in accordance with the objectives and provisions of this Act.

g. The fixing and collecting of fees for grants of communications licences and other regulatory services provided by the Commission (National Communications Act, 2003).

3.8.4 ICT Regulator - NITDA

The National Information Technology Development Agency (NITDA) is a Federal government agency set up by an act of the National Assembly for the implementation of the Nigerian Information Technology (IT) policy. The mission of the agency is to develop and regulate IT for sustainable national development. Its vision is to become the prime catalyst for transforming Nigeria into an IT driven economy. NITDA's mandates as enshrined in the NITDA Act of 2007 are being achieved through several programmes and initiatives (NITDA, 2018).

3.9 Role of Law Enforcement in Investigating and Prosecuting Cybercriminals

Government institutions, especially policing agencies, by law have certain regulatory authority, jurisdiction and criminal justice components that involve investigating and prosecuting a certain combination of IT-enabled abuse, attacks and crimes (McQuade, 2006).

3.9.1 Role of the Economic and Financial Crimes Commission

The Economic and Financial Crimes Commission was established through an act of parliament called the EFCC Act 2004 in order to fight corruption and create credibility to attract foreign direct investment in Nigeria (Obuah 2010). Chawki et al. (2015) states that, the EFCC was established in 2003 in order to make Nigeria compliant with the recommendations from the Financial Action Task Force (FATF) that listed Nigeria as one of the 23 Non-Cooperative Countries and Territories (NCCT) in the international community fight against money laundering. The EFCC is mandated to prevent, investigate and prosecute economic and financial crimes. The EFCC is also charged with the responsibility of enforcing the provisions of laws in regards to economic and financial crimes. Such laws and regulations are the Bank and other Financial Institutions Act (BOFIA) of 1991, the Miscellaneous Offences Act, the Failed Banks and Financial Malpractices in Bank Act of 1994, the Money Laundering Act of 1995, the Advance Fee Fraud and Other Fraud Related Offences Act of 1995, the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission (Establishment) Act of 2004 (Tive 2005; EFCC Act 2004).

3.9.1.1 Functions of the EFCC

Section 6 of the EFCC Act (2004) makes provisions for the following functions of the EFCC:

1. The enforcement and the due administration of the provisions of the EFCC Act.
2. Investigation of all financial crimes including advance fee fraud, counterfeiting, money laundering, illegal charge transfer, future market fraud, computer credit card fraud, cyber-crime, contract scam etc.
3. Coordination and enforcement of all economic and financial crimes laws and enforcement functions conferred on any other person or authority.
4. Adoption of measures to identify, trace, freeze, confiscate or seize proceeds from terrorist activities, economic and financial crime related offences.
5. Maintaining liaison with the office of the Attorney-General of the Federation, the Nigerian Customs Service, the Immigration and Prison Service Board, the Central Bank of Nigeria, the Nigerian Deposit Insurance Corporation, the Nigerian Drug Law Enforcement Agency and all government security and law enforcement agencies.
6. The facilitation of efficient exchange of scientific and technical information and the

conduct of joint operations geared towards the eradication of economic and financial crimes.

7. The collection of all reports in regards to suspicious financial transactions, analysis and dissemination to all relevant government agencies.
8. Carrying out an effective and rigorous public enlightenment campaign against economic and financial crimes within and outside Nigeria.

3.9.1.2 Special Powers of the EFCC

The special powers of the EFCC are clearly stated under Section 7(1)(2) of the EFCC Act (2004). The Commission has the power to conduct an investigation into any person, corporate body or organization that has committed an offence related to economic and financial crimes under the EFCC Act or any law related therein.

Obuah (2010) argues that the EFCC has extensive special and police powers to cause an investigation to be conducted into the properties of any person if the persons income and lifestyle is not justified by his/her source of income. The commission is also charged with the responsibility of enforcing the provisions of the Bank and other Financial Institutions Act (BOFIA) of 1991, the Miscellaneous Offences Act, the Failed Banks and Financial Malpractices in Bank Act of 1994, the Money Laundering Act of 1995, the Advance Fee Fraud and Other Fraud Related Offences Act of 1995, the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission (Establishment) Act of 2004; any other law or regulations relating to economic and financial crimes, including the Criminal code of penal code (Tive 2005; EFCC Act 2004).

3.9.1.3 EFCC Mode of Operation

The EFCC is an autonomous agency headed by an executive chairman under the supervision of a board. The Commission operates within the confines of the law and its mode of operation is stipulated in Section 12 (1) of the EFCC Act (2004) that states, 'for the effective conduct of the functions of the Commission, there may be established for the Commission the following units':

General and Assets Investigation Unit: The General and Assets Investigation Unit as stated in Section 13(1) is charged with the responsibility for the prevention and detection of offences in

violation of the EFCC Act, the arrest of economic and financial crime perpetrators, the investigation of assets and properties of individuals arrested for committing any economic or financial crime, the identification and tracking of proceeds and properties involved in any offence under the Act and the forfeiture of such proceeds and properties to the Nigerian government. Most importantly, the unit deals with matters connected with extradition of criminals and mutual assistance in criminal matters involving economic and financial crimes.

Legal and Prosecution Unit: The Legal and Prosecution Unit is an integral part of the EFCC that is charged under Section 13(2) of the EFCC Act (2004) with the responsibility of prosecuting offenders that have committed any form of economic and financial crimes, supporting the investigation unit by providing the unit legal advice and assistance and conducting proceedings necessary towards the recovery of assets or property forfeited under the EFCC Act.

Training Unit: Section 11 of the EFCC Act (2004) states that the commission shall initiate and develop specific training programs for its law enforcement and other personnel charged with the responsibility for the eradication of offences under the Act. Such programs should include methods used in the detection of offences stated under the EFCC Act, methods used by individuals involved in economic and financial crimes and their countermeasures, collection of evidence, legal prosecution and defense and dissemination of information of economic and financial crimes.

Other special units mentioned in the EFCC Act (2004) are the Research Unit and Administrative unit. However, section 12(2) of the Act stated that the EFCC had powers to set up any unit or committee in order to assist it in the discharge of its functions under the EFCC Act.

3.9.1.4 Role and Function of the Nigerian Financial Intelligence Unit (NFIU)

The Nigerian Financial Intelligence Unit (NFIU) is a Nigerian version of the global financial intelligence unit (FIUs) domiciled within the EFCC as an independent unit operational in Africa. The NFIU seeks to comply with international best practices on combating Money Laundering and Financing of Terrorism (Nigerian Financial Intelligence Unit [NFIU], 2015). The NFIU was established based on the provisions of 'Recommendation 29' of the Financial Action Task Force (FATF) standards and Article 14 of United Nations Convention Against Corruption (UNCAC). In compliance the FATF recommendation and UNCAC requirements, the NFIU became fully

operational in 2005. The Unit has since developed standards for the receipt, analysis and dissemination of financial intelligences to LEAs and enhances compliance with the regulatory framework on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) in Nigeria (NFIU 2015).

3.9.1.4.1 Mandate of the NFIU

The NFIU (2015) derives its powers from the Economic and Financial Crimes Commission (EFCC) Act, 2004 and the Money Laundering (Prohibition) Act 2011 as amended in 2012. The main mandate of the NFIU as stipulated by international best practices is to serve as the designated national center for receipt and analysis of:

1. Suspicious transaction reports
2. Other relevant information to money laundering, associated predicate offences and terrorist financing;
3. Dissemination of the results of the analysis to relevant law enforcement agencies and bodies (NFIU, 2015).

3.9.1.4.2 Functions of the NFIU

According to the NFIU (2015), the Unit has the following responsibilities:

1. To advise the government and regulatory bodies on prevention and tackling of economic and financial crimes.
2. To receive reports on cross-border movement of currency and monetary instruments.
3. To liaise with compliance officers and ensure strong compliance culture by reporting entities.
4. To receive currency transactions reports, suspicious transactions reports, currency declaration reports and other data related to money laundering and terrorist financing activities from financial institutions and designated non-financial institutions (DNFIs).
5. To maintain a robust financial intelligence database for data collection, analysis and exchange with other FIUs and LEAs around the world.
6. To promote public awareness of matters related to economic and financial crimes, money laundering and terrorism financing.

3.10 Role of EFCC in Tackling Cybercrime

Chawki et al. (2015) argues that the Nigerian government through the activities of LEAs such as the EFCC has mapped out strategies and policies to effectively tackle the transnational nature and scope of cybercrime and cybercriminals. Amongst such measures are Enforcement Approach, Legislative Approach, Administrative Approach and Partnership.

3.10.1 Enforcement Approach

Abubakar (2009) states that, the EFCC since its inception in 2003 has adopted various strategies to reduce the occurrence of 'Advance Fee Fraud' scams which has become a threat to Nigeria's economic development and national image. Such strategies include Intelligence; Disruption; Enforcement; Prevention and Education.

3.10.1.1 Intelligence

The EFCC uses the following intelligence strategies, according to Abubakar (2009), in order to curtail the activities of fraudsters and cybercriminals:

1. The registration of all Internet Service Providers (ISPs), cybercafés and Telecommunication companies in line with the provisions of the Advance Fee Fraud Act 2006.
2. The effective utilisation of the Nigerian Financial Intelligence Unit (NFIU) to track all financial transactions online.
3. The use of confidential informants to locate and provide intelligence on location and suspects involved in scams and fraudulent activities.
4. The receipt of anonymous tips and information through the EFCCs website.
5. The adoption of a suspicious activity reporting system with cybercafés, banks, courier and money transfer companies.
6. The development of due diligence by working with local associations of ISPs, Telco's and cybercafé operators to prevent the misuse of their facilities by scammers.

3.10.1.2 Disruption

The Nigerian government through the EFCC uses disruptive measures such as cyber raids, freezing of bank accounts and termination of telephone services. Such measures include:

1. Raids on suspected black spots such as cybercafés and fictitious production centres used by scammers.
2. Freezing of bank accounts suspected of being involved in illegal activities such as money laundering.
3. Termination of service of telephone/fax lines that feature on scam documents.
4. Partnership with ISPs, cybercafés operators, telecommunication providers, courier and money transfer companies to disrupt illegal activities of fraudsters.
5. National raid of currency brokers who are conduits for money laundering activities.
6. Collaborating with FBI Internet crime complaint centre (IC3) to block fraudulent email addresses and websites.
7. Interception of over N55 Billion Naira worth of fraudulent cheques in 'Operation Stop Payment' in 2007.
8. Interception of suspicious incoming packages related to fraudulent internet purchase scams as well as outgoing fraudulent documents (Abubakar 2009).

3.10.1.3 Enforcement

Abubakar (2009) states that through collaboration with foreign LEAs and organisations, the EFCC has been able to effectively investigate and prosecute the activities of scammers. Such enforcement initiatives are:

1. Establishment of specialised units for specific offences such as cybercrime, card fraud and postal investigation amongst others.
2. Collaboration with foreign agencies on investigation such as FBI, USPIS, USSS, UK SOCA, City of London Police, Metropolitan Police etc.
3. Seizure of assets of suspected offenders
4. Restitution to foreign victims in line with due process and international best practices.
5. Effective prosecution of fraud related offences and successful convictions
6. Collaboration with Interpol to organize the West African enforcement initiative on Advance Fee Fraud in 2007.
7. Conducting a National cybercafés raid of over 90 notorious cafes and arrest of over 100 suspects in 2008 that are currently facing various criminal charges in Nigeria.

3.10.1.4 Prevention and Education

Section 6(p) of the EFCC Act (2006) provides for the EFCC to carry out and sustain an effective public enlightenment campaign against economic and financial crimes within and outside Nigeria. In view of that, Waziri (2009) commented on the launching of the Anti-Corruption Revolution Campaign (ANCOR) which was aimed at enabling Nigerians to participate effectively and to take ownership of the fight against economic and financial crimes.

Therefore, the EFCC undertook a sustained campaign through television, radio and the internet to educate and inform especially the youth on the evils of Advance Fee Fraud. The EFCC also hosted, supported and participated in local lectures, seminars and conferences that amplified the negative effects of advance fraud to the Nigerian society (Abubakar 2009).

3.10.2 Administrative Approach

Administrative measures involve setting up dedicated and specialized units to tackle the menace of advance fee fraud. Such technical measures are created to prevent and prosecute the activities of cybercriminals (Chawki et al. 2015).

3.10.2.1 Transaction Clearing Platform

The Transaction Clearing Platform (TCP) of the EFCC was set up to assist individuals and companies to undertake basic due diligence in relation to business proposals received from or intended for execution in Nigeria (Waziri 2009).

Babefemi (2011) stated that, up to 2011, the TCP had treated over 17,000 enquiries from foreign investors, thus, saving investors from losing over $15 billion dollars to scam contracts and business proposals. The key components of the Transaction Clearing Platform as enumerated by Waziri (2009) were:

1. The platform would be operated and coordinated by dedicated and experienced EFCC staff.
2. Minimally it would verify genuine investors and the veracity of the business proposals they received from Nigeria.
3. The verification would be basic and investors would be advised to do further due diligence as shall be deemed necessary.
4. The service would be easily accessible from the official EFCC websites (i.e.

www.efccnigeria.org)

5. The platform would send advisory emails to victims and potential victims of '419' using email addresses extracted from the depository of suspected and convicted fraudsters in Nigeria.

3.10.2.2 Operation Eagle Claw

The Eagle Claw is another initiative of the EFCC dedicated to tackling internet fraud which is commonly known as 'Yahoo Yahoo'. The EFCC is partnering with software giant, Microsoft to fine tune the technical modalities that would enable the commission to wipe out the high prevalence of fraudulent emails (Ukanwa 2015). Fabi (2009) mentioned that, the 'Eagle Claw' was aimed at improving Nigeria's tarnished image as one of the world's top countries for internet crimes.

According to the BBC (2009), the EFCC has been able to shut down over 800 fraudster's email accounts and has arrested all those behind 18 high-profile cybercrime syndicates. Fabi (2009) argued that upon full deployment of the Eagle Claw, the EFCC would have the capacity to take down about 5000 email accounts monthly. The EFCC aimed to deploy operatives working 24 hours, 7 days a week to detect key words found in fraudulent emails and only clean emails would be allowed to go out of Nigerian cyberspace.

3.10.2.3 Operation Cyber Storm

Operation Cyber Storm was a coordinated and simultaneous raid on notorious internet cafes by the EFCC in 2008. The operation was located in major cities across the six geopolitical zones in Nigeria in order to arrest internet fraudsters (Akintoye 2008). Oladipo (2012) describes how the operation yielded several arrests and exposed several owners of un-registered cafes.

Akintoye (2008) mentioned that evidence recovered during the raid included 753 CPUs, 27 laptops and other accessories while 136 suspects were arrested across the country. Oladipo (2012) stated that one of the suspects arrested during the raid, an undergraduate of Olabisi Onabanjo University, was in 2012 sentenced to five years imprisonment over an attempt to obtain money under false pretences. Additionally, a former member of the National Assembly is currently standing trial in a state High Court over an alleged illegal use of his premises and failure to register his cyber café will all regulatory agencies including the EFCC.

3.10.3 Partnership Approach

The EFCC is also partnering with Microsoft by using smart technology rather than cyber raids on internet cafés to tackle the activities of scammers (BBC 2009).The EFCC strengthened its partnership with its external stakeholders through signing Memoranda of Understanding (MoU) in 2014 with the National Lottery Regulatory Management, British American Tobacco Company and the Spanish National Police. The EFCC also signed an administrative cooperation arrangement on the establishment of the Economic Crime Agency Network (ECAN). The network is made up of the City of London Police, Corrupt Practices Investigation Bureau of Singapore, the European Anti-Corruption Fraud Office and the US FBI amongst others.

3.11 UK and International Response

With the rapid increase of proliferation of ICT and the borderless nature of the internet, cybersecurity has become a complex transnational issue that requires international cooperation for ensuring the safety of the internet (UN, 2011). Drinkwater (2015) argues that because the threat of cybercrime is international, therefore, the response should be through a collective sharing of information, intelligence and evidence for an international response to be effective.

3.11.1 UK Laws

Computer Misuse Act (1990) was created to criminalise unauthorized access to computer systems and equally to discourage cybercriminals from using a computer to assist in the commission of a criminal offence or from hindering access to data stored in a computer. The Act contains 3 main sections namely:

a. **Section 1 –** Unauthorized access to a Computer material:
b. **Section 2 –** Unauthorized access with intent to commit or facilitate commission of further offences:
c. **Section 3 –** Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer:

3.11.2 UK Cyber Security Strategy 2011-216

The UK funded the National Cyber Security Programme of £860 million between 2011 and 2016 to deliver the 2011 National Cyber Security Strategy. The aim was to:

a. Tackle cybercrime and make the UK one of the most secure places in the world to do business on the internet.
b. Make the UK more resilient to cyber-attack and to protect the UKs interest on the cyberspace.
c. To help mould an open, vibrant and stable cyberspace that supports open society.
d. Build the UK's cyber security knowledge, skills and capability (UK Government, 2016).

3.11.3 Council of Europe Convention on Cybercrime

The Council of Europe convention on cybercrime was created in order to pursue a common criminal policy aimed at the protection of the society against cybercrime through adopting appropriate legislation and fostering international cooperation (Council of Europe, 2011). Shehu (2014) states that the Budapest convention on cybercrime is another instrument aimed at combating cybercrime. It aims at:

a. Laying down commons definitions of certain offences enabling relevant legislation to be harmonised at the national level;
b. Defining common types of investigative powers better suited to the IT environment, therefore, enabling criminal procedures to be brought into line between countries; and
c. Determining both traditional and new types of international cooperation.

3.11.4 AU Response

Internet penetration is growing rapidly in Africa and across the globe due to the dramatic increase in the use of mobile technology. African government, the private sector and individuals rely on the internet to conduct sensitive transactions and store important data. However, most African countries are lagging behind in fighting cybercrime and strengthening their cybersecurity measures (Tamarkin, 2015). Tamarkin (2015) further argues that African countries are becoming safe havens for cybercrime activities because of increased internet availability at lower costs, a rapidly growing internet user base and a lack of effective cybercrime laws on the continent.

Recently, the African Union took a positive step in addressing some of these problems by adopting an AU Convention on Cyber Security and Personal Data Protection. The convention embodies the existing commitments of African Union Member States at sub-regional, regional and International levels to build the Information society by strengthening existing legislations on

ICT of member states and Regional Economic Communities (Dotzauer, 2014; African Union, 2014).

The AU convention attempts to address a wide range of online activities such as electronic commerce, data protection, cybersecurity and cybercrime. With regards to cybercrime, it requires member states to adopt laws that criminalise:

a) Attacks on computer systems (e.g. fraudulently accessing a computer system)
b) Computerised data breaches (e.g. fraudulently intercepting data)
c) Content-related offences (e.g. disseminating child pornography)
d) Offences relating to electronic message security measures (African Union, 2014; Tamarkin, 2015)

Dotzauer (2014) further states that the goal of the Convention is to address the need for a harmonized legislation in the area of cyber security in member states of the African Union and to establish in each Member State a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. The convention also seeks to modernise the legal instruments for tackling cybercrime by the formulation of policies for the adoption of new offences specific to ICTs. However, Tamarkin (2015), raised some concerns and challenges with the AU approach by criticising the content-related offences section as imposing 'dangerously broad limitations on free speech'. Also, the scope of the convention is very ambitious as it deals with many areas of electronic activities beyond cybercrime, thus, limiting the number of member states that can implement the convention as few countries have enacted cybercrime laws. Furthermore, many African countries lack the technical expertise to draft and enforce such laws

3.12 Recommendations to Tackling Cybercrime

The diversity and varied approaches of regional and international bodies are all aimed at having a global approach to tackling the issue of cybersecurity and cybercrime (Broadhurst, 2006). Grabosky and Broadhurst (2005) state the basic elements of an effective regime for regional cooperation in tackling cybercrime should include the following:

a) Improving security awareness by providing adequate resources to secure transactions and equip system operators and administrators.

b) Strengthening international partnership by updating existing treaties and agreements to recognise the existence, threats and transnational nature of high-tech computer-related crimes and strive for legal harmonization,
c) Improving coordination and collaboration by provision of systematic exchange of information and expertise between the private sector and law enforcement agencies.
d) Taking concrete steps to ensure that technology does not outpace the ability of law enforcement to investigate and make laws adequate for coping with the ever-evolving nature of cybercrime.
e) Developing computer forensic skills by law enforcement and investigative personnel; and
f) Developing mechanisms for operational cooperation's between law enforcement agencies and different countries through the use of a computer emergency response teams.

3.12.1 Education and Awareness

According to Kortjan and Solms (2014), the negative consequences of the lack of knowledge and cybersecurity awareness has become an important issue in addressing cybercrime. They argued that, education and awareness can provide users to be knowledgeable about the risks that are present online. Additionally, education plays an important role in developing a culture of secure behaviours amongst users in the cyber domain. Dix (2017), however, argued that a comprehensive national security education campaign is mandatory for raising public awareness of the risk and impact of some cyber activities, hence the need to deploy basic protective measures in using online digital devices.

Furthermore, Aloul (2012) argued about the importance of user education and training in combating security threats online. He further states that, different groups have to be involved in order to 'produce an IT security-aware resident'. Some of the recommendations, according to Aloul (2012) are:

1. Government should make and enforce cybercrime laws by partnering with other governments to effectively tackle cybercrime. Governments should also create a Computer Emergency Response Teams (CERT) that are dedicated to the detection, prevention and response of cyber security incidents

2. Law enforcement agencies such as the police should have a computer forensics teams that are specialised in obtaining, recovering and examining digital evidence stored on digital devices.
3. The users should train themselves by regularly reading magazines and books on cyber security threats and steps to take to protect themselves from such threats.
4. Schools and Universities should offer cyber security awareness campaigns and integrate cyber security topics into their course curriculum.

Olayemi (2014) also recommended for the development and promotion of national security awareness and education programme at all levels from the primary to the tertiary institutions.

3.12.2 Laws and Policy

According to Grabosky (2001), one of the greatest challenges posed by the activities of cybercrime is 'the enormously enhanced potential for transnational offending. He further argued that, common laws and policies are required in order to garner the legal assistance of a foreign state to assist in a cybercrime investigation. Olusola et al. (2013b) states, governments should work together in strengthening the legal frameworks for cybersecurity. However, Hassan et al. (2012) state, the Nigerian government must enforce laws regarding cybercrime in order to deter cybercriminals from their nefarious activities.

3.12.3 Partnership

According to Binns (2017), collaboration is an essential element of a successful police investigation. The continued rise of cybercrime has brought a new vigour in law enforcement partnership with the private sector. She further argued that, partnerships helps to foster the flow of information and there is an information sharing gap between stakeholders which can provide an avenue for cybercriminals.

Standard police practices are not adequate to curtail cybercrime, therefore, law enforcement and businesses must partner to address cybercrime (WEF, 2016). WEF (2016) proposed some recommendations as a first step in achieving mutual agreement so as to tackle cybercrime on a global scale. The recommendations are:

1. Public and private sectors should exchange information related to cyber threats and vulnerabilities.
2. Public and private sectors should cooperate to promote and adopt the Budapest Convention on Cybercrime, or some of its principles.
3. Public and private sector should work to enhance trust and discuss issues such as encryption and protection of privacy in order to find appropriate solutions.
4. Public and private sectors should work to create and coordinate platforms in order to increase information-sharing and improve investigations and prosecutions.

3.12.4 Funding

There is shortage of expertise and resources to assist African states in ratifying international cybercrime conventions (Tamarkin, 2015), therefore, there is a need to increase the budget of law enforcement agencies to tackle crime (Barej, 2017). According to Cobb (2016), governments around the world are working to increase the supply of cyber-skilled workforce, thus, education and recruitment efforts are receiving more funding. The funding gap could be achieved by encouraging law enforcement authorities and the private sector to join existing public-private collaboration initiatives and to increase coordination between them (WEF, 2016).

3.12.4 Training

Ajayi (2016) argued that most cybercriminals are well skilled in computer and cyberspace issues, therefore, their expertise should not be compared with law enforcement officials who are ill-trained and poorly remunerated. He states further that the forgoing factor makes any effort at investigation and enforcement of cybercrime laws futile. Also, there is the challenge in recruitment and retention of law enforcement officers with the required skill sets to tackle cybercrime (Saunders, 2017). Therefore, in order to better tackle cybercrime, WEF (2016) recommends that the public-private sectors should cooperate through:

a. The sharing of best practices in IT education and training of end users
b. The sharing of technical prevention and protection measures
c. The fostering of technology innovations and investments to meet the global cyber-security challenges (WEF, 2016).

3.13 Cybercrime Investigation Timeline in Nigeria (1990-2016): Nigeria

The cybercrime investigation timeline in Nigeria was created by the researcher to serve as a guide in contextualising cybercrime in Nigeria. The timeline (Table 3.7 & Figure 3.2) is a graphical visualization of cybercrime investigation in Nigeria looking at it from a historical perspective using pre-defined parameters over a period of 26 years from 1990 to date. These parameters were identified during the review of relevant literatures. The parameters identified are the population of Nigeria (NPC, 2016); the mobile phone users, internet users, penetration rate and data retention of CDR (NCC, 2016 & EFCC, 2004); the digital technology used in communication (NCC, 2017b); the laws and policies (Criminal Code, 1990; EFCC, 2004; NCC, 2003; AFF, 2006; Evidence Act, 2011; ACJA, 2015; Cybercrime Act, 2015); the initiatives used in tackling cybercrime (Eyitemi, 2011; Adomi & Igun, 2008; Nkanga, 2006; Ladan, 2015; ngCERT, 2014a; ngCERT, 2014b; NFIU, 2015; Abubakar, 2009; Waziri, 2009; Babafemi, 2011; Fabi, 2009; Oladipo, 2012; BBC, 2009) and stakeholders involved in investigating cybercrime (Criminal Code, 1990; EFCC, 2004; NCC, 2003; AFF, 2006); the approaches used in investigation (Abubakar, 2009; Chukkol, 2014); the cybercrime trends in Nigeria over the years (Tive, 2006; Stevens, 2006); the investigation, conviction and financial losses (EFCC, 2014; Sesan et al., 2012) and the challenges in investigating cybercrime (Adesina, 2017; Ajayi, 2016; Odumesi, 2015; Olusola et al., 2013b; Hassan et al., 2012; ITU, 2012; Oluwu, 2009). This map helps reveals the gaps and also understand how factors such as technology and Internet penetration affects cybercrime investigation.

Table 3.7 and Figure 3.2 illustrate the cybercrime investigation time (1990-2016)

Cybercrime Investigation Timeline (1990-2016) Table

PARAMETERS	TIME LINE				
	1990 - 2000	***2001 – 2002***	***2003 - 2006***	***2006 - 2011***	***2011 - 2016***
POPULATION	100 – 124 million	127 – 131 million	134 – 143 million	143 – 164 million	164 – 178 million+
MOBILE USERS	<200K*	266k – 1.5 million	3 – 32 million	32 – 109 million	109 – 214 million
INTERNET USERS	0 – 78k	113k – 414k	740k – 7.9 million	7.9 – 46 million	46 – 92 million
PENETRATION (%)	0 – 0.1%	0.1% - 0.3%	0.6% - 5.5%	5.5% - 28.4%	28.4% - 46.1%
DATA RETENTION	< 3 Months	3 Months	3 Months	3 Months	3M – 2 Years
TECHNOLOGY	PABX Telephony Fixed Wired	GSM Fixed Wired Fixed Wireless	GSM Technology Fixed Wired Fixed Wireless	GSM Technology CDMA Fixed Wired/Wireless	Smart Phones Cloud Computing 3G & 4G
LAWS & POLICIES	Criminal Code Penal Code	Criminal Code Penal Code	EFCC ACT 2003 NCC ACT 2003 AFF ACT 2006	EVIDENCE ACT 2011 EFCC ACT 2003 AFF ACT 2006	CYBECRIME ACT 2015 ACJA 2015
INITIATIVES	Special Fraud Unit	FATF Compliance EFCC Created	NFIU Created Cyber Café Raids Fix Nigeria Operation Octopus	Cyber Storm ANCOR & TCP Microsoft Partnership Eagle Claw	Cybersecurity Policy Cybersecurity Strategy NG-CERT EFCC-CERT
STAKEHOLDERS	**NPF, NITEL, CBN, LEA**	**EFCC, NPF, NCC, CBN, TELCOS**	**EFCC, NPF, NCC, CBN NFIU, TELCOS, ISPs**	**EFCC, NCC, CBN, TELCOS, ISPs**	**EFCC, NCC, TELCOS LEA, ISPs**
APPROACH TO INVESTIGATION	***Manual Analysis of:*** Fax, Telephone, Telex & Post Mail	Manual Tracing Manual Analysis	CDR Analysis Social Engineering Email Analysis Cyber Raids	Manual Scrolling Manual Extraction Manual Analysis	Digital Forensics OSINT Network Forensics Lawful Interception
CYBERCRIME TREND	AFF Letters Forged Financial Instrument	AFF Letters Scam Emails Yahoo-Yahoo Forged Instrument	SCAM Emails AFF Schemes Yahoo – Yahoo Forged Instrument	Romance Scam Contract Scam Yahoo – Yahoo Forged Instrument	Credit Card Fraud DDoS, Defacement ATM Cloning Hacking
INVESTIGATION	NA	NA	NA	NA	93 Cases (2013) 147 Cases (2014)
CONVICTIONS	NA	NA	NA	NA	NA
FINANCIAL LOSS ($)	NA	NA	NA	NA	$13 Billion (2012)
CHALLENGES	1. Cumbersome 2. Time Consuming 3. Unreliable	1. Time Consuming 2. Unreliable 3. No Forensics	1. Risky 2. No Forensics 3. Lack of Cyber Laws	1. No Cybercrime Act 2. Case Overload 3. Skill Sets	1. Training 2. Work Force 3. Workload Increase

Table 3.7: Cybercrime Investigation Timeline 1990-2016

Cybercrime Investigation Timeline (1990-2016) Map

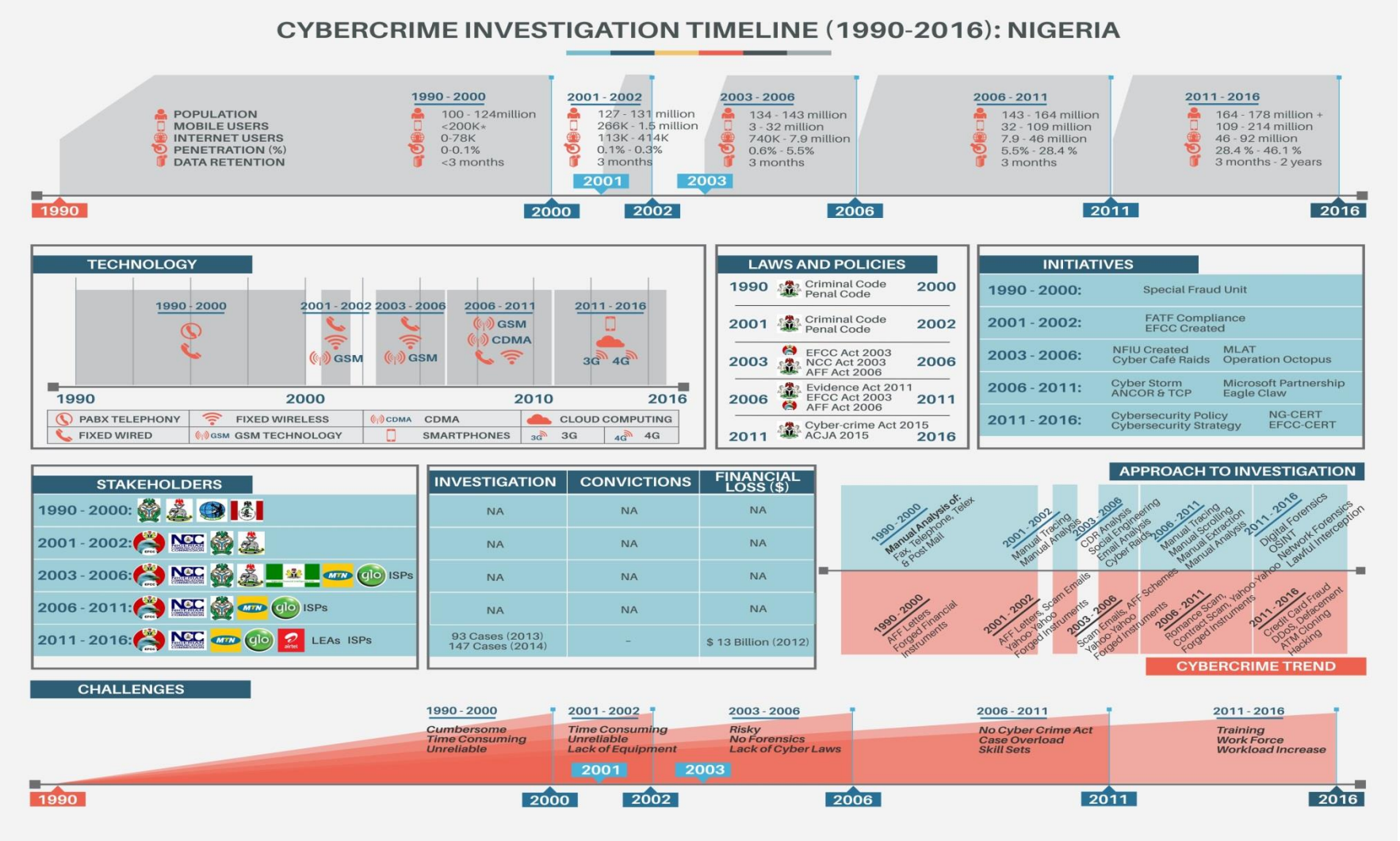


Figure 3.2: Cybercrime Investigation Timeline 1990-2016 Map

3.14 Critical Assessment

In order to review the literatures, the researcher did a critical assessment of the key components that are vital in understanding cybercrime in Nigeria. Also, since the research scope is narrowed down to cyber-enabled crime of advance fee fraud in Nigeria from a law enforcement perspective viewed through the theoretical lens of RAT, the researcher had to include variable such as 'causes of cybercrime' (section 3.5), 'limitations to investigating cybercrime (section 3.6) and role of other stakeholders and of LEAs (section 3.8 & 3.9) in understanding cybercrime policing in Nigeria. These key components and themes from the literature review formed the Cybercrime Investigation Timeline (1990-2016) that outlined some of the gaps in the current approach in investigating cybercrime.

3.15 Conclusion

In conclusion, this chapter reviewed the trends, laws, policies and stakeholders that are key stakeholders in the investigation and prosecution of cybercriminals in Nigeria. The chapter also examined the activity of the Economic and Financial Crimes Commission in tackling the menace of cybercrime over the years. Furthermore, it enumerated the challenges and limitation in tackling cybercrime, and stated the necessary recommendations to tackle it. Finally, it summarised the entire chapter with a detailed map of cybercrime investigation timeline in Nigeria.Table 3.8 showing the research objectives that were achieved by the researcher.

S/N	RESEARCH OBJECTIVE	ID	OBJECTIVE ACHIEVED
1	To examine the different definitions and categorizations of cybercrime through review of relevant literature.	**OBJ2**	**YES**
2	To explore the different forms of cybercrime that is prevalent in Nigeria through review of relevant literature and interviews.	**OBJ3**	**YES**
3	To understand the different reasons cybercrime is committed in Nigeria through review of relevant literature and interviews.	**OBJ4**	**YES**
4	To explore the benefits of partnerships in investigating cybercrime in Nigeria through review of relevant literature and interviews.	**OBJ5**	**YES**
5	To examine the current measures used by LEAs in Nigeria and the UK in tackling cybercrime.	**OBJ6**	**YES**
6	To examine the current measures used by LEAs in Nigeria and the UK in tackling cybercrime through review of relevant literature and interview of members of the CAC.	**OBJ7**	**YES**
7	To explore the current laws used in investigating cybercriminals in Nigeria through review of relevant laws and policies.	**OBJ8**	**YES**
8	To explore the challenges and limitations in investigating cybercrime in Nigeria through review of relevant literature and interview of members of the CAC.	**OBJ9**	**YES**

Table 3.8: Chapter 3 achievement of research objective and research question

4.0 CHAPTER 4: THEORETICAL FRAMEWORK

4.1 Introduction

This chapter gives an overview of the theoretical component of the research topic. It guides the formulation of the research objectives and questions and guides the researcher in narrowing down the scope of the research within various theoretical arguments in understanding crime and the policing of cybercrime within the Nigerian context. The chapter examines various theoretical arguments that fit into the research paradigm and justifies the selection of the theoretical argument that guides the researcher in understanding crime and cybercrime within the scope of law enforcement activities in acting as capable guardians in policing the internet.

4.2 Overview of Theories

McQuade (2006) defines theory as "an interrelated and testable set of propositions that explain a phenomenon". Theories can provide an in-depth understanding in developing appropriate crime prevention and enforcement strategies for protecting information systems and infrastructure. The classical school of criminology based on rational choice and deterrence theories only examined the 18th century legal structures and condemned or criticised arbitral punishments imposed on criminals without fairness, justice and concern for human rights (Williams & McShane 1993). McQuade (2006) argues that these writings did not consider the role of crimes committed with the aid of technology nor address "the social, physical or psychological implications of technologies used to punish offenders". However, Grabosky (2001), has argued that since the convergence of computing and communications has begun to change we live and the way we commit crime, it was important to emphasise that 'virtual criminality' was still in the same category as terrestrial crime. He further argues that the motivation of those who committed computer-related crime was still driven by 'time-honoured motivation of greed, lust, power, revenge, adventure and the desire to taste forbidden fruit'.

Criminological research has expanded its scope over the past two decades to improve our understanding of the impact of technology on the practices of offenders, factors affecting victims and the applicability of traditional theories of crime to virtual offenses (Bossler and Holt, 2014). New opportunities for crime and victimisation presented by technological changes have been acknowledged by criminologists (Clarke 2004; Cohen and Felson, 1979) and Clarke (2004:55) has argued that 'the internet has created a completely new environment in which traditional

crimes- fraud, identity theft and child pornography-can takes new forms and prosper'. Reyns (2013) further argued that only a little technological advancement has had a profound impact on societal routine activities and was especially true of the advent of the Internet. According to Kigerl (2012), criminal law is only as good as the criminological theory underlying the behavior it is intended to deter or limit. There have been debates on applying new theories of crime to cybercrime considering it to be in a different category to terrestrial crime (Adams, 1998; Capeller, 2001), However, Yar (2005) has argued that Routine Activity Theory previously applied to aggregate level crime rates has been considered appropriate for cybercrimes.

This research will draw on the principles of four criminological theories namely routine activity theory, general deterrence theory; general theory of crime; and theory of technology enabled crime. These theories have some or all of the components that are relevant to the research in understanding cybercrime vis-à-vis traditional criminological assumptions on crime and deviant behaviours.

4.3 Routine Activity Theory (RAT)

Within the scope of classical and choice theory, the perception of the available opportunities to commit crime was considered as an essential element (McQuade 2006). Cohen and Felson (1979) argued that for crime to take place, three requirements needed to be present namely, a motivated offender, a suitable target and an absence of a capable guardian. The RAT approach to crime causation is ecological and the accessibility, location and presence or absence of certain characteristics or people is what proves to be predictive of criminal behaviour (Kigerl, 2012; Cohen and Felson, 1979). Akers and Sellers (2004), stated that a motivated offender must be someone who is willing to commit a crime and for whom the opportunity was present to allow the crime to be committed. A suitable target is the one the motivated offender values such as credit card information and that target also be visible, accessible and able to be illegally obtained by the offender (Clarke and Felson, 1998). Finally, the capable guardian must be absent; a capable guardian such as encryption, anti-virus or law enforcement officer is any person or thing that obstructs the motivated offender from acquiring the target (Cohen and Felson, 1979). Figure 4.1 illustrates the variables of RAT.

Figure 4.1: Variables of Routine Activity Theory

4.3.1 Suitable Target

Cohen and Felson (1979) argued that structural changes in combined routines can influence the convergence in time and space of motivated offenders and suitable targets in the absence of capable guardians. The theory argues Holtfreter et al. (2010) assumes that a constant supply of motivated offenders focuses on the behaviours, activities and situational contexts that place potential targets at risk of victimisation. According to Reyns (2013), at the time routine activity theory was introduced by Cohen and Felson (1979), the Internet did not exist, and the assumption was that most offenses would take place between a motivated offender and a suitable target at a physical location in the absence of capable guardians. Reyns (2013) argued that with the advancement of technologies, access to the internet and the capability to participate in these remote activities continues to increase. The increase in Internet-based routine activities and the gradual increase of criminal opportunities have made it appropriate to adopt the theory to crimes in which both the victim and offender do not physically meet. Wall (2005) mentions that, the internet has created a transnational environment that gives new opportunities for criminal activities which are currently a subject of existing criminal and civil law. However, Yar (2005) argued that in understanding routine activity theory, the suitable target that is being attacked can be understood according to its four-fold constituent properties namely value, inertia, visibility

and accessibility. He states that the offenders rationale for picking a suitable target depends on whether the target is for 'personal pleasure, for sale,' or to be used in perpetuating another criminal or non-criminal activity. The target of cybercrime like terrestrial crime vary and attract different valuations as Yar (2005) further states that most cybercrime targets are 'informational in nature', because all entities present and move on the internet are forms of digital code. According to Bennett (1991:148), routine activity theory argues that there is connection between target visibility and suitability as the 'potential offender must know of the existence of the target'. As such, Yar (2005) argues that properties and persons that are more visible to the offender are likely to become targets because the internet is a public domain unlike closed ICT networks such as VPNs and intranets. Clarke (2004:55) has argued that, 'the internet has created a completely new environment in which traditional crimes – fraud, identity theft and child pornography can take new forms and prosper'. According to the Internet World Stats (2016) as of June 2016, the world internet population is more than 7.3 billion users. Furthermore with an increasing internet penetration especially in developing countries, the number of targets and offenders increases daily. It is difficult to estimate how many users of the internet are using it for illegal activities (UNODC, 2013). In understanding accessibility of a suitable target, Felson (1998:58) states that the term means the 'ability of an offender to get to the target and then get away from the scene of a crime'. Yar (2005) argued that 'the greater the target's accessibility, the greater its suitability, and vice versa'. Felson (1998:55) argued that, the valuation of the target will vary according to the shifting value attached socially and economically to particular goods at particular times. Also, factors such as scarcity and fashion will determine in placing value on the target by offenders and others. However, the offenders rationale in a particular target rests upon whether the target is for 'personal pleasure, for sale,' or to be used in committing another crime (Yar, 2005).

4.3.2 Motivated Offender

Clarke and Felson (2008:2) argued that three minimal elements for direct-contact predatory crime are a likely offender, a suitable target, and the absence of a capable guardian against crime. They further state that a likely offender was anybody who for any reason might commit crime. Lopez (2014) maintains that in RAT, a crime can only take place if there is a motivated offender, thus, meaning that there must be a motive to begin with. The motive varies based on the

objective of the offender, and most often motivated offenders as elements of crime are very difficult to control or foresee in the prevention of crime. The digital era has begun to pose new challenges for many countries and yet many governments and legal systems are limited in their ability to adopt the new technologies, thus, limiting the functions of the traditional police. As we have seen, the motives for computer-related offences are nothing new, technology may change rapidly but human nature does not change as succinctly expressed by Grabosky (2001), 'old wine in new bottles'. Grabosky (2001) further argues that, the unprecedented growth of the internet and communications technologies has created parallel opportunities for prospective offenders and parallel risk for prospective victims. As the internet continues to be the backbone of future commerce, it will be increasingly used as a medium of fraud.

4.3.3 Absence of a Capable Guardian

Over the years, capable guardianship has evolved from knights of feudalism to the private security services of modern times which vastly outnumber sworn police officers in many developed economies (Grabosky 2001:248). Guardianship refers to 'the capability of persons and objects to prevent crime from occurring' (Tseloni, Farrell, Pease and Wittebrood, 2004). Routine activity theorists argue that the mere presence of a guardian in proximity to the suitable target is a crucial deterrent. Where the capable guardian is a person, he/she acts as someone 'whose mere presence serves as a gentle reminder that someone is looking' (Yar, 2005). The policing of crime in both terrestrial and cyberspace has become a 'pluralistic endeavour' as responsibilities for the control of cybercrime will be similarly shared between law enforcement officers, information security specialists and individual users. The first line of defence as it has always been with the terrestrial space is self-defence (Grabosky, 2001).

A guardian can be anyone or anything that creates a protection on the target victim. The motivated offender is discouraged from committing an offense when they know that the target has a guardian. Therefore, capable guardians as elements of crime can be controlled, modelled or changed to prevent crime (Lopez, 2014). Also, Tseloni et al. (2007:74) referred to guardianship as 'the capability of persons and objects to prevent crime from occurring'. However, Cohen and Felson (2008:3) stated that the capable guardian 'was not to seen to be a policemen or security guard in most cases'. This was a deliberate attempt to distance routine activity theory from the rest of criminology because it is entrenched to the criminal justice system as central to crime

explanation. Cohen and Felson (2008) further argued that the most likely persons to prevent a crime is not a police officer but rather friends, neighbours and owners of a targeted property. They state that the absence of a suitable guardian is important, as an offender must find a suitable target in the absence of a guardian before a crime can occur. Although there may be direct intervention, Yar (2005) argued that routine activity theorist view 'the simple presence of a guardian in proximity to the potential target as a crucial deterrent'. In understanding the concept of guardianship in the cyber world, Yar (2005) contended that it depends on the guardians presence together with the suitable target at the time when the 'motivated offender converges upon it'. However, Felson (1998:53) stated that the problem faced by guardianship is more intensified in the cyberspace than in the terrestrial world because in the terrestrial space, the police 'are very unlikely to be on the spot when a crime occurs' while in the cyberspace it is only when informal guardianship has failed that a formal assistance of LEAs are sought. In summary, RAT concept of guardianship as argued by Yar (2005) is applicable to cyberspace even when the 'structural properties of the environment amplifies the limitations upon a establishing' a cyberspace guardianship.

This theory is considered appropriate when applied to cybercrime in Nigeria, because it extends the criminological understanding of deviant behaviours and the applicability of motivated offenders, suitable target and guardianship with the scope of the research.

4.4 General Deterrence Theory

General deterrence theory generally combines choice theory with rational choice theory because people can be deterred from choosing to commit crime on the basis of severity, swiftness and the certainty of punishment. This theory stipulates that stiffer fines and harsher penalties deter people from committing crime in the first place or encourage them to commit lesser crimes. A key component of deterrence is publication of potential and actual punishment as a form of deterrence (McQuade 2006). McQuade (2006) further argues that imposing and publicising penalties received by offenders is the fundamental concept underlying general deterrence theory. Informal sanctions can also deter individuals from committing IT-enabled abuse and cybercrimes.

Even though, this theory is suitable to this research, it would require the collection of empirical quantitative and qualitative data through surveys and interviews to be able to ascertain whether

deterrence is a veritable tool in crime prevention in Nigeria. Therefore, this theory was not adopted as the research is framed from an interpretivist paradigm and a qualitative approach to collecting data.

4.5 Theory of Technology-Enabled Crime

The advancement of the internet and the accessibility of computer technology has created new opportunities for individuals and businesses as well as those who engage in fraudulent activities. The rise of emerging technologies and online communication has not only resulted in an astronomical increase in criminal activities but has also resulted in new forms of deviance and criminal online behaviours. This has posed challenges for the legal systems as well as law enforcement agencies across the globe (Brenner, 2007). Olayemi (2014a) argues that the theory combines several components of criminological theories to better understand why crime related to "computer and telecommunications technology" is amongst the most difficult forms of crimes to prevent, investigate and control. McQuade (2006) states that technology-enabled crime theory accounts for: (a) Technological evolution and relative complexity of new forms of crime; (b) Technological and economic factors that creates innovative forms of social abuse and crimes; and (c) Technological shifts in criminal, policing and security management capabilities.

The theory provides a framework for understanding all forms of criminality especially deviant behaviours that are perpetrated online or with the help of telecommunications technologies. The theory is also vital in examining contemporary threats posed by new trends of cybercrime, transnational crime and the terrorism networks that have defied traditional approaches of the criminal justice system in their prevention and control crime (Olayemi, 2014a).

The theory was considered, however, there are few criminological literatures available in understanding the applicability of such theory to this research context within the scope of LEAs in Nigeria. Also, the theory would require the collection of quantitative and qualitative empirical data in order to understand the issues involved in policing cybercrime in Nigeria.

4.6 General Theory of Crime

The general theory of crime was coined by Gottfredson and Hirschi (1990). They claimed that their theory had a universal status as it was valid across time and space. They argued that the cultural imbalance theories which they defined as those theories that applied only to particular

cultures has tended to dominate traditional comparative criminology. Proponents of these theories, such as Marenin and Reisig (1995), stated that each culture had its own definitions of crime as well as historically specific root causes of crime and deviance. Therefore a theory explaining common 'criminogenic factors across cultures cannot be developed'. Thus, Gottfredson and Hirschi (1990:174-175) argue that:

> *Cultural variability is not important in the causation of crime, that we should look for constancy rather than variability in the definition and causes of crime, and that a single theory of crime can encompass the reality of cross-cultural differences in crime rates.*

Gottfredson and Hirschi (1990:15) argued that people who commit crime, which they define as 'acts of force or fraud undertaken in pursuit of self-interest,' are characterised by low levels of self-control which forms the very core concept in the general theory of crime. They further argue that individuals are governed by pain, pleasures and self-interest calculation, thus, lacking any 'innate conscience which extends beyond themselves and must be socialized to morality'. As crime is committed within specific contexts, Marenin and Reisig (1995) argued that, Nigeria is as a developing country that has oil but an expanding population, implied that the needs of the population were greater than the vast amount of money generated by the revenue from oil. Amongst the consequences of a growing population and a small per capita income are the development of massive and visible differences in wealth and lifestyles, the salience of classes in public life and the possibilities for massive corruption in the country. Crime in Nigeria can be divided into three categories of normal, political-economic and riotous. The main problem with Gottfredson and Hirrschi (1990) general theory is the differences in levels of crimes in Nigeria. The theory needs to account for the main factors that are peculiar to the country like developing status, political instability, economic insecurities and group dynamics. Personal factors such as self-control also plays out within these general contexts. The vast majority of Nigerians, argued Marenin and Reisig (1995), despite all temptations and societal pressure were still law-abiding. Some commit crime according to the general theory of crime and some do not despite lacking self-control. However, Odekunle (1986:93) maintains that the activities of elites in the country does far more damage to its reputation and people than normal crime and crime committed by the working class. He argues further by stating that, 'the real criminals in the country are the elites; their crimes are part of their routine and normal day-to-day business and functions; the

cost of their crimes to the nation is incalculable but it is enormous, cumulative and treasonable.' In summary, the general theory of crime despite being universal and cross-culturally accurate only at certain levels offers little and limited insight into understanding the structure or multi-faceted dynamism of criminality and cybercrime in Nigeria.

4.7 Selected Theoretical Framework

Routine Activity Theory (RAT) was adopted as the theory's approach to crime causation is applicable in understanding cybercrime in Nigeria. The theory analysis of a suitable target extends the understanding on victims of cybercrime in Nigeria. The theory also attempts to understand the motives of cybercriminals in Nigeria as to what Grabosky (2001) called, 'old wine in new bottles'. Finally, the theory is appropriate as it considers the suitability of a capable guardian from a law enforcement perspective, whose 'mere presence' argued Yar (2005) serves as a deterrent. Detailed discussion on RAT application to research scope in (Section 8.3).The use of Grabosky 'old wine in new bottle' alludes to the fact that the motive of a cybercriminal and that of traditional criminal are mostly the same and usually to gain an illegal advantage over their victims. The research is trying to understand amongst other things whether cybercriminals in Nigeria as 'motivated' offenders are geared towards committing crime based on 'greed and financial gain'. Thus, the use of Grabosky 'old wine in new bottle' is appropriate in explaining RAT 'motivated offender' in understanding cybercriminals in Nigeria. Figure 4.2 illustrates the seven case studies that participated in the research.

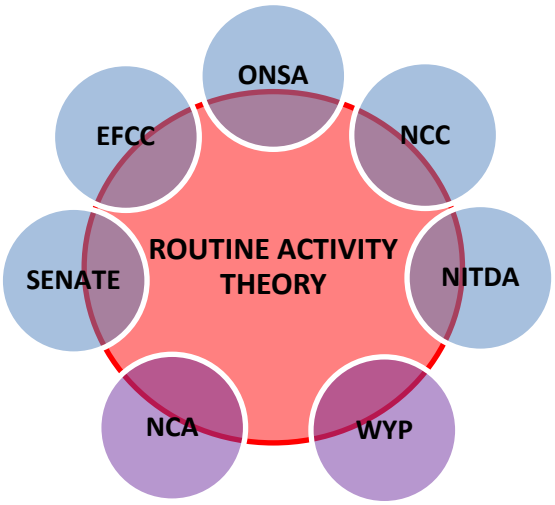


Figure 4.2: Correlation between Theoretical Framework and Case Studies

4.8 Conclusion

In conclusion, the theoretical framework chapter presents classical and modern criminological theories and their application to understanding cybercrime within the research scope. The chapter gave an argument and justification of the selected research theory.

5.0 CHAPTER 5: RESEARCH METHODOLOGY

5.1 Introduction

This chapter aims to examine the research methodology used in this study so as to properly understand and identify the relevant approaches needed to adequately address the research questions underlying this research. The methodologies would further take into account the various components in formulating and designing research such as the philosophy of the research, approach and research strategies and techniques used in order to better understand the aims and objectives of the research.

Furthermore, issues such as validity, reliability and the ethics of research will be elaborated. In order to achieve the aim of the research, the following guidelines were formulated in order to fulfill each phase of the research process and progression:

1. To elaborate the significance of research and the meaning of research.
2. To discuss and justify the research approach adopted
3. To explore the research philosophy and establish the epistemological and ontological positions which form the foundation of the approaches undertaken.
4. To justify the research design chosen and theoretical framework used in the research.
5. To study and justify the most appropriate data collection techniques used.
6. To select the most suitable method for the analysis and interpretation of data collected.
7. To elaborate on the issue of research validity and reliability.
8. To discuss the issues of ethics in research and how it was strictly observed.

There are different methodologies used to understand how to conduct a research. Walsh (2001) argues that the most common approach views research as a series of practical skills and activities that are used in order to conduct a particular type of investigation. This type of research views a project from the perspective of what the researcher does and the methods in which they conduct the research. However, Kumar (1996) views research as a way of thinking and further explains that the approach aims to understand research by using critical questions, examination of data collected and using them to understand a problem more thoroughly.

5.2 Research Model

In order to adapt a model for a research design, there is a need to comprehensively review literatures on various research methodologies and designs. However, there are varied views, interpretations and frameworks used by researchers throughout the description of the research process. Also many authors are not categorically clear on how the sequencing of the research deliverables is within their models. Authors such as Saunders et al (2016) and Crotty (1998) argue that in most social research literature, the majority of the discussion and the terminology relates one way or the other to four elements namely methods, methodology, theoretical perspective and epistemology. This research has adopted a theoretical path based on Crotty's (1998) study of the hierarchal levels of research and Saunders et al. (2016) 'research onion'. This methodological pathway will guide the researcher in order to systematically approach and conduct the research study effectively.

Figure 5.1: Methodological Theoretical Phases (Adopted from Saunders et al., 2016; Crotty, 1998)

Each of these stages are now discussed insofar as they relate to the current research.

5.3 Research Philosophy

The research philosophy a researcher adopts is based on certain assumptions of ways they view the world. These assumptions form the basis for a researcher's strategy and the methods to be used as part of those strategies (Saunders et al 2016). Saunders et al., 2012 (p.102) further argues that the philosophy a researcher adopts would be influenced by practical considerations and more so by the perception the researcher has of the relationship between knowledge and the process by which it is developed.

The relationship between the data collected or analysed and theory is one of the heavily contested debate amongst philosophers for centuries and the failure to properly understand philosophical issues can negatively affect the quality of research (Easterby-Smith, Thorpe and Jackson 2008).

Easterby-Smith (2008) argues that there are three critical reasons why philosophical understanding of research is so important. Firstly, it assists in clarifying the research design. This not only includes considering what kind of evidence is needed and how it is collected and analysed but also how it provides appropriate answers to fundamental questions investigated in the research. Secondly, having a knowledge of philosophy helps a researcher to make the best decision in choosing which design is most appropriate. It guides the researcher to avoid wasting time on figuring out which design approach to use and also to recognise their limitations. Thirdly, it helps researchers to identify and create designs that are not part of their previous research experience. It further suggests how to adapt research designs according to limitations of different subject areas.

Oates (2014) argues that, in understanding that researchers have different roles of either being subjective or objective, different research strategies can be both acceptable and good academic research because they have different "underlying philosophical paradigms".

According to Saunders et al. (2016) a clearly thought out and consistent set of assumptions will make a credible research philosophy which will determine the methodological choice, research strategy, data collection methods and analysis. Clearly, it is the researcher's assumptions about the world that determines what approach and strategies to use. Researchers in business and management need to be conscious of the philosophical commitments that are considered

throughout the choice of the research strategy because it has an impact on how research is understood and undertaken. Saunders et al. (2016) also agrees that the philosophy of research is an important foundational phase in any research process.

5.3.1. Epistemology and Ontology

Oates (2014) argues that philosophical paradigms consist of "different views about the nature of our world (ontology) and the ways we can acquire knowledge about it (epistemology)".

Ontology can be defined as the assumptions about the nature of reality. It also shapes the manner in which we see and study our research objects; therefore, ontology determines how we see the world and the choices of what to research in a research project (Saunders et al. 2016). Easterby-Smith et al (2008) argues that amongst philosophers of natural science, the discussions and debate is between realism and relativism. Realism comes in several forms. Traditional realists begin by stating that the world is concrete and external and that only through observation can science progress to have a direct correlation with the phenomenon being investigated (Easterby-Smith et al. 2008). On the other hand, Easterby-Smith et al. (2008) argue that internal realists concentrate more often on the process of observation (epistemology) and they accept that scientific laws once discovered are absolute and independent from further observation. The relativist states that scientific laws 'may not be quite immutable'. As Collins (2010) argues, the relativist identifies that there are many truths and that scientific laws are not just to be discovered but that these truths are determined by the views of the observer. Therefore, relativist ontology assumes that different observers would have varied views that what is important can vary from time and place.

O'Leary (2007) defines nominalism as a view that abstract concepts do not exist outside our mind and have no corresponding reality. Nominalism can therefore be seen as the opposite of realism. The position of nominalism argues Easterby-Smith et al. (2008), is that it includes the labels and names we associate with experience and events which are important.

Ontology must be considered together with epistemology as the two are equally dependent on one another and difficult to conceptually distinguish when discussing issues related to research (Crotty 1998). Crotty (1998) further argues that talking about the construction of meaning (epistemology) is talking about the construction of a meaningful reality (ontology). Therefore,

epistemology involves knowledge and embodies an understanding of what it means to know, that is 'how we know what we know' (Crotty, 1998:8). Easterby-Smith et al. (2008:60) defines epistemology as a 'general set of assumptions about the best ways of inquiring into the nature of the world'. These positions have been depicted in the table 5.1 below

Ontology of Social Science	**Representationalism**	**Relativism**	**Nominalism**
Truth	Requires verification of predictions	Is determined through consensus between different viewpoints	Depends on who establishes it.
Facts	Are concrete, but cannot be accessed directly	Depend on viewpoint of observer	Are all human creations
Epistemology of Social Science	**Positivism**	**Relativism**	**Social Constructionism**

Table 5.1: Ontologies and Epistemologies in Social Science (Adapted from Easter-Smith et al. 2008)

Based on the analysis above, this researcher's ontological position is that of relativism due to the fact that different observers would have varied views which are interpreted differently at various times and various places. This position was reached as Easterby-Smith et al. (2008) argued that ontology dealt with the nature of reality while epistemology dealt with the connection between reality and the researcher.

5.4 Research Paradigms

Bryman and Bell (2015) state that paradigms are used to describe a group of beliefs that forms the general world view of the researcher. Paradigms influence what should be studied, how it should be studied and how the results should be interpreted. However, Collis and Hussey (2009) argue that, the term paradigm is often used loosely in academic research and has a different meaning to different people. Mertens (2003:139) summarises the definition of paradigm as a 'worldview, complete with assumptions that are associated with that view'. However, more recently, Morgan (2007:49) defined paradigm as a 'system of beliefs and practices' that helps researchers choose both their research questions and methodology. Creswell (2009:6) argues that discipline, beliefs of advisors and past experiences are what shape the paradigm of an individual when conducting research.

5.4.1 Traditional Approaches

Many centuries ago, there was only one research because the 'scientific achievement' argued by Kuhn (1962) came from one source. Presently, we refer to that source as *natural science* in order to distinguish them from the *social sciences.* The emergence of the social science led to the development of another research paradigm.

Smith (1983) stated that until the 19th century, most research focused on inanimate objects of the physical world such as physics. The approach used by most of these scientists was through observation and experiment. Their belief about the world and knowledge was based on a paradigm called positivism which had its roots in realism. However, with the coming of industrialization and capitalism, Collis and Hussey (2014) argued that researchers turned their attention to 'social phenomena'. A phenomenon is defined as 'an observed or apparent object, fact or occurrence'. From the outset, the new social scientist utilised the methods established by natural scientists but the compatibility of the traditional approach was challenged and criticised by many theorists which went on for many decades (Smith, 1983). The alternative to positivism can be referred to as interpretivism.

5.4.1.1 Positivism

Collins and Hussey (2014) argue that positivism is based on the belief that reality is independent of us and the aim is to discover theories based on empirical research through observation and experimentation. Similarly, Saunders et al. (2016) refer to positivism as the 'philosophical stance of the natural scientist and entails working with an observable social reality to produce law-like generalizations'. Researchers conducting a research based on the positivist paradigm are still focusing on theories to explain and predict a social phenomenon. They still embrace logical reasoning so that their approach is based on precision, objectivity and rigour rather than on being subjective (Creswell 2014). Positivism is also defined as 'a perspective which assumes that the properties of the social world can be studied using objective scientific methods' (Huzynski and Buchanan, 2007:15). However, since it is assumed that social phenomena can be measured, positivism is associated with quantitative methods of analysis (Collins and Hussey, 2014). Many authors have criticised positivism since interpretivism was developed as a result of the inadequacies of positivism. Such criticisms of positivism as elaborated here are:

a. It is impossible to divide people from the social contexts in which they exist.
b. People cannot be understood without examining the perceptions they have of their own activities.
c. A highly structured research design imposes constraints on the results and may ignore other relevant findings.
d. Researchers are not objective, but part of what they observe. They bring their own interests and values to the research.
e. Capturing complex phenomena in a single measure is misleading. (Collis and Hussey, 2014:45)

5.4.1.2 Interpretivism

Saunders et al. (2016) argues that Interpretivism like critical realism was developed as a critique of positivism from a subjective perspective. It emphasizes that humans differ from physical phenomena because they create meaning. The central theme of Interpretivism is that the world is subjective and socially constructed (Remenyi et al., 2005). Collis and Hussey (2014) thus, argue that Interpretivism is based on the belief that social reality is not objective but highly subjective because reality is shaped by our perceptions. Interpretivism focuses on exploring the complexity of social phenomena with the aim of acquiring an interpretive understanding. Therefore, interpretivist adopt a range of methods that 'seek to describe, translate and otherwise come to terms with the meaning, frequency of certain more or less naturally occurring phenomena in the social world' (Van Maanen, 1983:9).

Saunders et al. (2016) argue that the focus of an interpretivist study is to understand the meanings and interpretations of 'social actors'; therefore, understanding their worldview is so complex to be widely generalised. Understanding what people think and how they communicate (verbally or non-verbally) and feel is important (Easterby-Smith et al., 2014).However, similar to positivism, Hammersley (2013) has some criticisms of interpretivism:

a. Descriptions are too vague and inconsistent in providing a sound basis for comparing the orientations of different people and their characteristics within different situations.
b. It does not provide a means of showing how one set of factors, rather than another, plays a key role in bringing about particular outcomes.
c. It encourages the study of a small number of cases, thereby failing to provide a platform

for broader conclusions.

d. It is preoccupied with a coherent and newsworthy narrative, rather than checking the validity of the interpretations produced.
e. It presents the standpoint of the researcher, rather than that of the true response provided by the individuals being studied.

5.4.1.3 Assumptions of positivism and Interpretivism

Collis and Hussey (2014) state that before any research project can be designed, the researcher must consider the philosophical assumptions that underpin Interpretivism and positivism in order to determine whether your research orientation at this stage is 'broadly interpretivist or broadly positivist'. Prior to a researcher's decision to choose a particular paradigm, considerations must be given to more modern approaches to research paradigm. Due to the criticisms, debates and inconsistencies of the traditional approach, it has led to a series of new formulations of paradigms based on the traditional approach. These modern approaches will be analysed before the chosen research paradigm of this study is presented. Table 5.2 shows a comparison between the philosophical assumptions of positivism and Interpretivism.

Philosophical Assumption	Positivism	Interpretivism
Ontology	Real, One true Reality, Granular things.	Multiple realities; subjective and socially constructed.
Epistemology	Scientific method; observable and measurable; Researcher distant from phenomena under study.	Knowledge comes from subjective evidence from participant; Theories and concept too simplistic.
Axiology	The results are unbiased and value-free; Researcher maintains objective stand.	The findings are biased and value-laden; Researchers interpretations key to contributions.
Methodology	The researcher takes a deductive approach; Large samples and typically quantitative methods of analysis.	The researcher takes an inductive approach; small samples and typically qualitative methods of analysis
Rhetorical	The researcher uses the passive voice, accepted quantitative words and set definitions.	The researcher uses the personal voice, accepted qualitative terms and limited a priori definitions.

Table 5.2: Assumptions of the two paradigms (Adapted from Collis and Hussey 2014; Saunders et al. 2016)

5.4.2 Modern Approaches

Collis and Hussey (2009) mention that, there are other approaches within the two main paradigms of positivism and interpretivism. Under the modern approaches the researcher will discuss Pragmatism, Post-Positivism, Transformative and Constructivism.

5.4.2.1 Pragmatism

Pragmatism originated in the late 19th century USA mostly in the work of Charles Pierce, William James and John Dewey. It seeks to reconcile objectivism and subjectivism, facts and values, different experiences and accurate and rigorous knowledge. It achieves this by considering 'theories, concepts, ideas, hypotheses and research findings not in an abstract form, but in terms of the roles they play as instrument of thought and action, and in terms of their practical consequences in specific context' (Saunders et al. 2016). Collis and Hussey (2014) argue that rather than be restricted by a single paradigm, pragmatist advocate that researchers should be 'free' to mix methods from different paradigms choosing them based on their usefulness in answering the research question.

Creswell (2014) criticizes pragmatism through seven points by comparing them with his views of mixed method research. He states the following:

a. Pragmatism is not committed to any one system of philosophy and reality. This certainly applies to mixed methods, as researchers use both quantitative and qualitative assumptions when they conduct their research.
b. Individual researchers have a freedom of choice. Therefore, researchers are free to choose the methods, techniques and procedures that best suit their needs and purposes.
c. Pragmatists do not see the world as an absolute unity. Evidently, mixed methods researchers use different approaches in collecting and analysing data rather than using only one approach.
d. Truth is what works at the time. In reality, mixed method researchers use both qualitative and quantitative data in order to best provide the understanding of a research problem.
e. Pragmatists agree that research always occurs in social, historical, political, and other context. Mixed methods studies may include a 'postmodern turn, a theoretical lens that is

reflective of social justice and political aims'.

f. Pragmatists look to the 'what' and 'how' to research based on intended consequences. Mixed methods researchers need to establish the purpose of their research and a rationale as to why quantitative and qualitative data needs to be mixed in the first place.
g. Pragmatists believe in an external work independent of the mind as well as what is lodged in the mind.

5.4.2.2 Post Positivism

Teddie and Tashakkori (2009) argue that post-positivism was developed as a result of dissatisfaction with positivism. Post-positivism is a term used to represent the thinking after positivism, thus, challenging the traditional notion of the absolute truth (Phillips and Burbules, 2000). Creswell (2014) state that positivist's hold a deterministic philosophical stand in which 'causes' determine 'outcomes'. Therefore, the problem studied by post-positivists reflects the need to identify and examine the causes that affect outcomes. Key assumptions of post-positivism can be highlighted as the following:

a. Knowledge is conjectural, thus, absolute truth can never be found. Therefore, evidence established in research is always fallible.
b. Research is the process of making claims and then refining and discarding some claims for more robust ones.
c. Data, evidence, and rational considerations shape knowledge.
d. Research seeks to develop relevant valid statements. The ones that can adequately explain the situation or describes the causal relationship being investigated.
e. Being objective is an essential aspect of competent inquiry; researchers must examine methods and conclusions for bias (Creswell, 2014).

5.4.2.3 Transformative

Transformative approach is another group of researchers that have a modern philosophical assumption. This approach started between the 1980s and 1990s by researchers who criticised the post-positivist assumptions of mandated structural laws and theories that did not fit marginalised individuals in the society or current issues such as oppression, discrimination and

social justice that needed to be addressed (Creswell 2014).

Mertens (2010) argues that a transformative worldview states that research inquiries need to be interconnected with politics and a political change agenda to confront social oppression at all levels at which it occurs. This approach assumes that the inquirer will proceed collaboratively so as not to marginalise the participant as a result of the inquiry. Transformative research provides a platform for these participants, thereby raising their consciousness or advancing an issue in order to improve their lives (Creswell 2014).

Mertens (2010) carefully summarizes the main features of the transformative paradigm as follows:

a. It places central emphasis on the study of lives and experiences of diverse groups that have been traditionally marginalised.
b. The approach focuses on the inequities of these diverse groups based on gender, race, sexual orientation, ethnicity, diversity that result in asymmetric power relationships.
c. The approach links political and social actions to these inequities.
d. The approach uses a programmed theory of beliefs about how a programme works and why the issues of domination, oppression and power relationships exist.

5.4.2.4 Constructivism

Constructivism or social constructivism proposes that reality is constructed through social interaction whereby social actors create partially shared meanings and realities (Saunders et al. 2016). Creswell (2014) argues that 'social constructivists' individuals seek understanding of the world and environment they live and work in, thereby developing subjective meanings from their experiences. The meaning varies and is multiple which leads the researcher to look for the complexity of the views rather than narrow down the views into a few categories of ideas. Easterby-Smith (2008) argues that one of the strength of this approach is that data collection is less artificial and it is flexible and good for theory generation. However, he further states that, the approach can be time consuming and may not have credulity with policy makers. Creswell (2014) states that the researcher's aim is to make sense of the meanings others hold about the world and rather than start with a theory, inquiries generate or inductively develop theory.

In discussing constructivism, Crotty (1998) highlights some of the several assumptions:

a. Human beings construct meanings as they interact with the world they are interpreting. Qualitative researchers usually use open-ended questions so that participants can share their views.
b. Humans engage with their world and make sense of it according to their historical and social perspectives. Therefore, qualitative researchers seek to understand the context or setting of the participant by visiting the context and gathering information personally.
c. The basic generation of meaning is always socially based on constant interaction with the human environment. The process of qualitative research is mostly inductive as the inquirer generates meaning from the data collected in the field.

5.5 Selection of Research Paradigm for Research

Several authors such as (Saunders et al., 2016; Collis and Hussey, 2009; Easterby-Smith et al., 2008) have different classification of research paradigms. While some agree that modern approaches developed from the traditional approaches, others differ. However, after examining both traditional and modern approaches the researcher will be adopting the traditional interpretivist point of view based on the following rationales:

a. The phenomenon of cybercrime has multiple realities, thus it is subjective and socially constructed. The factors explaining cybercrime in Nigeria might not necessarily be the same factors that affect it elsewhere. The main aim of the research is to identify any improvement in the laws, policies and approaches within the scope of LEAS in Nigeria and UK in tackling cybercrime.
b. The data and information being sought through literature review and interviews are subjective and the researcher's interpretations are key to the contribution of this research.
c. This study has taken an inductive approach and is collecting qualitative data for analysis

5.6 Classification of Research Methodology

Collis and Hussey (2014) argue that research can be classified according to purpose, process, logic and outcome of the research. Classification based on the purpose of the research which entails the reasons why the research is conducted can be categorised as exploratory, descriptive,

analytical or explanatory and predictive. Saunders et al. (2016), however, argue that research can be designed to fulfill either an exploratory, explanatory, descriptive or evaluative purpose, or some combinations of these.

5.6.1. Exploratory Research

Exploratory research is used to define the questions or hypotheses to be used in a research study. It is used to guide the researcher's understanding of a research problem and might be used where there is little literature about the subject matter, thus, the real-life phenomenon is investigated in order to identify the topics to be researched in the study (Oates, 2012). Saunders et al. (2016) point out that research questions that are exploratory are more likely to begin with 'What' or 'How'. Furthermore, questions that are asked during the data collection to understand and explore the issue, problem or phenomenon will likely start with 'What' or 'How'. There are a number of ways to conduct exploratory research through review of literature, interviewing 'experts' in the subject matter; conducting in-depth interviews or conducting focus group interviews.

Collis and Hussey (2014) states that, exploratory research focuses on gaining insights and understanding about the issue or problem being investigated for more detailed investigation to be conducted at a later stage. Therefore, exploratory research hardly provides conclusive answers to the problem at issue but rather gives guidance on what future research if any should be further conducted.

5.6.2 Descriptive Research

Descriptive research is conducted to describe a phenomenon as it exists. It is usually used to identify and acquire information on the characteristics of a specific problem or issue (Collis and Hussey 2014). However, Saunders et al. (2016) argue that the main purpose of descriptive research is to gain an accurate profile of events, persons or situations.

Descriptive research questions are likely to begin with, or include, either 'Where', 'Who', 'What', 'When' or 'How'. Questions asked during the data collection phase of the research likely to start with, or include, 'Who', 'What', 'When', 'Where', or 'How'.

Oates (2016) states that descriptive research leads to a detailed and rich analysis of a particular phenomenon and its context. Descriptive research may be an extension of a piece of exploratory research (Saunders et al. 2016).

5.6.3 Explanatory Research

Explanatory or analytical research is a continuation of a descriptive research. Researchers doing explanatory research do not just describe the characteristics but also analyse and explain why and how the phenomenon being studied is happening. Therefore, explanatory research seeks to understand a phenomenon by discovering and measuring the causal relations among them (Collis and Hussey, 2014). Saunders et al (2016) state that, explanatory studies establish causal relationship between variables. Research questions that seek explanatory answers are more likely to begin with or include 'Why' or 'How' while questions that are asked during the data collection phase would most likely start with or include 'Why' or 'How'.

5.6.4 Selected Classification for Research

After carefully considering the main features of the different research types discussed, it has helped the researcher understand how each of the research types are in line with the study being conducted. Conducting a comparative research on cybercrime investigation between two countries (i.e. UK and Nigeria) initially required reviewing literature in order to understand the topic further; thus, the use of exploratory research at the initial stage. The researcher also needed to interview 'experts' in order to understand the problem and the issues being investigated.

Research Type	Was it Used	Where and How	Why
Exploratory	Yes	Literature Review Interview	Understand Issue Identify Themes
Descriptive	No	No	No
Explanatory	Yes	Literature Review	Identify Themes

Table 5.3: Showing Justification for Choosing Research Types

5.7 Research Methodology

Collis and Hussey (2014) argue that there are a number of methodologies and methods used for collecting and analyzing primary and secondary data and you need to adopt a detailed approach to ensure that the research design correlates with the philosophical assumptions of your paradigm. Creswell (2014) suggests that knowledge claims, methods and strategies used in a study by a researcher determines the tendency of the research approach. He suggests the following:

a. The issue of problem to be addressed needs to be considered thoroughly and the research needs to be designed that best suits the problem.
b. The researcher needs to consider his or her skills and experience and identify which approach best complements these.
c. The researcher needs to consider the audience to whom the findings from the research will be addressed.

The table below as summarized by Collis and Hussey (2014) lists some methodologies used in social science and some of which are compatible for use under either paradigm. Table 5.4 showing methodologies associated with the main paradigm

Positivism ← → **Interpretivism**	
Experimental studies	Hermeneutics
Surveys (using primary and secondary data)	Ethnography
Cross-sectional studies	Participative inquiry
Longitudinal studies	Action research
	Case studies
	Grounded theory
	Feminist, gender and ethnicity studies

Table 5.4: Methodologies associated with the main paradigm (Adapted from Collis and Hussey 2014)

The researcher considered different methodologies before narrowing down and selecting the most suitable method for the research study. The methodologies considered were experimental, surveys, archival and case studies etc. The following is a brief overview of some of the methodologies which were not considered followed by the justification of the selected methodology.

a. Experimental study is a methodology use to investigate the relationships between variables. It allows causal relationships to be identified and the experiment is conducted in a systematic way under laboratory conditions or in a natural setting (Collis and Hussey 2014). Experimental research was not considered because the research does not fit within the positivist paradigm. The research does not also seek to investigate relationships between variables in order to understand the problem.
b. Collis and Hussey (2014) define survey as a methodology designed to collect primary and secondary data from a sample with the aim of generalising the results to a population. Traditionally, surveys are associated with a positivist methodology but can also be used under an interpretivist paradigm. However, surveys were not used because this research is an interpretivist and qualitatively based research.
c. Ethnography is a methodology whereby the researcher uses socially acquired and shared knowledge to understand the observed patterns of human activity (Collis and Hussey 2014). This approach was not used as this research seeks to collect primary data through interviewing stakeholders within the law enforcement community and most of this data was not available online or in literature and there were also some ethical issues involved in terms of participant consent to the research.

Case study is a methodology used to look at one or a small number of organisations, events, or individuals generally over time (Easterby-Smith et al., 2008). This approach was considered for the research. Yin (2009:18) defines a case study as an empirical inquiry that:

a. Investigates a contemporary phenomenon in depth and within its real-life context usually when the boundaries between the phenomenon and context are not clearly evident.
b. Copes with the technical distinctive situation in which there will be many more variables of interest than data points.
c. Relies on multiple sources of evidence, with data needing to converge in a triangulation.
d. Benefits from the prior development of theoretical propositions to guide data collection and analysis.

This research is based on a comparative case study of both the UK and Nigeria in terms of their laws, policies, procedures and best practices in investigating cybercriminals. As argued by Eisenhardt (1989:534), the best data collection technique is to combine data methods such as archive searching, interviews, questionnaires and observations. The evidence may be qualitative, quantitative or both. For this research, it is a qualitative based approach that seeks to use archival records, documentation and interviews to gain an in-depth understanding of cybercrime investigation in both the UK and Nigeria especially amongst members of CAC.

5.8 Research Approach

Saunders et al. (2016) argue that the development of theory provides a crucial reason for identifying the relevant theories to use when writing research questions and objectives. Research project will be designed to test a theory or develop a theory. Researchers that adopt a clear theoretical position that they would wish to test through the collection of data will be driven by a deductive approach. However, researchers that explore a topic and develop a theoretical explanation as the data are collected and analysed will be driven by an inductive approach. Therefore, the researchers will be considering between the two approaches namely deductive and inductive before formally giving justification for the selection of the desired research approach.

5.8.1 Deductive Approach

Deductive research is a study whereby a conceptual and theoretical structure is developed and tested by empirical observation; therefore, particular instances are deduced form a general inference (Collis and Hussey 2014). Blaikie (2010) put forward six sequential steps through which a deductive approach will progress:

1. Put forward a tentative idea, a hypothesis, a premise or set of hypotheses to form a theory.
2. Using literature or by indicating the conditions under which the theory is expected to hold, deduce a testable proposition or number of propositions.
3. Examine the premise and the logic of the argument that produced them, comparing this argument with existing theories to see if it offers an advance in understanding. If it does, then continue.

4. Test the premise by collecting data to measure the concepts and to analyse them.
5. If the results of the analysis are not consistent with the premises, then the theory is false and must either be rejected or modified and the process started again.
6. If the results of the analysis are consistent with the premise then the theory is corroborated.

5.8.2 Inductive Approach

Collis and Hussey (2014) define inductive research as a study in which theory is developed from the observation of empirical reality; thus, general inferences are induced from a particular instance. Gill and Hussey (2010) argue that the logical ordering of induction is the opposite of deduction as it involves moving from the 'plane' of observation of the empirical world to the construction of theories and explanations about what has been observed. The major differences between deductive and inductive approaches are highlighted in Table 5.5:

Deductive Approach	Inductive Approach
Based on scientific principles	Based on gaining understanding of meanings human attach to events
From theory to data	A detailed understanding of the research context
Need to explain causal relationships among variables	Flexible structure to allow changes to research as it progresses
Quantitative data approach	Qualitative data approach
Application of controls to ensure validity of data	Realization that the researcher is part of the research being conducted
Concepts needs to be operationalized	Less emphasis on generalization
Structured methodology	
Researcher independent of research	

Table 5.5: Differences between Deductive and Inductive (Adapted from Saunders et al., 2016)

This study adopted an inductive approach. Based on Table 5.5, this research is conducting an in-depth study in order to understanding the phenomenon of cybercrime from a law enforcement and investigative point of view. Also, the researcher is using a qualitative approach and there is less emphasis on generalization within the research as it is subjective within a social construct.

5.9 Design of Research Question

Collis and Hussey (2014) define a research question as a specific question the study is designed to investigate and attempt to answer. According to Saunders et al. (2016:42), the research question

> 'will influence your choice of literature review, your research design, the access you need to negotiate, your approach to sampling, your choice of data collection and analysis methods, and help to shape the way in which you write your project report'.

Collis and Hussey (2014) proposed a model to use in identifying research questions. At each stage of the model, they argue that the researcher needs to read, reflect and discuss what they are going to do with others. Figure 5.2 illustrates the model identifying research question

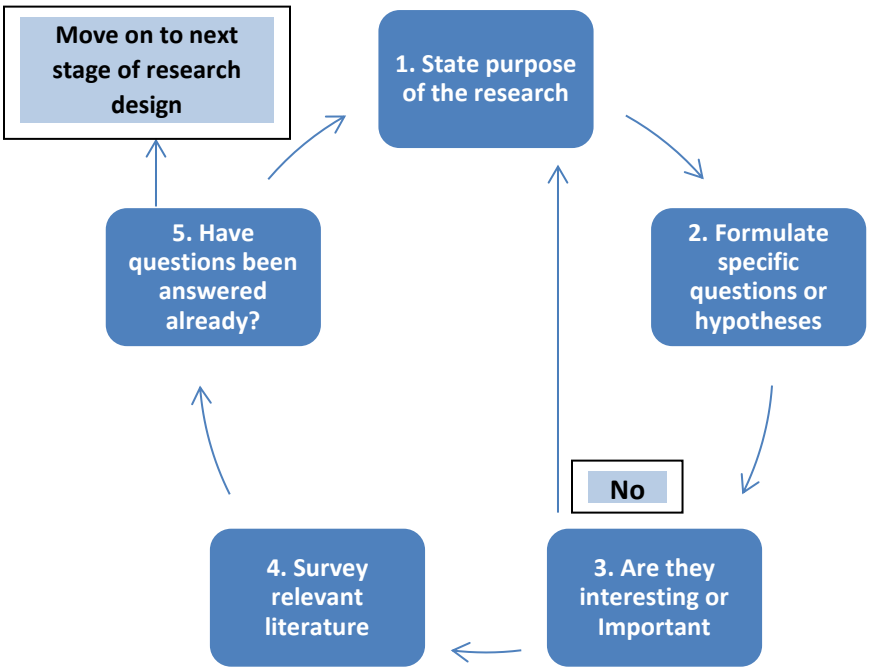


Figure 5.2: Model identifying research questions (Adapted from Collis and Hussey, 2014)

Clough and Nutbrown (2012) argue that in order to clarify a research question, the researcher needs to adopt the 'Russian doll principle'. This means refining a draft research question until it reflects the true meaning of the research idea without including any unnecessary words or

intentions. By stripping away any unnecessary layers (larger outer doll), the clearly defined and refined research question (smaller doll) should reveal to the researcher the appropriate focused starting point for the research. Collis and Hussey (2014) argue that a research question that is more qualitative in nature should have a central question which should be supported by a series of related sub-questions. Creswell (2014) offers some suggestions on designing a research question in an interpretivist study as follows:

a. Avoid using words that suggest a relationship between variables, such as 'effect', 'influence', 'impact' or 'determine'.
b. Use open-ended questions without referring to the literature or theory unless otherwise dictated by the research design.
c. Use a single focus and specify the research site.
d. Do not underestimate the influence of your paradigm on your research.

The research seeks to explore the different approaches in investigating cybercriminals in the UK and Nigeria and especially amongst selected members of the Cybercrime Advisory Council. This approach is necessary it would identify improvements needed in tackling cybercrime globally. The following research questions evolved throughout the research process. They were formulated based on the literature review themes and the aims and objectives of the research. Therefore, in order to identify improvements that are needed to tackle cybercrime globally, the researcher aims to answer the following question:

1. How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?
2. Are Law Enforcement Agencies in Nigeria capable guardians in tackling cybercrime and explored in relation to Routine Activity Theory?
3. To what extent are the current laws adequate in investigating cybercrime in Nigeria?
4. How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?
5. What improvements are needed in the International efforts in tackling cybercrime globally?

The above mentioned research questions were formulated from a detailed review of the literature

and has been tested through Collis and Hussey's model as discussed above. Due to the importance of the continued interaction between the researcher and the subjects of the study some of the questions were modified as the research process evolved.

5.10 Research Choices

Saunders et al. (2016) mentions that the common research choices in a business management study are quantitative or qualitative or the mixed methodology involving the combination of both methods.

5.10.1 Quantitative research

Collis and Hussey (2014) argues that some people prefer to take a quantitative approach to answering their research question thereby designing studies that involve collecting quantitative data and analysing it using statistical methods. In some instances, researchers do not collect new data but use statistics to analyse existing data from a database, archive or other published source. Bryman and Bell (2015:727) define quantitative research as:

> 'Quantitative research usually emphasizes quantification in the collection and analysis of data. As a researcher strategy it is deductivist and objectivist and incorporates a natural science model of the research process (in particular, one influenced by positivism), but quantitative researchers do not always subscribe to all three of these features.'

Quantitative research is generally associated with positivism especially when used with a known and highly rigid data collection technique. Quantitative research is usually associated with deductive approach where the aim is on using data to test theory. However it also incorporates an inductive approach, where data are used to develop theory (Saunders et al. 2016). Some of the characteristics of a quantitative research design is that it may use a single data collection method such as a questionnaire and a suitable quantitative analytical procedure. This approach is known as a *mono method quantitative study,* while a quantitative research design that uses more than one quantitative data collection technique and corresponding analytical procedure is known as a *multi-method quantitative study* (Saunders et al. 2016). Saunders et al. (2016) argue that quantitative research is usually associated with experimental and survey research strategies.

5.10.2 Qualitative research

Denzin and Lincoln (2011) argue that qualitative research is usually associated with an interpretive philosophy. It is interpretive due to the researchers need to understand the subjective and socially constructed meanings expressed about the phenomenon. Qualitative research is sometimes regarded as naturalistic since researchers need to interact with the natural setting or research context in order to establish trust, participation and have an in depth understanding (Saunders et al., 2016). Bryman and Bell (2015:727) define qualitative research as:

> 'Qualitative research usually emphasizes words rather than quantification in the collection and analysis of data. As a research strategy it is inductivist, constructivist, and interpretivist, but qualitative researchers do not always subscribe to all these features.'

Yin (2014) argues that many forms of qualitative research start with an inductive approach to theory development where a naturalistic and emergent research is used to build theory or in order to develop a better theoretical perspective in the existing literature. However, some qualitative research strategies begin with a deductive approach to test an existing theory. Some characteristics of qualitative research is that it studies participants' meanings and the relationship between them using different data collection methods and analytical procedures to develop a conceptual framework and theoretical contribution (Saunders et al. 2016). Bansal and Corley (2011) argue that while qualitative research is known by its methodological variants, it still remains vital irrespective of the method used to demonstrate methodological rigour and theoretical contribution. Saunders et al. (2016) argue that in a qualitative research data collection is non-standardized so that the questions and procedures may change and emerge during a research process that is both naturalistic and interactive. It is also likely to use non-probability sampling techniques. Qualitative research may use a single data collection method such as a semi-structured interview and a corresponding qualitative analytical technique which is known as a mono method qualitative study. Where it uses more than one qualitative data collection technique it is known as a multi-method qualitative study. The strategies used in a qualitative research are action research, case study, ethnography, grounded theory and narrative research.

The differences between quantitative and qualitative research are presented in Table 5.6

Variables	Quantitative Research	Qualitative Research
Research philosophy	Generally positivism. Partly interpretivist	Generally interpretive. Sometimes used within realist and pragmatist philosophies.
Approach to theory development	Usually associated with Deductive approach. It may incorporate inductive	Generally inductive approach Some start with a deductive approach.
Characteristics	Measurement numerically. Analysis using graphs and statistics.	Data collection non-standardized. Likely to use non-probability sampling
Research strategies	Associated with experimental and survey research.	Action research, case study, ethnography, grounded theory and narrative research.

Table 5.6: Comparative Analysis of Qualitative and Quantitative (Adapted from Saunders et al., 2016)

5.10.3 Comparative Analysis of Qualitative and Quantitative

Corbetta (2003) identified four key areas of distinction by which qualitative and quantitative approaches can be compared and contrasted. These four areas are theory-research relationship, physical data collection, data analysis and production of results. However, some authors such as Hardy and Bryman (2004) have pointed out some of the similarities between qualitative and quantitative research as follows:

a. *Both are concerned with data reduction.* Both qualitative and quantitative research collect large amount of information and data. In quantitative research, they reduce the amount of data to make sense of it through a process of statistical analysis. While in qualitative data analysis, researchers develop concepts out of the rich data they have collected.
b. Both are concerned with answering research questions. Even though the kinds of questioned asked in a quantitative and qualitative research are usually different, they are both fundamentally concerned with answering questions about the nature of social reality.
c. Both are concerned with relating data analysis to the literature. Qualitative and quantitative research are all trying to relate their findings to themes, points or ideas thrown up by the literature relating to the research topic.
d. Both are concerned with variation. Both research approaches seek to find out variation

and then to represent the variation they uncover.

e. Both must address the question of error. In a quantitative research, error must be reduced as much as possible so that variation that is revealed is real variation and not the product with a problem on how the questions are asked of how the research instruments are administered. While in qualitative research, the researcher aims to reduce error by ensuring that there is compatibility between his or her concepts and the evidence that has been gathered.

Several Authors (Halfpenny, 1979; Bryman, 1988; Hammersley, 1992) have explored the differences between qualitative and quantitative by emphasising on some of the following issues:

a. Numbers vs Words: Quantitative research are most times associated with applying measurement procedures to social life while qualitative research often use words in the presentation of analyses of the society. However, qualitative researchers are also concerned with the analysis of visual data.
b. Researchers' perspective vs Participant perspective: In quantitative study, the researcher is in control. The number of concerns they bring to an investigation defines the investigation. However, in qualitative research, the perspective of those being studied such as their important and significant views provides the point of orientation.
c. Unstructured vs Structured: Qualitative research is invariably structured in order to allow actors meanings and of concepts emerging out of data collection to be enhanced.
d. Natural settings vs artificial settings: Whereas qualitative researchers investigate people in their natural environment, quantitative researchers conduct their research in a contrived context.
e. Macro vs Micro: Quantitative researchers are often portrayed as involved in discovering large-scale social trends and connection between variables but qualitative researchers are often seen as concerned with small-scale aspects of social reality.

5.10.4 Selected Approach

The selected approach of this research is a qualitative approach using semi structured interviews, documentation and archival records; thus, a multi-method qualitative approach was adopted. This is necessary because conducting research on cybercrime investigation in Nigeria requires

accessing primary data administered through interviewing key stakeholders within the criminal justice system in Nigeria. Most of the data are not readily available through secondary means of data collection. Also, many laws, policies, and documents were reviewed and analysed in order to comprehensively compare the policing approaches between the UK and Nigeria.

5.11 Time Horizon

Saunders et al. (2016) states that an important question to be asked in designing research is, 'Do I want my research to be a 'snapshot' taken at a particular time or do I want it to be more akin to a diary or a series of snapshots and be representation of events over a given period?'. They identified two time horizon called cross-sectional (i.e. snapshot) and longitudinal (i.e. diary). The time dimension of any research is important as different research questions view time in distinctive variations. Blumberg, Cooper, and Schindler (2011) argue that research topics vary based on the research topic or theme. The research could be carried out once and represent an overview at a particular point of time which makes it cross-sectional or it could be a longitudinal study repeated over an extended period of time.

A cross-sectional study is a method used to investigate variables or group of subjects in different contexts over the same period of time (Collis and Hussey, 2014). Saunders et al. (2016) argue that cross-sectional studies often use the survey strategy. They may be seeking to explain how factors are related in different organisations or seeking to describe an incidence of a phenomenon. However, the study may also use qualitative or mixed methods research strategies. Collis and Hussey (2014) point out that a cross-sectional study is usually conducted when there is a limited resource or time constraint. Data are collected once over a short period of time before they are analyzed and reported. Easterby-Smith (2008) further argues that, cross-sectional designs that include questionnaires and survey techniques are either from the relativist or positivist tradition. However, a major limitation to cross-sectional design is how to select a sample that is large enough to be representative of the population. Also, another problem is how to isolate the phenomenon being studied from other factors that could influence correlation. Finally, a cross-sectional study does not explain how correlation exists; only that it does or does not exist (Collis and Hussey, 2014). Although, Lyles and Salk (1996) argued that balanced equity stakes will lead to the highest chance of knowledge transfer. Collis and Hussey (2014) state that cross-sectional studies can be conducted simultaneously and are not expensive,

therefore, there is no problem of change happening due to the passage of time. Collis and Hussey (2014) define longitudinal study as a methodology used to investigate variables or a group of subjects over a long period of time. It is usually associated with a positivist methodology but can be used with an interpretivist paradigm. The main aim of longitudinal study is to examine the dynamics of a research problem by investigating the same variables or group of variables over the period in which the problem occurs. Oates (2006), however, states that a longitudinal study involves researches investigating the case over time usually between one month to several years by analysing those relationships and processes that are continuous and those that change. According to Saunders et al. (2016), longitudinal studies provide a researcher with a measure of control over some of the variables being studied. A longitudinal study under an interpretivist study usually focuses on qualitative data (Collis and Hussey 2014).

Having explored the two main studies under the time horizon of research, this research topic is based on a longitudinal study because of the evolving nature of cybercrime as being dynamic, ever-changing and requiring different counter-measures and strategies to tackle it over different period of time

5.12 Data Collection Methods

Remenyi et al. (2005) states that collection of evidence or data by a researcher depends on the research strategy and tactics being followed as well as the research question. A combination of data collection technique is frequently required in one research in order to support various research strategies. In order for a researcher to answer some of their research questions or achieve their objectives, data needs to be collected so as to be analysed. That process of data collection according to several authors such as (Collis and Hussey, 2014; Bryman and Bell, 2014; Saunders et al., 2016) all agree that two methods are used in collecting data, namely primary data and secondary data. Collis and Hussey (2014) define a method as a technique used for collecting and analyzing data during research. The following section will examine each of these methods and give justification for the selection of the methods.

5.12.1 Primary Data Collection Method

Primary data are data that are generated from an original source such as through experiments,

questionnaire survey, interviews or focus group (Collis and Hussey, 2014). Easterby-Smith (2008) argues that the value of primary data is that it can lead to new insights and a greater confidence in the outcome of the research. However, Remenyi et al. (2005:287) defines primary data as data collected from original sources and not collected from already published sources such as databases or directories. Primary data may be collected either directly or remotely. In a direct data collection approach, the researcher interviews the participant personally and records the response directly, while in a remote data collection approach, the participant interviewed without the interviewer being present. However, there are other intermediate approaches conducted over the phone or through the email (Remenyi et al., 2005).

5.12.2 Secondary Data Collection Method

Secondary data are data collected from an existing source such as databases, internal records publications and may be available in hard copy form or retrieved through the internet (Collis and Hussey, 2014). This resonates with Easterby-Smith (2008) who defines secondary data as 'research information that already exists in the form of publications or other electronic media which is collected by the researcher'. Saunders et al. (2016) summarises the advantages of using secondary data:

a. It requires fewer resources to collect and access. It is less expensive and time consuming to use secondary data than collecting primary data.
b. Secondary data can provide comparative and contextual data.
c. Secondary data provides a source of data that is often permanent and readily available.
d. It allows for the feasibility of a longitudinal study due to time constraints in research.

However, according to Saunders et al. (2016), some of the drawbacks of using secondary data are but not limited to: no proper control over data quality, initial purpose may affect how data are presented, access may be difficult or costly and may be collected for a purpose that does not match the researcher's needs.

5.12.3 Overview of Data Collection Methods

Based on the multi-method qualitative research adapted for this research, the following methods would be discussed for suitability within this study.

5.12.3.1 Documented Data

Saunders et al. (2016) argue that the digitisation of data and creation of archives online has increased the scope of researchers to use other secondary data. Lee (2012:391) defines a document as a 'durable repository for textual, visual and audio representations'. Categories of textural documents include:

a. Communications between individuals or groups such as email, social media and blog posting and letters.
b. Print and Online media sources such as articles
c. Records of individuals such as diaries, electronic calendars and notes.
d. Organisational sources such as contracts, agreements, memos, policy statements, strategy documents and administrative records etc.
e. Government sources such as publications, reports and national statistics.

However, great care and considerations should be taken when using documents for research purposes even though they offer a rich source of data to be analysed. Data provided could be qualitative or quantitative (Saunders et al. 2016). Prior (2007) states that document can be used to show: what is omitted and not just what is contained; which facts are used and why others are not used and how they are used in an organization and how they are distributed and to whom.

5.12.3.2 Case Study

The use of case study is one of the several approaches through which the author is conducting the research on the topic. This research method is used in many situations to contribute knowledge of individual, group, organisational, social, political and related phenomena (Yin, 2009). A case study is a methodology that is usually used to explore a single phenomenon or case in a natural setting using varied methods for obtaining an in-depth knowledge (Collis and Hussey, 2014). The advantages of using case study in research over other research methods is applicable when (a) "how" or "why" questions are being posed, (b) the investigator has little control over events, and (c) the focus is on a contemporary phenomenon within a real-life context (Yin 2009). Although, Collis and Hussey (2014) have categorized case study as a

methodology used by interpretivists, however, it can be used by positivist as summarised by Yin (1994:13) who defines case study as an empirical inquiry that:

a. Investigates a contemporary phenomenon comprehensively within its real-life context especially when the boundaries between phenomenon and context are not clearly evident.
b. Copes with the technically distinctive situation in which there will be multiple variables of interest than data points.
c. Relies on multiple sources of evidence with the need of data to converge in a triangulating fashion.
d. Benefits from the prior development of theoretical propositions to guide data collection and analysis.

Yin (2014) distinguishes between four case study strategies based upon the two discrete dimensions namely; single case versus multiple cases; and holistic cases versus embedded case. Table 5.7 below shows the basic types of case studies based on a 2 × 2 matrix.

	Single-Case design	**Multiple-Case design**
Holistic (Single unit of analysis)	**TYPE 1**	**TYPE 3**
Embedded (Multiple units of analysis)	**TYPE 2**	**TYPE 4**

Table 5.7: Basic Types of Designs for Case Studies (Adapted from Yin, 1994)

Saunders et al. (2016) argue that a single case is often used to represent a critical case or a unique case while rationale for using a multiple case focuses on the basis that similar results can be replicated across cases. Yin's (1994) second discrete dimension is the holistic versus embedded case which refers to unit of analysis. This occurs when within a single case, attention is also given to a subunit or subunits. However, Ryan, Scapens and Theobald (2002) identify four other types of case study as:

a. Descriptive case study, where the object is restricted to describing current practices.
b. Illustrative case study, where the research tries to illustrate new and possibly innovative practices adopted by particular companies.
c. Experimental case studies, where the researcher examines the difficulties in implementing new procedures in an organization and then evaluating the advantages.
d. Explanatory case study, where existing theory is used to understand and explain what is happening.

There are different stages in a case study as enumerated by Collis and Hussey (2014); firstly is the selection of the case, secondly is conducting preliminary investigation; thirdly is the analysis of data and finally is writing of the report. According to Yin (1994), data collection for case studies can rely on various sources of evidence. Six sources of data further explained are documentation, archival records, interviews, direct observation, participant-observation, and physical artifacts. However there are other sources such as films, photographs and videotapes etc. Table 5.8 gives an overview of the six major sources while comparing their strengths and weaknesses.

Source of Evidence	Strengths	Weaknesses
Documentation	• Stable and can be reviewed repeatedly. • Unobtrusive • Contains exact names, details and reference of an event • Has a broad coverage	• Access may be deliberately blocked • Reporting bias • Retrievability can be low • Biased selectivity if collection is incomplete.
Archival Records	• Precise and quantitative • Stable and can be reviewed repeatedly. • Unobtrusive • Contains exact names, details and reference of an event • Has a broad coverage	• Accessibility due to privacy reasons • Access may be deliberately blocked • Reporting bias • Retrievability can be low • Biased selectivity if collection is incomplete.
Interviews	• Targeted: focuses directly on a case study topic • Insightful: provides perceived causal inferences	• Bias due to poorly constructed questions • Response bias • Inaccuracies due to recall • Reflexivity: Interviewee gives what interviewer wants to hear.
Direct Observation	• Covers events in real time • Covers context of events	• Time-consuming • Selectivity unless broad coverage • Cost hours needed by human observers
Participant-Observation	• Insightful into interpersonal behavior and motives • Covers events in real time • Covers context of events	• Bias due to investigator's manipulation of events. • Time-consuming • Selectivity unless broad coverage • Cost hours needed by human observers
Physical Artifacts	• Insightful into cultural features • Insightful into technical operations	• Selectivity • Availability

Table 5.8: Six Sources of Evidence: Strengths and Weaknesses (Adapted from Yin, 1994)

5.12.3.3 Interviews

Interviews are methods of collecting primary data in which a sample of participants are asked questions to find out what they think, feel or do (Collis and Hussey, 2014). Arksey and Knight (1990) argue that interviews conducted based on an interpretivist paradigm are concerned with exploring 'data on understanding, opinions, what people remember doing, attitudes, feelings and the like, that people have in common'. However, Saunders et al. (2016) describe research interviews as a purposeful conversation or dialogue between two or more people whereby it requires the interviewer to establish rapport and ask specific and clear questions to which the respondent or interviewee is able and willing to answer and listen attentively.

Different authors and researchers namely (Saunders et al., 2016; Collis and Hussey, 2014; Easterby-Smith, 2008) have categorised interviews differently. However, the categorisation based on Saunders et al. (2016) states that interviews can be grouped as: structured interviews, semi-structured interviews, and unstructured or in-depth interviews. Collis and Hussey (2014) argue that in an unstructured interview, none of the questions are prepared in advance but evolve during the progression of the interview. The researcher uses open-ended questions which cannot be answered with a 'yes' or 'no' answer.

Unstructured interviews are informal and are usually used to explore in depth a broad area about which the researcher has an interest. The interviewee is given the opportunity to discuss freely about behaviors, events and beliefs in relation to the research subject area. This kind of interaction is sometimes called non-directive and has been labelled as an informant interview because the interviewee's perception guides the conduct and progress of the interview (Saunders et al. 2016).

According to Saunders et al. (2016), structured interviews use questionnaires that are based on standardised or identical set of questions and are usually referred to as interviewer-completed questionnaires. Structured interviews are also known as quantitative research interviews because they are used to collect quantifiable data. Easterby-Smith et al. (2008:145) suggests that semi-structures and unstructured interviews are appropriate methods when:

a. It is necessary to understand the constructs that the respondent uses as a basis for their

opinions and beliefs about a particular matter.

b. The purpose of the interview is to develop an understanding of the respondents 'world' so that the researcher might influence it.
c. The step by step logic is not clear
d. The subject matter is highly confidential or commercially sensitive
e. There are issues about which the interviewee may be reluctant to answer other than confidentially in a face to face situation

Saunders et al. (2016) argue that there are many instances for collecting data using semi-structured or in-depth research interviews. These situations can be grouped into four categories as follows: the purpose of the research; the importance of establishing personal contact, the nature of the data collection questions; the length of time required and completeness of the process. Interviews can be conducted with individual or groups using a variety of methods. Each method has different strengths and weaknesses as cost, size, location and accessibility of the sample are important factors (Collis and Hussey, 2014). Walsh (2001) highlighted some of the strength and weakness of each of the methods as shown in 5.9:

SURVEY APPROACH	STRENGTH	WEAKNESSES
POSTAL QUESTIONNAIRE / ONLINE	- Saves on interviewing time - Can reach a large number of people - Respondents can think about their answers	- Response rates are often low - You don't know who actually fills in the questionnaire - Can be expensive
FACE-TO-FACE INTERVIEW	- Response rate is high - The interviewer can clarify questions - The interviewer can probe replies to get full answers	- Time-consuming - The interviewer may be biased and influence the respondents' answers
TELEPHONE INTERVIEW	- Convenient and quick - The interviewer can clarify questions and probe answers	- Can be expensive - You don't know who is answering - People may not tell the truth, and you can't see their non-verbal behavior to assess this.

Table 5.9: Strength and Weakness of different Methods of Interviews (Adopted from Walsh, 2001)

5.12.4 Selected Data Collection Methods for Research

Walsh (2001) classified source or data as either primary or secondary. Primary data is vital when a research question cannot find an answer from a secondary data which is a pre-existing source of data and information. The researcher will be using both sources of data for the study.

In regards to the research topic, the use of interviews and documented data (qualitative) were chosen as a primary source of data for this research topic due to the following reasons:

1. The nature of the study (i.e. cybercrime) requires the researcher to collect original data from the relevant stakeholders in Nigeria and the UK. Stakeholders such as Law Enforcement Agencies (LEA), the Ministry of Justice, Members of Parliaments, Internet Service Providers, Federal High Court Judges and members of Nigerian Bar Association.
2. Interviewing selected mid-level or management staff of the relevant stakeholders greatly offers an insight into the mode of operations of the organization in regards to investigating cybercriminals.

5.12.4.1 Secondary Data

Secondary data represents studies made by others for their own purpose (Blumberg et al., 2011). Source of data here includes books, semi-scholarly professional publications, peer-reviewed journals, newspapers, internet and documented data. This approach was used in this study because secondary data was expected to provide the researcher with the opportunity to carefully analyse existing literature on the research topic in order to gain a better understanding of the phenomenon of cybercrime. It also offered the researcher the opportunity to know and understand the latest trends, existing policies and practices in the field of cybercrime and policing the internet.

5.12.4.2 Interviews

In relation to the advantages and limitations of the interview method, it was chosen as a primary source of data for this research topic for the following reasons:

1. The nature of the study requires collection of original data from the key stakeholders such as the EFCC; data which are sensitive and some even classified.

2. Interviewing selected mid-level or management staff on the activities of their various units or departments within the EFCC and other stakeholders offers an in-depth understanding into the mode of operations of the organisation, its policies and strategies in investigating cybercriminals in Nigeria. Most of these data and information are not readily available either in publications or the internet.

For the purpose of this research, stakeholders have been grouped accordingly:

a. **Law Enforcement Agencies (LEA):** LEAs form an integral part of this research as they would be able to give an in depth insight about the latest trends in the cyber space. As important stakeholders, the reason for interviewing LEAs is to discover what are the measures put in place to curtail activities of cybercriminals; effectiveness of the measures and policies and practices that needs to be put in place to globally combat cybercrime. The researcher interviewed investigators, prosecutors and analysts from two law enforcement agencies namely the Economic and Financial Crimes Commission (EFCC) in Nigeria and the West Yorkshire Police in the UK. The researcher also interviewed members of the Cybercrime Advisory Council (CAC) in Nigeria.
b. **Regulators:** This group of stakeholders is bodies, agencies and NGOs responsible for either regulating a government agency, telecommunications sector and also the civil society organizations. The researcher planned to interview the telecommunications regulator in charge of regulating the mobile network operators (MNO), internet service providers (ISPs) and cybersecurity and forensic professional bodies. The rationale for interviewing this group was that most of the crimes perpetrated on the internet were the ISPs and MNO, thus, it was necessary to know what policies and measures were put in place to drastically prevent, detect or even stop cybercrime from taking place. Also professional bodies play a vital role in building capacity for law enforcement and other bodies.
c. **Policy Makers:** Policymakers play a vital role in creating the policy framework and direction for the LEAs and regulators to operate or carry out their statutory mandate as it entails cybercrime investigation. Stakeholders interviewed included Members of Parliament, and Cybersecurity Officers of the Office of the National Security Advisor (ONSA). The rationale for interviewing policy makers was to identify the laws and policy

regarding cybercrime and cybersecurity and find out how effective these policies have been in curtailing the activities of cybercriminals in Nigeria. Also, the researcher wanted to find out what partnership, collaboration and Mutual Legal Agreement Treaty (MLAT) these stakeholders have with local and international partners in the global fight against activities of cybercriminals.

5.12.4.3 Documented Data

The following documented data were used in this research:

a. **Government Reports:** These sets of documents are data compiled by various government agencies and parastatals that play a vital role in investigating cybercrime in Nigeria and the UK. Some of the documents to be analyzed included the National Cybersecurity Policy and Strategy of both countries. Also, the researcher used annual reports of key LEAs in the UK and Nigeria in order to get an accurate picture of the cybercrime scene as it related to trends in cybercrime and partnership agreement with other stakeholders.

b. Laws and Acts of Parliament: Government Laws, Acts and Policies are vital documents that give any country the institutional, legal and administrative mandate to carry out its statutory functions within any government establishments. The documents to be considered included laws that prohibit cybercrimes; laws that regulates ISPs and other Acts of parliament that provides the legal framework for cybercriminals to be investigated and prosecuted.

c. **Administrative Records:** Administrative records such as minutes and standard operating procedures are vital data that would give the researcher an in depth understanding on what LEAs, Regulators and Policy makers are doing to administratively tackle the issue of cybercrime in Nigeria.

5.12.4.4 Case Study

The use of case study is one of the several approaches through which the researcher conducted the research on the topic. Yin (2009:4) argues that, case study is used in many situations to contribute knowledge of individual, group, organisational, social, political and related phenomena.

Case study analysis was used in this research because it was expected to permit a critical examination of the activities of the Economic and Financial Crimes Commission (EFCC) as an organization. The advantages of using case study in this instance over other research methods is applicable when (a) "how" or "why" questions are being posed, (b) the investigator has little control over events, and (c) the focus is on a contemporary phenomenon within a real-life context (Yin 2009).

Collecting case study evidence involves getting data and information from six different sources namely: documentation, archival records, interviews, direct observation, participant-observation and physical artifacts. For the purpose of this research, the author utilised documentation and interviews because most of the documented data were easily accessible from the organizations website (i.e. http://www.efccnigeria.org) or were accessible to the researcher and interviews conducted on mid-level and management staff would suffice in making a case study analysis of the organization.

However, case study was not the only research method used, due to some constraints such as access to some organisations' data; it was used alongside other research methods to complement the research process.

Table 5.10 shows the different research methods and how they distinguish from each other.

METHOD	Form of Research Question	Requires Control of Behavioral Events?	Focuses on Contemporary Events?
Experiment	How, Why	Yes	Yes
Survey	Who, What, Where, How many, How much	No	Yes
Archival Analysis	Who, What, Where, How many, How much	No	Yes/No
History	How, Why	No	No
Case Study	How, Why	No	Yes

Table 5.10: Relevant Situation for Research Strategies (Adopted from Yin, 1994)

5.12.4.5 Sampling Theory and Selection

Easterby-Smith (2012:332) defines a sample as 'a subset of the population from which inferences are drawn based on evidence'. Also, the general purpose of collecting data from a sample is to enable the researcher to make statements about the population from which the sample is drawn from.

According to Easterby-Smith et al. (2012), the two basic principles of sampling decisions are representativeness and precision. The accuracy of the conclusions that are drawn from a sample depends on whether it has the same characteristics as the population from which it is originally drawn. While precision is all about how credible the sample is. The combination of both precision and representativeness is to achieve a credible sample

Saunders et al. (2016) distinguishes two different sampling techniques namely: probability or representative sampling; and non-probability sampling. Probability samples the chances or probability of each case that is selected from the target population is known and is equal for all cases. It is usually associated with survey and experiment research strategies. However, non-probability sampling methods, according to Easterby-Smith (2012), shares the same characteristics, thus, it is possible to share the probability of any member of the population being sampled. Therefore, they can never give the researcher the same level of confidence as probability-based sampling does especially when drawing inferences about the population of interest from a specific sample.

Table 5.11 shows the various sampling designs as highlighted by Patton (1990:182).

S/N	TYPE	PURPOSE
A	**Random probability sampling**	Representativeness: Sample size a function of population size and desired confidence level.
1	**Sample random sample**	Permits generalization from sample to the population it represents.
2	**Stratified random and cluster samples**	Increases confidence in making generalizations to particular subgroups or areas.
B	**Purposeful Sampling**	Selects information-rich cases for in-depth study. Size and specific cases depend on study purpose.
1	**Extreme or deviant case sampling**	Learning from highly unusual manifestations of the phenomenon of interest.
2	**Intensity sampling**	Information-rich cases that manifest the phenomenon intensely but not extremely.
3	**Maximum variation sampling**	Documents unique or diverse variations that have emerged in adapting to different conditions. Identifies important common patterns that cut across variations.
4	**Homogeneous sampling**	Focuses, reduces variation, simplifies analysis, facilitates group interviewing.
5	**Typical case sampling**	Illustrates or highlights what is typical, normal, average.
6	**Stratified purposeful sampling**	Illustrates characteristics of particular subgroups of interest; facilitates comparisons.
7	**Critical case sampling**	Permits logical generalization and maximum application of information to other cases.
8	**Snowball or chain sampling**	Identifies cases of interest from people who know people who know people who know which cases is information rich.
9	**Criterion sampling**	Picking all cases that meet some criterion
10	**Theory-base or Operational construct sampling**	Finding manifestations of a theoretical construct of interest so as to elaborate and examine the construct.
11	**Confirming and disconfirming cases**	Elaborating and deepening initial analysis, seeking exceptions, testing variation.
12	**Opportunistic sampling**	Following new leads during fieldwork, taking advantage of the unexpected.
13	**Random purposeful sampling**	Adds credibility to sample when potential purposeful sample is larger than one can handle.
14	**Sampling politically important cases**	Attracts attention to the study (or avoids attracting undesired attention by purposefully eliminating from the sample politically sensitive cases).
15	**Convenience Sampling**	Saves time, money, and effort. Poorest rationale; lowest credibility. Yields information-poor cases.
16	**Combination or mixed purposeful sampling**	Triangulation, flexibility, meets multiple interests and needs.

Table 5.11: Sampling Strategies (Adopted from Patton, 1990)

Miles, Huberman and Saldana (2014) state that another way of classifying sampling approaches is that qualitative researchers usually work with small samples of people that are part of their context unlike quantitative researchers who aim for bigger number of context-stripped cases and seek statistical significance. Patton (1990) also agrees and further states that the adopted sample design is directly connected to the research philosophy and the research methods in the study.

5.12.4.5.1 Qualitative Sampling Techniques

Patton (1990) argues that sampling strategies suitable to a qualitative research has two advantages namely, it provides a detailed description of the phenomenon being researched and secondly, it assists in identifying patterns across different sources of data. With emphasis on Patton's (1990) summarised table (Table 5.11) showing various sampling techniques, each of the sampling strategies have a suitability of either being positive or negative for this research study. For example, random probability sampling and simple random sample is not suitable for this research because these are strategies used mainly in a quantitative research while this research is strictly qualitative. Also, the extreme case sampling was not a suitable option because it can produce skewed results and may not be representative. 'Snowballing sampling' was not considered as well because it did not fit in to the research design adopted for this study. 'Opportunistic sampling' was considered unsuitable because this study is not 'following new leads during fieldwork, taking advantage of the unexpected, flexibility' (Patton, 1990:183). 'Confirming and disconfirming cases' was ruled out as this research is not 'deepening initial analysis, seeking exceptions, testing variations' (Patton, 1990,183).

Having considered the various and diverse qualitative sampling strategies highlighted in Patton's (1990) table (Table 5.11) showing different strategies, the researcher has chosen the 'criterion sampling' as most suited to the interview methodology for this research. Patton (1990:176) argues that 'the point of criterion sampling is to be sure to understand cases that are likely to be information-rich because they may reveal major system weaknesses that become targets of opportunity for program or system improvement'. Nonetheless, certain drawbacks of this strategy, are that this process will give the entire population of the research interest an equal opportunity of being considered and selected for this study. The criterion used to select cases included:

- **a.** Participants were staff and members of the Cybercrime Advisory Council as stipulated in the Cyber Crimes (Prohibition and Prevention) Act, 2015.
- **b.** Participants were involved in investigating economic and financial crimes.
- **c.** Participants are stakeholders in the prevention, detection, investigation and prosecution of cybercrime and computer related offences.

d. Participating stakeholders were willing to give both individual and management consent.

e. Participants are active stakeholders in the global fight to tackle cybercrime.

Out of possible ten organisations identified, only seven were equal to the 'criterion' to be part of the research.

5.12.4.6 Data Analysis

Saunders et al. (2016:714) defines data as 'facts, opinion and statistics that have been collected together and recorded for reference or for analysis'. Collis and Hussey (2014) argue that a researcher's method for analysing data depends on their paradigmatic stance and whether the data is quantitative or qualitative.

Robson (2011:466) state that there are a number of challenges presented to both positivists and interpretivists when analysing data. One of the challenges is that there is 'no clear and universally accepted set of conventions for analysis corresponding to those observed with quantitative data'. Another challenge, according to Collis and Hussey (2014) is that, the data collection method can also include the basis of the analysis making it difficult to distinguish methods by purpose.

Morse (1994) argues that all the different approaches to analyzing qualitative data are based on four elements namely:

a. **Comprehending:** Is the process of acquiring a detailed and full understanding of the setting, culture and study before the research begins. He argues that the researcher does not need to be familiar with the literature at the beginning of the research but should remain distant from it in order for new discoveries to be made without being contaminated by preconceptions.
b. **Synthesising:** Is the process of bringing together different themes and concepts from the research and making them into a new and integrated pattern.
c. **Theorising:** Morse (1994:32) states that this is a 'constant development and manipulation of malleable theoretical schemes until the best theoretical scheme is developed'.

d. **Re-contestualizing:** Re-contextualizing the data through the process of generalization in order that the theory emerging from the research can be applied to other settings and population.

Qualitative data analysis (QDA) software like NVivo is widely available and beneficial to a researcher analyzing large amount of qualitative data (Collis and Hussey, 2014). Dembowski and Hanmer-Lloyd (1995) identified the following ways in which QDA software such as NVivo can assist an interpretivist researcher. These are, importing and storing text; coding the data; searching and retrieving text segments; stimulating interaction with the data; and relationship building within the data. Also, Gilbert (2002) enumerates three stages that researchers experience in the use of QDA software in analyzing qualitative data:

a. The tactile digital divide where the researcher must get used to working with the data on the computer screen rather than the hard copy.
b. The coding trap whereby the researcher finds the software bringing them closer to detail of the data and too much time is wasted in coding without taking into account a more reflective view.
c. The meta-cognitive shift in which the researcher learns to reflect on how and why they should work in a particular way and what impact this has on the analysis

The analysis of data collected through interviews would be documented, transcribed and analyzed by using NVivo software. This would allow the researcher to create multiple themes, group responses, categorize journal articles and map out research strategies that will enable the researcher have a better understanding of the data collected.

5.13. Reliability and Validity

Collis and Hussey (2014:53) refers to validity as 'the extent to which a test measures what the researcher wants it to measure and the results reflect the phenomena under study'. Issues such as faulty procedures, research errors, poor sample or misleading measurements can undermine validity. Reliability, according to Saunders et al. (2016) refers to the replication and consistency of the findings; that is researchers are able to replicate a previous research design and achieve the same findings.

Since this research investigation is based on a qualitative approach, the researcher will be discussing reliability and validity within qualitative research. Afterwards, the selected reliability and validity strategy will be selected for this study.

5.13.1 Pilot Investigation

Prior to collecting primary data through interviews, a pilot investigation was conducted. Collis and Hussey (2003) argue that a pilot study allows the researcher to refine their questions, evaluate their validity, ensure that data collected fits the research questions and assists in developing a refined and better version of the final interview questions. Therefore, the design and results of the pilot study are presented in Chapter Six called 'Pilot Study'.

5.13.2 Interview Validity Strategy

In order to ensure reliability within the interview data, this research adopted a conceptual framework which can be used to help design a strategy in order to formulate a valid interview. For the purpose of this research, Foddy (1993:22) Figure 5.3 model of symbolic interactionist view of question and answer behavior was considered.

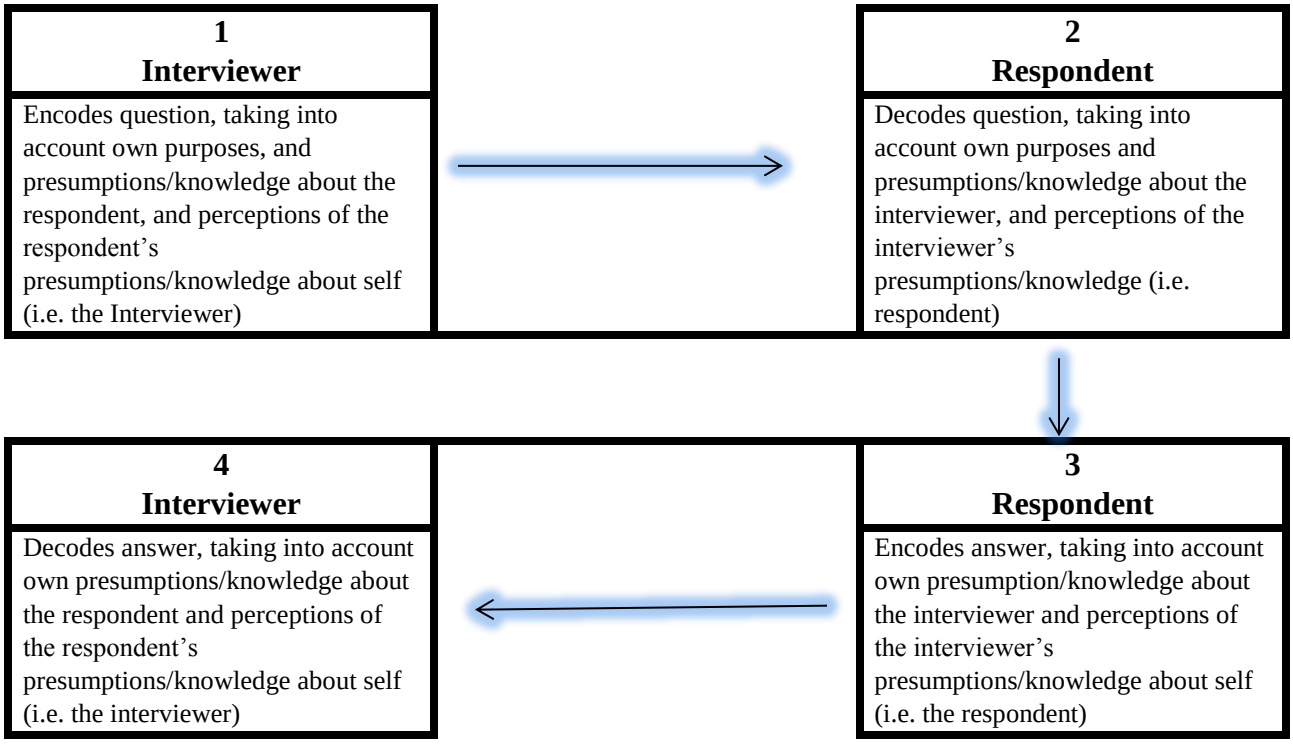


Figure 5.3: Symbolic Interactionist view of Question-Answer Behavior (Foddy, 1993)

The framework shows how messages can be encoded and decoded differently by the interviewer and the respondents. Wengraf (2011) argues that the main philosophy behind the Foddy (1990) model is that it is highly unlikely that the meaning of any utterances as decoded by the respondent will be identical to that encoded by the interviewer. Therefore, researchers have to carefully analyse the interview transcript in order to assess the varied options of meaning when encoding and decoding to ensure reliability.

Foddy (1990:21) discusses the implication of symbolic interaction theory for social research as:

> 'the most basic implication of symbolic interaction theory for social researchers is the hypothesis that the meaning ascribed to social acts is a product of the relationship within which those acts take place. Symbolic interaction theory predicts that respondents will constantly try to reach a mutually shared definition of the situation with the researcher'.

5.13.3 Selected Validation Strategies

Saunders et at. (2016:206) defines validation as 'the process of verifying research data, analysis and interpretation to establish their validity/credibility/authenticity'. The validation techniques considered for the research investigation were triangulation, participant or member validation and peer debriefing.

5.13.3.1 Triangulation

Triangulation is the process that involves the use of more than one source of data and method of collection to confirm the validity/credibility/authenticity of research data, analysis and interpretation (Saunders et al., 2016). Due to this research using multi-method qualitative approach; triangulation was a suitable validation technique. Also, this research is an interpretivist study, thus, triangulation adds 'depth, breadth, complexity and richness' of the research (Saunders et al., 2016). The researcher is using interview data coupled with documented data so as to better understand the phenomenon of cybercrime especially as it relates to Nigeria.

5.13.3.2 Participant or Member Validation

Participant or member validation is a process of taking or sending research data back to participants to allow them to authenticate its accuracy, by permitting them to comment on and

make necessary corrections in order to validate the data (Saunders et al., 2016). This approach was used in order to validate data by allowing key stakeholders who had taken part as participants to give their professional inputs based on facts and data available to them through comments and corrections. Research findings were also presented to key stakeholders in both the UK and Nigeria in conferences.

5.14. Ethical Research Issues

Saunders et al., (2012) argues that ethical considerations would emerge as a researcher plans their research, seeks access to individuals and organizations, collect, analyses and report data. Ethics is thus defined as a set of moral principles or standard of behavior that guides moral choices about "our behaviors and our relationship with others" (Blumberg et al., 2011).

This research aimed to collect data through interviewing law enforcement personnel's, top government officials, lawmakers and policy makers both in the UK and Nigeria. Due to the sensitivity of the subject matter (i.e. cybercrime); the researcher was guided by the code of ethics of University's Research Ethics Committee. The researcher abided with the the following "General Ethical issues" as stipulated below (Saunders et al., 2012):

1. Strict adherences to dictates of established research ethics committees.
2. Seeking the proper consent from the university, organization and individuals before data is collected.
3. Providing privacy to participants
4. Allowing participants to voluntarily participate and the right to withdraw partially or completely from the process.
5. Maintaining confidentiality of data provided by individuals and their anonymity.

Bell and Bryman (2007) compiled and summarised ethical guidelines for researchers conducted by several professional bodies. They are as follows:

a. Harm to participants: The need to avoid potential harm through the research process and the need to properly ensure that the physical as well as the psychological wellbeing of participants, researchers and others.

b. Dignity: The need to respect the dignity or participants, researchers and others in a research and also to avoid causing any form of discomfort.
c. Informed consent: The need to ensure the fully informed consent of research participants.
d. Privacy: The need to protect privacy of research subjects or avoid invasions of privacy.
e. Confidentiality: The requirement to ensure strict confidentiality of research data whether relating to individuals, groups or organizations.
f. Anonymity: The protection of anonymity of individuals or organizations.
g. Deception: The need to avoid deception during the research process either through lies or behavior that is misleading.
h. Affiliation: The need to declare any professional or personal affiliations that may have influenced the research such as conflict of interest and sponsorship.
i. Honesty and Transparency: The need for openness and honesty in communicating information about the research to all interested parties.
j. Reciprocity: The research should be of mutual benefit to researcher and participants or some form of collaboration or active participation should be involved.
k. Misrepresentation: The need to avoid misleading, misunderstanding, misrepresenting or falsely reporting the research findings (Bryman & Bell, 2007 as cited in Collis & Hussey, 2014:31).

5.14.1 Research Ethical Consideration

Robson (2000) has summarized ten main ethical issues and mistakes that a researcher should avoid when conducting a research.

Table 5.12 categorizes the guidelines

S/N	Ten Questionable Practices in Social Research
1	Involving people without their knowledge
2	Coercing them to participate
3	Withholding information about the true nature of research
4	Otherwise deceiving the participants.
5	Inducing participants to commit acts diminishing their self-esteem
6	Violating rights of self-determination (e.g. in studies seeking to promote individual change)
7	Exposing participants to physical to mental stress
8	Invading privacy
9	Withholding benefits from participants.
10	Not treating participants fairly, or with consideration, or with respect.

Table 5.12: Ten Questionable Practices in Social Research (Robson, 2002:69)

During the research investigation process, participant invitation letter and participant consent forms were distributed to selected participants. The right of withdrawal from participation was made explicitly clear to all participants ***(See Appendix C, D, E & F)***. Participants were made aware of their voluntary participation and anonymity, and confidentiality was offered and ensured throughout the research process. Also, before collection of data from the participant's ethical approval was obtained from the University of Salford and also management consent was sought and obtained from the law enforcement agencies involved. Finally, the researcher ensured that Robson's (2002) Ten Questionable Habits (Table 13.13) were avoided.

5.15 Research Integrity

The integrity of the research study is maintained by adhering to the seven principles of interpretive research set forth by Klein & Myers (1999). Klein and Myers (1999) argue that, these principles were derived from anthropology, phenomenology and hermeneutics, however, the principles are not mandatory but they provide the researcher with some discretion in deciding how and when these principles may be applied in a research study.

Table 5.13 summarises the principles

S/N	PRINCIPLES FOR INTERPRETIVE FIELD RESEARCH	SUMMARY
1	**The Fundamental Principle of the Hermeneutic Circle**	The principle suggests that all human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form.
2	**The Principle of Contextualization**	Requires critical reflection of the social and historical background of the research setting in order for the intended audience to see how the current situation under investigation emerged.
3	**The Principle of Interaction Between the Researchers and the Subjects**	This principle requires critical reflection on how the research materials were socially constructed through the interaction between the researchers and participants.
4	**The Principle of Abstraction and Generalization**	This principle requires relating the idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action.
5	**The Principle of Dialogical Reasoning**	Requires sensitivity to possible contradictions between the theoretical preconceptions guiding the research design and actual findings with subsequent cycles of revision
6	**The Principle of Multiple Interpretations**	Requires sensitivity to possible differences in interpretations among the participants as are typically expressed in multiple narratives or stories of the same sequence of events under study.
7	**The Principle of Suspicion**	Requires sensitivity to possible 'biases' and systematic 'distortions' in the narratives collected from the participants.

Table 5.13: Summary of Principles for Interpretive Field Research (Klein and Myers, 1999)

5.16 Research Quality

According to Oates (2013) and Denzin & Lincoln (2000), interpretivist research quality is maintained through a set of standards and criteria that are equivalent to those used in positivist research. Table 5. 14 shows the different qualities in a positivist and interpretivist research

Positivism	Interpretivism (Current Study)
Validity	Trustworthiness
Objectivity	Confirmability
Reliability	Dependability
Internal Validity	Credibility
External Validity	Transferability

Table 5.14: Showing Quality in Positivist and Interpretivist Research (Oates, 2013)

The below mentioned criteria under interpretivist have been applied to the research study as follows: (Denzin&Lincoln, 2000; Miles et al. 2014; Miles & Huberman, 1994; Oates, 2013; Saunders et al. 2016; Shenton, 2004)

S/N	CRITERIA	Application in Current Research
1	**Trustworthiness:** Refers to the amount of trust that can be placed in the research	Research participants were given assurances that all information collected will be confidential and anonymous, therefore, this made participants more relaxed and willing to discuss freely. Also, this will increase the level of confidence and decrease the possibility of participant's bias (Saunders et al., 2016). Direct quotations were used rather than summaries.
2	**Confirmability:** Refers to checking if the findings flow from the data. This can be achieved by an audit trail.	Interview questions were prepared before the interview. Data analysis was based on the data derived from the interviews only. NVivo software was used to ensure a clear view of the data analysis process. Detailed methodological descriptions were used to show how the themes emerged from data collected (Shenton, 2004)
3	**Dependability:** Refers to the recording and documentation of data collection and research process to ensure that the results are consistent across time and researchers.	The research process was documented thoroughly in order to help readers understand the process and repeat it in future work (Shenton, 2004). All the interviews were recorded and transcribed word-by-word. One pilot study was conducted and peer review mechanism was used.
4	**Credibility:** Ensuring that the research subject had been identified and accurately described so as the findings are credible. It can be improved through prolonged engagement of the researcher with the research problem.	The researcher worked in a LEA (i.e. EFCC) which helped the researcher in developing a familiarity with the participants and the place i.e. 'prolonged engagement' (Shenton, 2004). Multiple interviews with different stakeholders were used as a source of triangulation. Research findings were presented in front of key stakeholders in the UK and Nigeria. Participant validation was used in some instances by giving the participants transcript of what they said.
5	**Transferability:** To check if the data can be generalized	Different stakeholders Interviewed; detailed description of research context (Chapter 2). Field Log kept and maintained.

Table 5.15: Research Quality and Application

5.17 Researcher Background

Being interpretivist and subjective in reality, the researcher states their relevant personal background, which will unavoidably impact on the research interpretations. Therefore, in this study the researcher declares his interests and worldviews. The researcher graduated with a Bachelors degree in Information Technology from the American University in Dubai. The researchers' area of concentration was Network Infrastructure Design and Administration. This provided the researcher a scientific and technical background that instilled a more positivist than interpretivist view. Subsequently, the researcher did a Masters degree in Forensic Computing from Coventry University which expanded the researchers' scientific background and provided professional knowledge on the role of forensic science in criminal investigation. The thesis centered on the perception of the public on law enforcement in tackling cybercrime and it was a quantitative survey administered online to participants. The researcher worked for about seven years as an IT and Forensic Analyst with the Economic and Financial Crimes Commission, thereafter left to pursue a PhD degree. Some of the rationale of the study is due to the researcher's previous working experience in a law enforcement organisation. Over the course of the PhD, the researcher was invited as a speaker and stakeholder to present some of the research findings to the West Yorkshire Police and some stakeholders in Nigeria who are members of the Cybercrime Advisory Council respectively. The researcher decided to conduct an interpretivist qualitative research through interviews as that would give more insight and get more accurate empirical data about cybercrime investigation in Nigeria.

5.18 Conclusion

The methodology chapter explored the different research methodologies which were used in this research and elaborated the chosen methodology for the research as well as justifications for choosing them. Table 5.16 and 5.17 summarises and states the researcher methodological choices. The table shows that the researcher is adapting a relativist philosophy with an interpretivist view. The researcher used both exploratory and explanatory approaches in classifying the research. The research is an inductive study and exclusively qualitative with data collection techniques involving both primary and secondary data. Data collected was analysed with software called NVivo and validity of data was authenticated through triangulation of data

and member validation approaches. Finally, the researcher was guided by good academic practices in adhering to ethical issues throughout the research process.

Table 5.16 showing researchers methodological choices.

S/N	Methodological Theoretical Phases	Researchers Choice	
1	Research philosophy	Relativism	
2	Research paradigm	Interpretivism	
3	Research classifications	Exploratory and explanatory	
4	Research approach	Inductive	
5	Research choices	Qualitative	
6	Time horizon	Longitudinal	
7	Data collection	**Secondary**	**Primary**
		Literature review	Interviews
			Documented data
			Case study
8	Data analysis	NVivo	
9	Validity, reliability	Triangulation; Member validation	
10	Ethical issues	Privacy, consent & confidentiality etc.	

Table 5.16: Researchers Methodological Theoretical Choices

Table 5.17 summarises the choices with explanation and reference page.

Table 5:17: Researchers methodological choices

S/N	Phases	Researchers Choice		Justification	Ref. Page
1	**Research Philosophy**	**Relativism**		Due to the fact that different observers would have varied views which are interpreted differently at various times and various places.	***p.94***
2	**Research Paradigm**	**Interpretivism**		Cybercrime has multiple realities; data collected is subjective; study is inductive and is collecting qualitative data.	***p. 103***
3	**Research Classifications**	**Exploratory and Explanatory**		Explorative to gain insights and Explanatory to understand variables of the research topic.	***p. 105***
4	**Research Approach**	**Inductive**		In-depth Study and less emphasis on generalization	***p. 115***
5	**Research Choices**	**Qualitative**		Semi-structured + Secondary Data	***p. 124***
6	**Time Horizon**	**Cross- Sectional**		Cybercrime studied in different contexts (i.e. UK & NG) over the same period of time	***p. 116***
7	**Data Collection**	**Secondary**	**Primary**	Study requires collection of original data from source; primary data not readily available. Interviews used to gain an in-depth understanding of phenomenon. Case study used to validate data collected from secondary sources.	***p. 124 - 131***
		Literature Review	**Interviews**		
			Documented Data		
			Case Study		
8	**Sampling Technique**	**Criterion Sampling**		Compatible with research because it gives the entire population an equal opportunity to be considered based on certain criteria.	***p. 128***
9	**Data Analysis**	**NVivo**		Allows researcher to create themes, group responses, categorized journal articles and map out research strategies effectively	***p. 131***
10	**Validity, Reliability**	**Triangulation, Participant or Member Validation**		Triangulation adds depth, breadth and richness to the data collected.	***p. 134***
11	**Ethical Issues**	**Privacy, Consent & Confidentiality.**		Robson (2002) 10 questionable practices were avoided and Saunders et al. (2012) 'general ethical issues' were adhered to.	***p. 136***

CHAPTER 6: PILOT STUDY

This chapter presents the pilot study which was conducted, the justifications for conducting it and its impact on the current research.

6.1 Introduction

Hundley and Teijlingen (2001) refer to pilot study as a mini version of a full scale study as well as the specific pre-testing of a particular research instrument such as a questionnaire or an interview. Pilot studies are a vital component of a good research design, however, it does not guarantee the success of the main study but can increase the likelihood of its success.

The term pilot study is usually used in two ways in social science research. It can refer to feasibility studies which are 'small scale versions, or trial runs, done in preparation for the major study' (Polit, Beck & Hungler, 2001). However, Baker (1994:182) argues that a pilot study can also be the pre-testing or 'trying-out' of a particular research instrument. Gomm (2009:245) defines a pilot study as a 'feasibility study, which is preliminary research carried out to support the planning of a more substantial study through':

a. Discovering what is of interest in a research setting
b. Choosing between alternative settings
c. Looking for possible difficulties which have to be overcome
d. Carrying out ethical appraisal of the proposed research
e. Conducting risk assessment
f. Testing research instruments and techniques (Gomm, 2009)

Saunders et al. (2016:723) also define a pilot test 'as a small-scale study to test a questionnaire or interview checklist to minimise the possibility of respondents having difficulties in answering the questions. They further argue that a pilot study minimises data recording problems as well as some assessment of the questions' validity and the reliability of the data that will be collected.

Pilot studies have certain limitations such as the possibility of making inaccurate predictions or assumptions on the basis of pilot data; problems arising from contamination; and problems related to funding (Polit. et al, 2001).

6.2 Justification of the Pilot Study

Hundley and Teijlingen (2001) have summarised the reasons for conducting pilot studies as follows:

a) Developing and testing adequacy of research instruments
b) Assessing the feasibility of a full-scale study or survey
c) Design a research protocol
d) Assessing whether the research protocol is realistic and workable
e) Developing a research question and research plan
f) Determining what resources are needed for a planned study
g) Assessing the likely success of proposed recruitment approaches

The preliminary interview questions were tested on five (5) participants within one organization to achieve the following objectives:

a. Testing the clarity of the interview questions
b. The estimated schedule for each interview
c. The conduciveness of the Interview venue
d. The use of the voice recorder to record the interviews
e. The effectiveness of the adopted interview approach (i.e. Face-to-face, semi-structured)

6.3 Observations from the Pilot Study

The following observations were made during the pilot study. The observations helped in identifying areas that needed improvement or questions that needed to be changed, removed or added. The observations are as follows:

a. The pilot study allowed the researcher to refine the research questions and amend them.
b. The pilot allowed the researcher to know how comfortable the respondents were with the interview being recorded. Most respondents were comfortable with the interview being recorded.
c. The researcher was able to know that the face-face semi-structured interview approach was very effective as most respondents were willing to discuss freely with the interviewer. This also allowed the researcher to observe facial expressions and non-verbal cues.

d. The researcher also realised that most participants had questions surrounding the ethics of the research and the researcher was able to explain to them their rights as codified in the 'participant consent forms' distributed before each interview.
e. The researcher observed that the participants were more comfortable with choosing the venue and timing that suited their schedules.
f. The researcher also observed that scheduling and time management was at the liberty of the participants. Therefore, the researcher had to keep on modifying the schedule to fit with the respondent's schedules.
g. The feedback from the pilot study allowed the participant to properly prepare for the main data collection process, which improved the overall quality of the interview question as well as the validity of the research.

6.4 Action Plan and Recommendation

The following steps and recommendations were implemented after the conclusion of the pilot study. The observations from the pilot study modified some of the interview questions. The following actions and recommendations were implemented in the main research interviews:

a. Each participant was accorded the flexibility in choosing the time and venue of the interview.
b. Some of the participants requested for interview questions before the main interview and they were obliged.
c. The pilot enabled the researcher to narrow down the selection of the participants based on their job roles and sector.
d. The pilot enabled the researcher to prepare a detailed and uniform opening statement before each interview.
e. The pilot study enumerated some of the themes and emergent themes of the research.
f. The pilot study validated the research instrument of recording all the interviews and making detailed notes.

6.5 Interview Stakeholders

Table 6.1 showing interview participants interviewed for the pilot.

PILOT INTERVIEW		
SN	**POSITION**	**OFFICE**
1	**Team Lead, Cybercrime Unit**	**EFCC**
2	**Team Lead, Public Interface Unit**	**EFCC**
3	**Team Lead, Cybercrime Prosecution Unit**	**EFCC**
4	**Team Lead, Enlightenment & Re-orientation Unit**	**EFCC**
5	**Team Lead, Cybercrime Unit Lagos**	**EFCC**

Table 6.1: Interview Stakeholders for Pilot Study

6.6 Conclusion

In conclusion, the pilot study enabled the researcher to justify the selection of participants, refining of interview questions, validation of research instruments and an actionable approach in conducting the main interviews of the research. The pilot study was included in the main study as the interview questions were not changed for the main study. Some of the questions were only rephrased and further divided into two or three questions.

CHAPTER 7:DATA ANALYSIS

7.1 Introduction

The data analysis chapter introduces the various research participants and how the research interview questions were design and developed. The chapter also examines the function of the interviewer and how the interview was administered to the participants. An overview of the interview transcription and coding of the data is further elaborated with emphasis on thematic analysis of the data. The chapter further presents the analysis of the findings and the interpretation of the themes. Finally, a summary of the findings and conclusions are discussed and elaborated.

7.2 Research Participant Representation

The Data Collection process started after the researcher obtained ethical approval from the University of Salford (See Appendix G). Patton (2002) argues that the number of interviews required for qualitative research depends on the purpose or the study and the resources and time available. In this research, the data collection process was continued until the data collection reached saturation and no longer revealed any new nodes, as Myers (2013:123) states that, 'no new insights are being discovered in the interviews'. The first interview was conducted on 8th of August, 2016 and the last interview was conducted on 18th December, 2017. The following steps were taken before the data analysis process:

1. All interviews were digitally recorded and transferred to a computer for transcription.
2. All soft copies of recordings were renamed and secured on a laptop.
3. All the interviews were transcribed verbatim using Microsoft Word.
4. All Interviews were transcribed without correction to grammar, deletion of repeated words or completion of incomplete sentences in order to transcribe the exact conversation (Bazeley, 2007).
5. Then the transcript was edited with questions having the Microsoft Heading 3 and responses having the 'Quote' heading.
6. All Interview transcripts were renamed and imported to NVivo Software for coding.
7. All Interviewees were coded as Participant 1 to 34 to protect anonymity and confidentiality.

SN	CODE NAME	SECTOR	DEPARTMENTS/UNIT/SECTION	DATE	TIME
1	Participant 1	LAW ENFORCEMENT	INVESTIGATION	30/08/16	12:00pm
2	Participant 2	LAW ENFORCEMENT	INVESTIGATION	11/08/16	9:00am
3	Participant 3	LAW ENFORCEMENT	INVESTIGATION	19/08/16	9:34am
4	Participant 4	LAW ENFORCEMENT	INVESTIGATION	18/08/16	2:23Pm
5	Participant 5	LAW ENFORCEMENT	INVESTIGATION	16/08/16	4:30pm
6	Participant 6	LAW ENFORCEMENT	INVESTIGATION	19/08/16	10:00am
7	Participant 7	LAW ENFORCEMENT	FORENSICS	11/08/16	11:55am
8	Participant 8	LAW ENFORCEMENT	FORENSICS	16/08/16	2:00pm
9	Participant 9	LAW ENFORCEMENT	FORENSICS	16/08/16	11:55am
10	Participant 10	LAW ENFORCEMENT	FORENSICS	15/08/16	2:00pm
11	Participant 11	LAW ENFORCEMENT	FORENSICS	16/08/16	10:00am
12	Participant 12	LAW ENFORCEMENT	FORENSICS	16/08/16	9:00pm
13	Participant 13	LAW ENFORCEMENT	MEDIA	24/08/16	10:00am
14	Participant 14	LAW ENFORCEMENT	MEDIA	12/08/16	10:07am
15	Participant 15	LAW ENFORCEMENT	MEDIA	11/08/16	10:15am
16	Participant 16	LAW ENFORCEMENT	MEDIA	25/08/16	2:02pm
17	Participant 17	LAW ENFORCEMENT	MEDIA	16/08/16	8:30am
18	Participant 18	LAW ENFORCEMENT	ICT	17/08/16	12:06pm
19	Participant 19	LAW ENFORCEMENT	ICT	11/08/16	2:18pm
20	Participant 20	LAW ENFORCEMENT	ICT	23/08/16	10:54am
21	Participant 21	LAW ENFORCEMENT	ICT	30/08/16	2:34pm
22	Participant 22	LAW ENFORCEMENT	ICT	17/08/16	4:33pm
23	Participant 23	LAW ENFORCEMENT	ICT	18/08/16	9:08am
24	Participant 24	LAW ENFORCEMENT	LEGAL	18/08/16	11:11pm
25	Participant 25	LAW ENFORCEMENT	LEGAL	17/08/16	2:43pm
26	Participant 26	LAW ENFORCEMENT	LEGAL	19/08/16	11:34am
27	Participant 27	LAW ENFORCEMENT	LEGAL	17/08/16	2:10pm
28	Participant 28	LAW ENFORCEMENT	LEGAL	19/08/16	9:23am
29	Participant 29	PRESIDENCY, ONSA	CYBERSECURITY	24/08/16	4:00pm
30	Participant 30	PARLIAMENT	ICT & CYBERCRIME	31/05/17	3:00pm
31	Participant 31	ICT SECTOR	CYBERSECURITY	05/06/17	1:10am
32	Participant 32	TELECOMMUNICATION	CYBERSECURITY	13/06/17	10:55am
33	Participant 33	LAW ENFORCEMENT	INVESTIGATION	16/11/17	12:28am
34	Participant 34	LAW ENFORCEMENT	INVESTIGATION	18/12/17	2:15pm

Table 7.1: Showing Interviewees Relevant Demographics

Table 7.1 shows all 34 interviewees and their relevant demographics. The participants came from five sectors namely Law Enforcement, Telecommunications, ICT, Parliament and the Nigerian Presidency. The law enforcement participants were divided into five key departments and units that are critical in the investigation of cybercrime. The departments and units are: Investigation, Forensics, Media, ICT and Legal. The researcher interviewed heads of departments and units and sectional heads and team leads of each of the five key departments. In total interviewees came from seven different organisations namely the Economic and Financial Crimes Commission (EFCC); National Crime Agency (NCA); West Yorkshire Police (WYP); Nigerian Communications Commission (NCC); Office of the National Security Advisor (ONSA); National Assembly (Senate); and National Information Technology Development Agency (NITDA). 32 participants were interviewed in Nigeria while the remaining 2 were interviewed in the UK. The other two columns of Table 7.1 show the date and time of all the interviews.

The use of NVivo software has been supported and criticised by researchers. Budding and Cools (2008) state that a drawback of computer-assisted qualitative data analysis software (CAQDAS) is the time invested in the learning of the software versus the actual advantaged of using the software. Also, they suggest that it is not worth using the software for small data sets as it can be processed quicker manually. From the researchers experience of using NVivo Software, the user needs to keep a backup at all times as file corruption and crashing of system occurred frequently during this research study.

However, NVivo was used for the following advantages it offers (Bringer, Johnston & Brackenridge, 2004):

1. Ability to organise data to help throughout the analysis process
2. Ability to set a password and have multiple backups to protect data from loss or theft.
3. Provision of quick access for data coding and retrieval
4. Automation allows researcher more time for analysis process
5. Helps with complex ‘Boolean’ (e.g. and, or, not) searches which is highly complicated when using manual tools.
6. It creates links between documents, memos, nodes and modes which increases transparency which can be difficult when using manual methods.

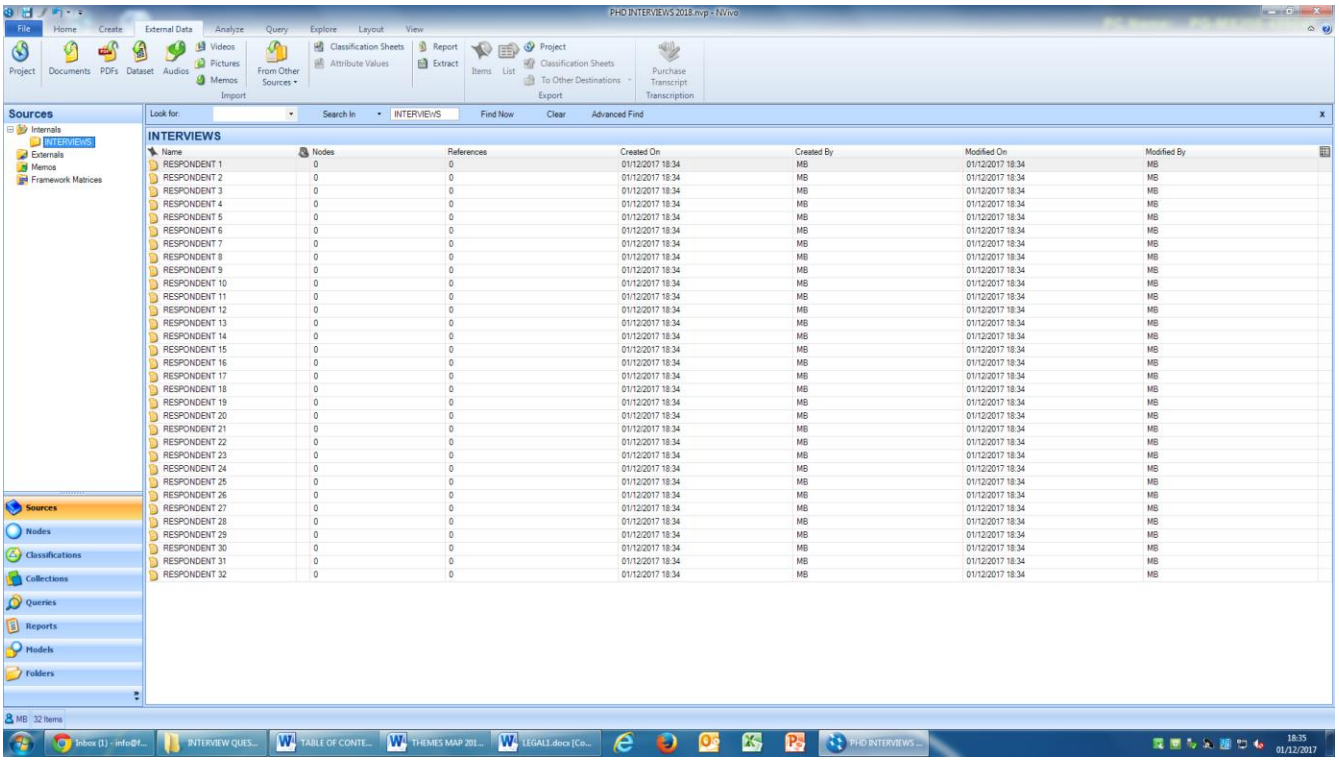


Figure 7.1: NVivo Explorer screenshot showing all the Interviews after transcription

Figure 7.1 Shows all the transcribed interviews imported into NVivo software. The left panel under source and internal shows the interview folder which contains all the interviews labelled Participant 1 to 34. The right panel shows the list of all the interviews and when they were created.

Figure 7.2 shows all the nodes and sub-nodes. The nodes are the themes that were informed by the research questions, literature review and theoretical framework while most of the sub-nodes are answers given by interviewees in answering an interview question.

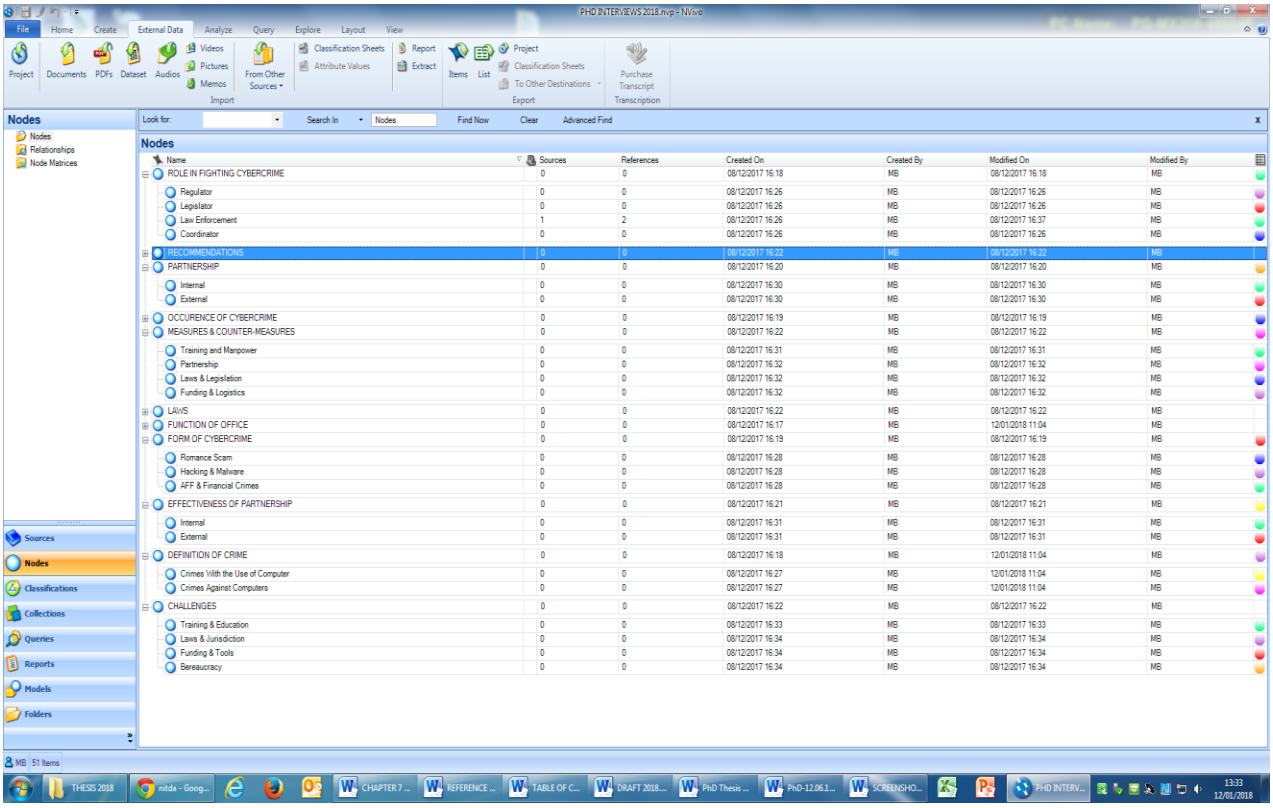


Figure 7.2: NVivo explorer screenshots showing all the nodes and sub-nodes

Figure 7.3 shows the coding process done on a particular interview. A portion of the transcript was used to code it to a particular node and sub-node respectively.

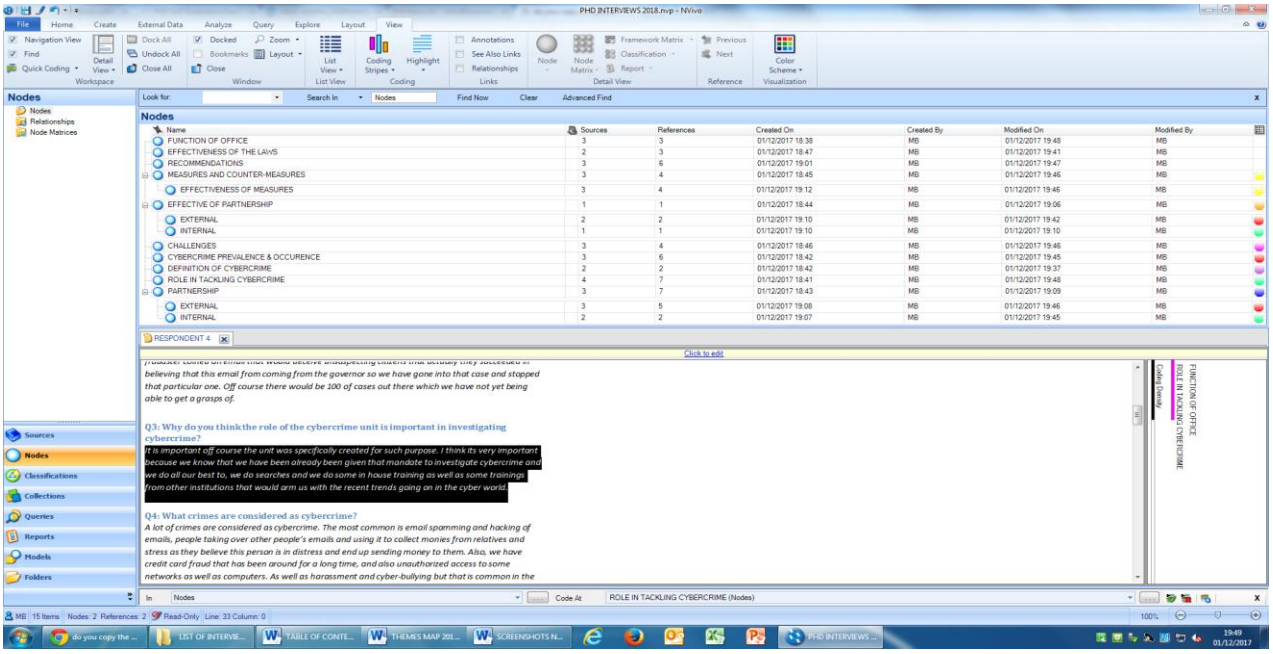


Figure 7.3: NVivo explorer illustrating the coding of an interviewee response

Figure 7.4 Shows the word cloud generated from all 34 interviews

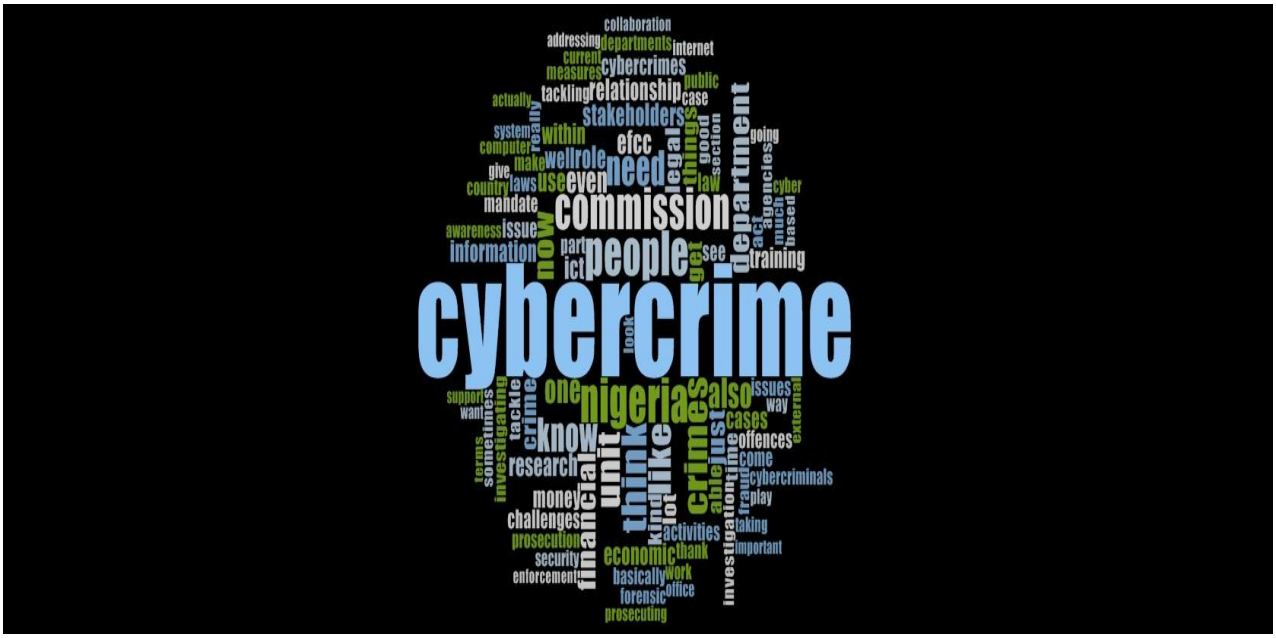


Figure 7.4: NVivo screenshot of word cloud generated from interviewees response

7.3 Design and Development of Interview Questions

The interview questions asked were designed and developed based on the following principles and issues:

1. Questions were created with consideration of the overall aim and objectives (Chapter 1 - Introduction) and the research questions of the study (Chapter 5: Methodology).
2. The researcher ensured the interview questions were fully related to the eleven themes depicted as a result of the literature review.
3. Questions were designed with consideration of the theoretical framework of Routine Activity Theory (RAT)
4. Background and specific questions were used so as participants could explain the phenomenon in their organisational context.

Table 7.2 shows the correlation between the research objectives, research questions, themes, interview questions and theoretical framework

TITLE	INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY				
AIM	To identify any improvements required in international efforts to tackle cybercrime within the scope of LEAs in the UK and Nigeria				
S/N	RESEARCH OBJECTIVES	RESEARCH QUESTIONS	LITERATURE THEMES	INTERVIEW QUESTIONS	THEORETICAL FRAMEWORKS
1	To examine the different roles played by members of the Cybercrime Advisory Council (CAC) in tackling cybercrime in Nigeria through review of relevant literature and interviews.		**T1: FUNCTION OF OFFICE** **T2: ROLE IN FIGHTING CYBERCRIME**	QUESTION 1, 2, 3	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
2	To examine the different definitions and categorizations of cybercrime through review of relevant literature.	**RQ4:** How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?	**T3: DEFINITION OF CYBERCRIME**	QUESTION 4	
3	To explore the different forms of cybercrime that is prevalent in Nigeria through review of relevant literature and interviews.		**T4: FORMS OF CYBERCRIME**	QUESTION 5	**RAT:** SUITABLE TARGET
4	To understand the different reasons cybercrime is committed in Nigeria through review of relevant literature and interviews.	**RQ1:** How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?	**T5: CAUSES OF CYBERCRIME**	QUESTION 6	**RAT:** MOTIVATED OFFENDER
5	To explore the benefits of partnerships in investigating cybercrime in Nigeria through review of relevant literature and interviews.		**T6: PARTNERSHIP** **T7: BENEFITS OF PARTNERSHIP**	QUESTION 7, 8, 9, 10	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
6	To examine the current measures used by LEAs in Nigeria and the UK in tackling cybercrime through review of relevant literature and interview of members of CAC.	**RQ2:** Are LEA in Nigeria capable guardians in tackling cybercrime and explored in relation to RAT?	**T8: MEASURES & COUNTER - MEASURES**	QUESTION 11 & 12	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
7	To explore the current laws used in investigating cybercriminals in Nigeria through review of relevant laws and policies.	**RQ3:** To what extent are the current laws adequate in investigating cybercrime in Nigeria?	**T9: LAWS**	QUESTION 13	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
8	To explore the challenges and limitations in investigating cybercrime in Nigeria through review of relevant literature and interview of members of the CAC.	**RQ2:** Are LEA in Nigeria capable guardians in tackling cybercrime and explored in relation to RAT?	**T10: CHALLENGES**	QUESTION 14	**RAT:** ABSENCE OF A CAPABLE GUARDIAN
9	To examine the recommendations and improvement required to tackle cybercrime in Nigeria and the UK through review of relevant literature and interview of members of the CAC	**RQ5** What improvements are needed in the International efforts in tackling cybercrime globally?	**T11: RECOMMENDATIONS**	QUESTION 15 & 16	

Table 7.2: Correlation between the Research Objectives, Research Questions, Themes, Interview Question and Theoretical Framework

7.4 Function of Interviewer and Interview Administration

McCracken (1998) argues that interviewers play a pivotal role in the collection of data and must decide to what extent they will actively participate. Therefore, the researcher must decide whether to take a 'backseat' role and allow the interviewee to speak openly or naturally or to be actively involved and help construct the way in which the data is obtained from the interviewee. The decisions the interviewer makes during the interview itself is crucial as Wengraf (2011) argues that these decisions may produce different effects to the results and that the skill of interviewing is one that requires careful review and practice.

During this research study, the interview data was collected in two phases and two geographical locations namely the UK and Nigeria. The first phase involved collecting data over a five-week period from one organisation where twenty-eight participants were interviewed. Also, another participant from another organisation was also interviewed. The second phase involved interviewing five participants from five organisations in both the UK and Nigeria. The researcher digitally recorded the data in order to prepare transcripts which were later analysed. All the interviews were recorded with the interviewee's permission with each participant completing a consent form. Table 7.3 shows the breakdown of all the variables in the interview administration.

S/N	VARIABLES	DESCRIPTION
1	**Location of Interviews**	Nigeria and United Kingdom
2	**Number of Participants**	34 Interviewees (32 Nigeria & 2 UK)
3	**Method of Interview**	Face-to-Face (32); Phone Interview (2)
4	**Storage of Data**	Digitally Recorded and Stored
4	**Duration of Interviews**	Average of 25-30 Minutes
5	**Documents Presented**	Participant Information Sheet Participant Invitation Letter Recruitment Material Consent Form
6	**Dates and Months**	July – August 2016; May – Dec 2017

Table 7.3: Interview Administration Variables and Description

7.5 Interview Transcription and Thematic Analysis

Sekaran and Bougie (2013) argue that transcription of interviews has many advantages such as allowing the researcher to examine thoroughly what people have said after the event as well as correcting the natural limitations of human memory. Even though, an audio recording best captures all the information stated verbally, the data processed into a transcript is much easier, accessible and better suited for analysis.

Thematic data analysis is defined according to Braun and Clarke (2006:76) as a method of analysing and reporting patterns and themes within qualitative data. Thematic analysis is used mainly in grounded theory or interpretive studies and is a suitable method of inquiry through the use of coding. Bryman and Bell (2007:725) define coding as 'the process whereby data is broken down into component parts, which are given names'. Coding is one of the most important steps taken during data analysis to help make sense of textual data (Basit, 2003). Braun and Clarke (2006) argue that the quality of coding depends on the quality of the transcription and that it is the 'bedrock' of the analysis process. However, Boyatzis (1998) argues that thematic analysis is much more complicated than organising and reporting patterns, meaning that it can help interpret various aspects of the research topic. A theme is defined as something important about the data in relation to the research questions and which represents a patterned response or meaning within the data (Braun and Clarke, 2006). Tuckett (2005) argues that the primary steps of thematic analysis starts before data collection at the literature review stage as this can enhance the resulting analysis by sensitising researchers to the more subtle features of the data.

In this research investigation, initial themes were identified from the literature review as a result of previous studies and the theoretical framework related to the research topic. However, during the transcription process and initial data analysis emerging themes were selected based on two features namely prevalence and uniqueness. The themes were selected in terms of whether or not they were prevalent across all the dataset. Also, emerging outcomes were developed from several of the original themes.

Braun and Clarke (2006) argue that one of the main criticisms of qualitative research relates to the lack of structure it provides, including the use of thematic analysis. Due to the nature of qualitative research, a standardised approach for analysis for interviews has not been developed (Saunders et. al., 2003). However, it can be stated that thematic analysis does offer a framework to structure the data. A fifteen-point checklist was devised by Braun and Clarke

(2006:96) to ensure validity and rigour when using thematic analysis (Table 7.4). The fifteen-point outline acts as a useful guide through the whole research process, starting from transcription to the final written report. This research used the criteria of good thematic analysis in order to verify reliability as set out in Table 7.4.

Process	No.	Criteria
Transcription	**1**	The data has been transcribed to a suitable level of detail and the transcripts have been checked against the recordings for exactitude.
Coding	**2**	Each data item has been given the same attention throughout the coding process.
	3	Themes have not generated from a few isolated examples, but instead the coding process has been thorough, inclusive and comprehensive.
	4	All relevant extracts for each theme has been collected
	5	Themes have been checked against each other and checked against the original dataset
	6	The themes are internally sound, reliable and distinctive.
Analysis	**7**	Data has been analysed and interpreted in depth rather than described and presented.
	8	Analysis and data match one another. The extracts demonstrate the analytical claims.
	9	Analysis presented provides a well-organised journey through the data and topics.
	10	A balance is provided between the analytical narrative and illustrative extracts is provided.
Overall	**11**	Enough time and resources have been provided to complete all phases of the critical analysis.
Written Report	**12**	The assumptions about, and specific approach to thematic analysis are clearly explicated
	13	There is consistency of the process and what is explained will be done is carried out to the final write up.
	14	The language and concepts used in the report are consistent with the epistemological position of the analysis.
	15	The researcher is positioned actively in the research process and themes do not simply emerge.

Table7.4: Criteria of Good Thematic Analysis (Braun and Clarke, 2006:96)

7.6 Coding Data for Thematic Analysis

Bryman and Bell (2007:725) define coding as 'the process whereby data is broken down into component parts, which are given names'. Coding of data is considered to be a crucial stage in the data analysis process. Basit (2003:144) states that the process of coding offers the researcher the opportunity to systematically comprehend textual data. He argues that,

> Codes act as labels for allocating units of meaning to the descriptive or inferential information compiled in a study and are attached to words, sentences or whole paragraphs, connected or unconnected to a specific setting.

Interview coding is used to capture what is in the interview data and to learn how people make sense of their experiences and act on them (Charmaz, 2006). Charmaz (2006) further argues that coding is the first step of data analysis as it helps to move away from particular statements to more abstract interpretations of the interview data. Maxwell (2005) argues that a researcher has a multiple of analytical options that are categorized into three: (1) *memos, (2) categorising strategies, and (3) connecting strategies.* It can be argued that a combination of these strategies is required when coding data. These strategies include reading the transcript and observation notes on many occasion; writing memos; developing coding categorisations; applying these themes to the data; and concluding in building contextual relationships between themes in the data.

Bringer et al. (2004) argue that the researcher must be transparent in their use of computer software and explain all the elements concisely and thoroughly. Buchanan and Jones (2010) see the use of software for data analysis as the beginning of a new age in qualitative research. It is widely accepted that software packages offer a certain level of organisation which is very hard to manage manually (Basit, 2003). Furthermore, computer based data analysis is useful in cutting, sorting, re-organising and collecting tasks which the researcher has previously done with note cards, scissors and coloured pens (Weitman and Miles, 1995). Walsh (2002) argues that it can also offer a level of transparency and can provide better accuracy than manual analysis. Welsh (2002) further found out that when conducting qualitative studies using NVivo software, that it is helpful while building a rigorous database for the data. Also, it demonstrated very clearly all the coded data and the way it had been coded. Further, she found out that the management of these long files was very easy using NVivo software.

Opponents of using the software, such as Buchanan and Jones (2010) argue that conducting analysis electronically can result in methodological impurities when data is transferred into an

environment of ‘ones and zeros’. Furthermore, this may result in a misrepresentation or simplification of the multi-dimensional qualities of the original data. Willig (2009) suggests that software-assisted data analysis may encourage too much scrutiny of specific words and phrases rather than the interpretation of the data as a whole.

Another argument puts emphasis on the usefulness of computers in counting and producing numbers. Welsh (2002) states this may force researchers into the trap of turning qualitative accounts into semi-quantitative analysis by enumerating the facts rather than interpreting them. Coffey and Atkinson (1996) argue that no amount of electronic coding can produce new theoretical insights without the application of disciplinary knowledge and the creativity of the researcher. Willig (2009) argues that software can often distance the researchers from their data.

Generally, the research community is divided in regard to the advantages and disadvantages of digital intervention in what is fundamentally a human endeavour (Basit, 2003). However, Welsh (2002:9) stated that in a study using both manual and computer-based (NVivo) analysis techniques, he argues that ‘in order to achieve the best results it is important that researchers do not rely either on electronic or manual methods and instead combine the best features of each’.

The researcher has adopted a combination of conducting analysis both manually and electronically. The researcher started the interview analysis by searching for themes manually in the transcript. Afterwards, the researcher inputted that data into the NVivo10 software. Then the researcher coded the interview data using the software because it was the best tool for organizing and presenting the data. However, the researcher used manual coding to get the emerging outcomes as the software did not offer anything new. This was due to the inability of the software to comprehend the organisational setting and context of the data and the researcher had to do them manually. Patton (2002) supports this approach as he argues that text by itself offers limited interpretation.

Miles and Huberman (1994) suggest a best practice for manual data analysis whereby the researcher prepares a provisional ‘starting list’ of codes prior to fieldwork. These codes emanate from the research questions, literature review and theoretical framework. This approach was adopted for this research as eleven themes were selected as the provisional list and subsequent codes or emerging outcomes were produced as a result of the analysis.

According to Braun and Clarke (2006) the analysis of the interviews was conducted as shown in Table 7.5:

S/N	PHASE	DESCRIPTION OF THE PROCESS
1	**Conduct Interviews**	Conduct Thirty-Four Interviews and digitally record each interview.
2	**Create Transcripts**	Transcribe each interview immediately after collecting data so as to ensure the researcher is familiar with the data.
3	**Initial Organising Data**	Begin coding the data as the initial coding will guarantee that all relevant material is allocated to the eleven themes.
4	**Code Data**	Code the data with each theme to show patterns and emerging outcomes.
5	**Review Codes**	Codes were reviewed thoroughly for accuracy.
6	**Name Codes**	Emerging outcomes of each theme were named and analysed.
7	**Analyse and Present Data**	Key features from the interview were presented and analysed within each theme. Emerging outcomes of each of the themes were deduced and presented.
8	**Compare Findings from the Interviews**	Findings were compared with documented data and literature and conclusions formed.

Table 7.5: Coding and Analysis of Interviews (Based on the work of Basit, 2003)

Table 7.5 shows the eight phases that the researcher followed and also the description of what each phase entailed. The first phase was conducting the interview then; creating transcripts; initial organising of data; coding data; reviewing data; naming codes; analysing and presenting data and comparing findings from the interviews respectively.

Table 7.6 showing the eleven themes and fifty-one emergent-themes of the research study.

S/N	THEMES	SUB-THEMES
1	FUNCTION OF OFFICE	ICT Regulation
		Law Enforcement
		Legislation
		National Coordinator
		Telecoms Regulation
2	ROLE IN FIGHTING CYBERCRIME	Investigation
		Forensics Support
		Legal& Prosecution
		ICT Support
		Media& Prevention
		National Coordinator
		Telecoms Regulation
		ICT Regulation
		Legislative Support
3	DEFINITION OF CYBERCRIME	Cyber-Enabled Crimes
		Cyber-Dependent Crimes
4	FORM OF CYBERCRIME	AFF & Financial Fraud
		Hacking & Malware
		Romance Scam
		Scam Messages
5	CAUSES OF CYBERCRIME	Financial Gain
		Greed
		Lack of Awareness
		Poverty
		Unemployment
		Vulnerability of Systems
		Weak Laws
6	PARTNERSHIP OF STAKEHOLDERS	Internal Partnership
		External Partnership
7	BENEFITS OF PARTNERSHIP	Internal Partnership
		External Partnership
8	MEASURES AND BENEFITS OF MEASURES	Awareness Campaign
		Best Practices
		Enforcement
		Funding & Logistics
		Partnership
		Training and Manpower
		Benefit of Measures
9	LAWS	Amendment of Laws
		Enforcement of Laws
		Laws Are Adequate
10	CHALLENGES	Bureaucracy
		Inadequate Funding & Tools
		Laws & Jurisdiction
		Technology
		Inadequate Training and Education
11	RECOMMENDATIONS	Education & Awareness
		Funding & Tools
		Laws & Policy
		Partnership
		Training

Table 7.6: Showing Nodes and Sub-Nodes in the Research Study

7.7 Demographic Interview Findings

Table 7.7 provides an overview of the background of the each of the seven organisations that participated in this research. The table is divided into five sections namely the name of the organisation; the sector to which they belonged; designation of interviewees; number of interviewees and the role they play in tackling cybercrime in Nigeria and the UK.

ORG	NAME OF ORGANISATION	SECTOR	NO	Role
A	**Economic and Financial Crimes Commission**	Law Enforcement	28	Enforcement of EFCC; AFF & Cybercrimes Act. Member of CAC
B	**Office of the National Security Adviser**	Presidency	1	National Coordinator of Cybercrimes Act. Member of CAC
C	**National Assembly – Senate**	Parliament	1	Making Laws – Oversight of all MDAs
D	**Nigerian Communications Commission**	Telecommunication	1	Telecoms Regulator. Member of CAC
E	**National Information Technology Development Agency**	Information Comm. Technology	1	ICT Regulator. Member of CAC
F	**National Crime Agency**	Law Enforcement	1	National Coordinator of National Cybercrime Unit
G	**West Yorkshire Police**	Law Enforcement	1	Territorial Police for West Yorkshire

Table 7.7 Overview of Seven Participants Organisation

Organisation A – Economic and Financial Crimes Commission (EFCC)

Organisation A is the leading law enforcement agency in the investigation of economic and financial crimes in Nigeria. The organisation has the powers to investigate advance fee fraud, a variant of cybercrime through the Advance Fee Fraud and Other Related Offences Act 2006 and investigate other forms of cybercrime through the Cybercrimes (Prohibition, Prevention) Act 2015. It is a key member of the Cybercrime Advisory Council in Nigeria.

Organisation B – Office of the National Security Advisor (ONSA)

Organisation B is the Office of the National Security Advisor under the National Security Advisor and acts as the overall coordinator of the Cybercrime Advisory Council. The ONSA is also the designated Nigerian Computer Emergency Response Team (ngCERT). The ONSA also serves as the National Forensic Lab of Nigeria. It initiated and coordinated the development of the National Cybersecurity Policy and Strategy of Nigeria.

Organisation C – National Assembly (Senate)

Organisation C is the National Assembly which houses the Senate and the House of Representatives. The National Assembly is one of the three arms of the Nigerian Government and it is solely responsible for making and amending laws. It also provides oversight functions of all Ministries, Departments and Agencies (MDAs) through its committee functions. The Senate Committee on ICT & Cybercrime are responsible for making input into ICT and Cybercrime Laws and provides oversight duties to MDAs that are mandated to tackle cybercrime in Nigeria.

Organisation D – Nigerian Communications Commission (NCC)

Organisation D regulates all mobile network operators (MNO) and internet service providers (ISPs) in Nigeria. It is responsible for providing guidelines, framework and enforcement of policies in the communications sector. It plays a key role in addressing the issue of cybercrime in Nigeria as it regulates all the ISPs and MNOs that manage all the communication platforms that are frequently used by criminals to commit crime online. It is a member of the Cybercrime Advisory Council (CAC).

Organisation E – National Information Technology Development Agency (NITDA)

Organisation E provides regulation, framework and guidelines for all Ministries, Department and Agencies (MDA) in the implementation of ICT in Nigeria. It is a member of the Cybercrime Advisory Council (CAC).

Organisation F – National Crime Agency (NCA)

Organisation F is a law enforcement agency responsible for leading the UK's fight against serious and organised crime. It coordinates the National Cyber Crime Unit (NCCU) which is the UKs response to cybercrime through partnership and coordination with other local and international stakeholders.

Organisation G – West Yorkshire Police (WYP)

Organisation G is the territorial police force responsible for policing the West Yorkshire region in England. It is the fourth largest police force in England and Wales and one of the few police forces to have a dedicated cybercrime unit in the UK.

7.8 Interview Findings – Analysis and Interpretation of Themes

After an overview of each of the organisation's background is given, the following provides a summary of each interview, which has been taken from the transcripts for each organisation and was based on the responses from the interviewees from the interview questions. Following this each theme is then analysed and an interpretation is provided.

7.8.1 Theme 1: Function of Office

In order to analyse this theme, the organisations were divided into their sector (See Table 7.1) based on their enabling laws, mandate and primary purpose of existence. The Function of the office was, thus, divided into five distinct sectors namely:

1. Law Enforcement
2. National Coordinator
3. Legislation
4. Telecommunications Regulator
5. ICT Regulator.

Figure 7.5 shows the themes and the emergent outcomes

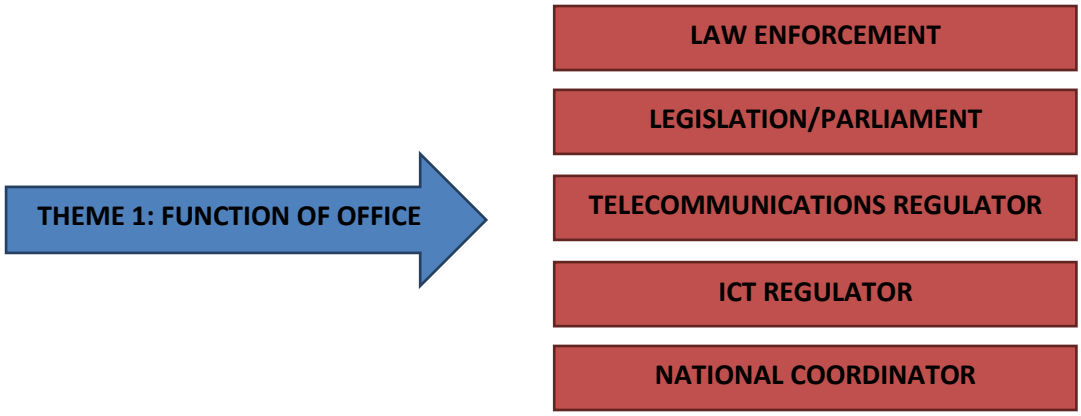


Figure 7.5: Theme 1: Function of Office & Sub-Themes

30 of the participants came from the law enforcement constituents from both the UK and Nigeria. All participants were asked what roles their respective organisations played in investigating and tackling cybercrime within their jurisdictions and in conformity with the mandate establishing them. Therefore, 'Theme 1: Function of Office' was analysed based on participants' answers provided.

The Law Enforcement members that participated in the research gave their answers by reflecting on the overall mandate of their organisation which was to fight crime and criminality in society and enforce relevant laws in tackling the menace of cybercrime.

> *the mandate of the EFCC is to investigate economic all economic and financial crimes……that it means what it means is that economic and financial crimes can come in so many forms and we see cybercrime one of those crimes that falls within EFCCs mandates. Because if you look at financial crimes in this day is there have now gone digital more or less and we have the duty again by law to enforce the Advance Fee Fraud Act. And we have seen a shift from the local traditional ways fraudsters do conduct their fraudulent activities.*(Participant 1, Cybercrime Investigator, 30/08/16).

This response was coded or repeated 28 times by most of the participant by stating that the primary role of their organisations was to fight economic and financial crimes and serious and organised crimes respectively. Each of their responses was reflective of the departmental role each of their unit or section played. 5 participants from the Legal department all commented on the function of their office from the perspective of the relevant section of the laws that empowered them to prosecute cybercrime.

> *The role that EFCC plays is as contained in section 13(2) of the Economic and Financial Crimes Commission Act 2004 as amended and is we prosecute offenders, we recover assets, we forfeit assets and we give legal advice and any other legal duties as it may be assigned to us.*(Participant 25, Cybercrime Prosecutor, 17/08/16).

The Office of the National Coordinator of the Cybercrime Advisory Council who is responsible for the enforcement of all cybercrime laws and policies, however, had a broad and encompassing mandate:

> *the provision of part 4 section 41 its says that the office of the National Security Advisor shall be the coordinating body for all security and enforcement agencies under this Act, its talking about the cybercrime Act. One, the main thing the Office of the National Security Advisor here is doing is to coordinate the cybercrime, the enforcement of the cybercrime Act both for the security and law enforcement agencies.* (Participant 29, National Coordinator, 24/08/16).

This response was only coded once as there was only one participant from Organisation B who was interviewed. The response further shows that the office is equally the responsible for other mandates such as:

> *The provision (a) states provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria. The (b) states ensure formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria.* (Participant 29, National Coordinator, 24/08/16).

The response from the legislative arm of the Nigerian government and a member of the Senate Committee on ICT & Cybercrime was different from other responses as the function of the National Assembly is strictly for making laws and oversight functions of Ministries, Department and Agencies in Nigeria.

> *The only role we play is for us to give an enabling law to allow the agencies that are handling cybercrime to have a backing and another law and when they law are there and there are people that commit these crimes so that they can be punished, that is the first assignment of the National Assembly. And then most people in this country do not even know that there is a law on cybercrime, though the law we are trying to re-enact and re-amend it and which it has already passed through the first reading and it is awaiting the second reading because of the situation we have all over the world, the dimension of cybercrime is taken.*(Participant 30, Senator, ICT & Cybercrime, 31/05/17).

The response from the Telecommunications Regulator in Nigeria was specific to its mandate in regulating users and providers of internet and telecommunication services. This response was only coded once as only one participant participated in the research study.

> *Well to start with NCCs mandate has to do with coming up with policy issues, regulations and guidelines to the telecommunications industry in respect to aspects that have to do with cybercrimes and cybersecurity in Nigeria. In doing that, NCC works with other stakeholders and relevant agencies and law enforcement agencies.* (Participant 32, Telecoms Regulator, 13/06/17).

The response from the ICT Regulator in Nigeria was equally specific to its mandate in regulating the use of ICT in Nigeria. The response was only coded once as one participant participated in the research study.

> *the department of Cybersecurity in NITDA was established about a few months ago. It is in response to the burning issue of cybersecurity and threats to national sovereignty and economic wellbeing of a country and with the prevalent issues of cybercrime being committed everywhere, it behoves on the current administration of NITDA that for us to be able to address this issues effectively there should be a department to handle that, so that was how the department of cybersecurity was born in NITDA.* (Participant 31, ICT Regulator, 05/06/17).

7.8.2 Theme 2: Role in Fighting Cybercrime

In order to analyse this theme, the interview participants were divided into their department, units and sections (See Table 7.1) respectively. These various departments served as sub nodes and participants were grouped accordingly. Theme 2 asked questions based on specific roles each of the departments or sections played in tackling cybercrime. In order to analyse this theme, it was further divided into nine (9) sub themes (See Table 7.6) namely: Investigation; Forensics; Legal; ICT; Media; National Coordinator; Legislation; Telecommunications Regulation; ICT Regulation; Legislation. 30 of the participants came from the law enforcement constituents from both the UK and Nigeria; One each from the National Coordinator, Legislation, Telecoms Regulator and ICT Regulation sector respectively. All participants were asked specific questions regarding the role their respective departments or sections within their organisation played in addressing the issue of cybercrime in Nigeria and the UK. Therefore, 'Theme 2: Role in Fighting Cybercrime' was analysed based on participant answers provided. Figure 7.6 shows the theme and the emergent outcomes.

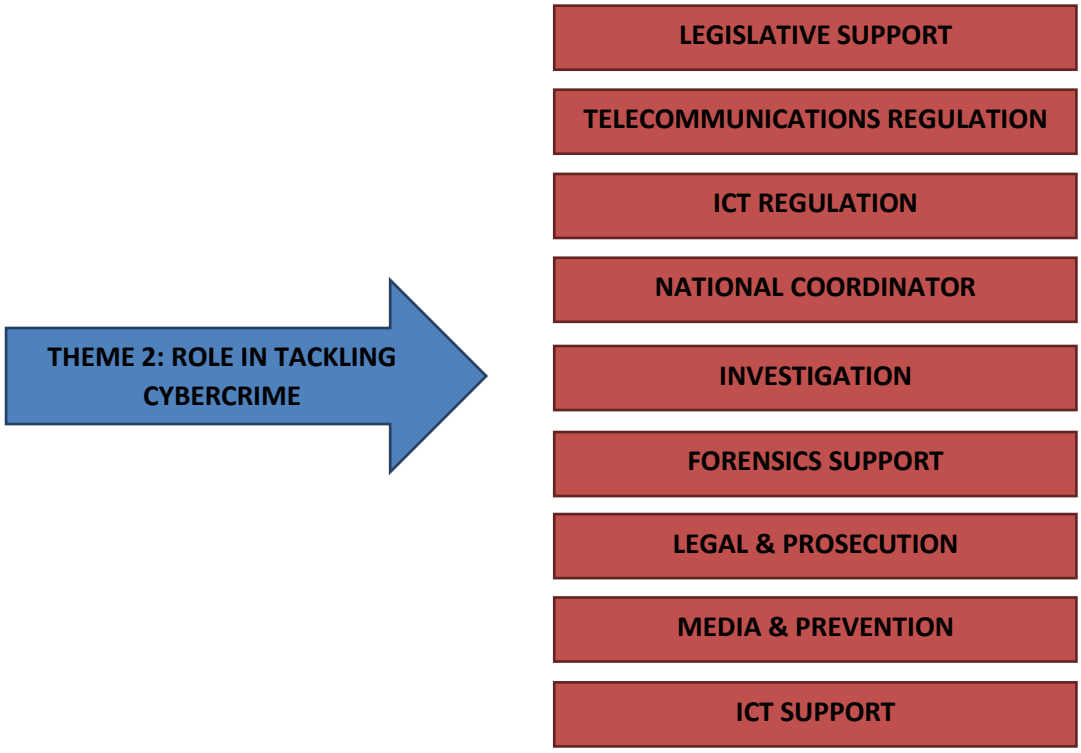


Figure 7.6: Theme 2: Role in Tackling Cybercrime & Sub-Themes

Investigation

The participants that fall under the 'Investigation' category are eight in number; six from Nigeria and two from the UK and they all worked in a law enforcement agency. The Investigators' answers mostly centered on the specific roles they played based on their mandates of investigation of financial and serious crimes. Also, participants were asked the relevance of their roles in investigating cyber-crime or computer related offences.

> *The mandate of the section is line with the mandate of the Commission only as it relates where we narrow it down to. The overall mandate is to rid Nigeria of the scourge of cybercrime. Create awareness; create awareness on the negative impact of cybercrime on Nigerian economy, on Nigerians themselves.* (Participant 2, Cybercrime Investigator, 11/08/16)

This answer was repeated six times by all of the Investigators in Nigeria. When further asked on the relevancy of their respective section in tackling cybercrime, one of the Investigators answered:

> *It is important of course the unit was specifically created for such purpose. I think its very important because we know that we have been already been given that mandate to investigate cybercrime and we do all our best to, we do searches and we do some in house training as*

> *well as some trainings from other institutions that would arm us with the recent trends going on in the cyber world.* (Participant 4, Cybercrime Investigator, 18/08/16).

This response was repeated four times, however, another participant who works in both investigation and ICT spoke specifically about the capability of the cybercrime unit as being the reason why the unit is relevant in tackling cybercrime.

> *The cybercrime unit is well equipped to handle cybercrimes offences. We are well trained and aware of the new trends in cybercrime investigation and they know all the necessary things that have to be done for the offence to be properly investigated which are not limited to statement taken.*(Participant 21, ICT Officer, 30/08/16)

Forensics Support

The participants that fall under the 'Forensics Support' category are 6 in number and all from a law enforcement agency in Nigeria. The forensic examiners' answers mostly centered on the specific roles they played based on professional scientific support they offer in investigating cybercrimes in Nigeria. Also, participants were asked about the relevance of their roles in investigating cyber-crime or computer related offences.

> *Now the role of the forensics in the EFCC primarily is to provide support, scientific support to the work of the investigators. In the four key areas, first area being digital forensics which is further divided into mobile phone forensics, computer forensics and live forensics.* (Participant 7, Forensics Examiner, 11/08/16).

This response was coded 4 times but one participant spoke mostly on the investigative rather than the supportive role, the forensic unit played.

> *Particularly cybercrime, off course, cybercrime, you cannot conclude the investigation of cybercrime without identifying digital data. It may exist in a form of programs, it may exist in a form of communication with cybercriminals, it may exist in a form of hardware's which are implemented on a device. So the unit specifically help to elicit evidence for the prosecution of cybercrime.* (Participant 10, Forensic Examiner, 15/08/16).

This response was repeated by another participant who held the view that forensics played more than a supportive role in investigation but could also investigate cybercrime.

Legal and Prosecution

The participants that fall under the 'Legal' category are 5 in number and all from a law enforcement agency in Nigeria. The cybercrime prosecution officers' answers were centered on their specific roles in prosecuting cybercrime and providing legal advice and training to both internal and external stakeholders. Also, participants were asked the relevance of their roles in prosecuting cybercriminals or computer related offences.

> *Our mandate says being the prosecuting department of the Economic and Financial Crimes Commission, we are charged with the prosecution of offenders, that is court related, charge them to court and then prosecute the case, start to finish.* (Participant 28, Cybercrime Prosecutor, 19/08/16)

This response was repeated three (3) times, however, one participant mentioned how the prosecution of cyber related offences had made the legal department prosecute it differently from other crimes.

> *Cybercrime is a new criminal system or a new platform in which modern crime is being committed by various individuals. The prosecution of cybercrime even though is a bit technical but the department prosecute cybercrime cases in the same manner and rigor in a way it prosecutes other offences as it relates to economic and financial crimes.* (Participant 27, Cybercrime Prosecutor, 17/08/16).

When the participants were asked about the relevancy of the legal department in investigating and prosecuting cybercrime, all five participants agreed that without the legal department, cybercrime in Nigeria would not be properly investigated to a logical conclusion.

> *The role of the legal and prosecution department cannot be over-emphasized, it is invariable. It is fundamental. Without the role of the legal and prosecution department, all offences that have to do with cybercrime would arrive dead. It is through the legal and prosecution department, offenders are identified, that, it is through the legal and prosecution department that offenders are taken before the court to face the law,* (Participant 26, Cybercrime Prosecutor, 19/08/16).

ICT Support

The participants that fell under the 'ICT Support' category were six in number and all from a law enforcement agency in Nigeria. The ICT participants' positions ranged from the Head of the Unit to the various ICT sections that were relevant in tackling cybercrime in Nigeria. Their answers were centered on the specific roles they played in rendering professional support and ICT services to relevant stakeholders in investigating cybercrime. Also, all the participants were asked about the relevancy of their roles in investigating cyber-crime.

> *We provide operational support, the operatives always seek support and training on how to use the systems and how to use the computers, how to use software's and we provide trainings for like cybercrimes training for members of the Operations unit, Legal unit and the different units that we have. And we also provide logistics as well.* (Participant 22, ICT Team Lead, 17/08/16)

This response centered on providing operational support and was repeated four (4) times while two (2) other responders specifically spoke about how ICT conducted research and provided training to investigators.

> *it also tries to research and find trends in cybercrime and help to educate the investigative cybercrime unit and basically it tries to breach the digital disconnect between the officers and technology*. (Participant 20, ICT Team Lead, 23/08/16)

When asked on the relevance of ICT in investigating cybercrime, all six (6) responded by linking the importance of having knowledge of ICT technology in order to properly investigate cybercrime.

> *It's a technology crime and at the same time IT department should play a role because you cannot even investigate cybercrime without IT because it is a technology based crime so definitely you would have to use that same technology to investigate those kinds of crimes.* (Participant 23, ICT Team Lead, 18/08/16)

Media and Prevention

The participant that fell under the 'Media' category are five (5) in number; two (2) from the Enlightenment and Re-orientation (E&R) Unit and three (3) from the Public Interface Unit (PIU). The Media Officer positions ranged from the Heads of the Sections to their various team members that were relevant in cybercrime prevention and awareness campaigns in Nigeria. Their answers were centered on the specific roles they played in rendering professional support through education, prevention and awareness campaign to members of staff of the organisation and the general public. Also, all the participants were asked about the relevancy of their roles in tackling cyber-crime in Nigeria.

Two members of the E&R responded by stating that their mandate was targeted at the public in raising awareness of cybercrime:

> *E&R has done a lot to conscientize the youth because it has been observed that it is the groups or this sector of the Nigerian population that is usually vulnerable to the cyber criminality. (*Participant 16, Media Team Lead, 25/08/16)

In contrast, the three (3) members of the Public Interface Unit that is responsible for responding to members of the public through the social media networks and face-to-face, all agreed about the information dissemination role they played in informing the general public.

> *we educate members of the public….. So all of these experience we were able to push it out and educate members of the public so that they would not fall victims of cybercrime and all of that.*(Participant 14, Media Unit Head, 12/08/16).

When asked on the importance of their units in addressing the issue of cybercrime in Nigeria, responses such as the following were received:

> *it is very important because we create awareness on the ills of committing the crime and also how it is done, the modus operandi, for members of the public to be weary of these methods*

that are used by internet fraudsters to defraud them (Participant 13, Media Unit Head, 24/08/16)

This was repeated three (3) times; however, one of the participants spoke solely on how the media officers acted as first responders to victims of cybercrime by counselling them.

We talk to them, we give them advice, we talk to them personally. Sometimes we become like psychologist or consultant because we need to talk to people some of them are affected really badly, while some don't even know what cybercrime is all about. (Participant 15, Media Team Lead, 11/08/16).

National Coordinator

There was only one participant from Organisation B which serves as the national coordinating agency on cybercrime investigation in Nigeria. The participant's answers were narrowed down to its mandate by law to coordinate all activities of other organizations and to serve as the designated national computer emergency response team where all cybersecurity and cybercrime offences were reported. Also, the participant was asked on the relevancy of their role in addressing issues of computer-related offences in Nigeria.

We have, ngCERT have a platform of where, we have a sun that tries to tell us the temperature of the Nigerian cyberspace where we monitor ahhh threat related to, threat related to botnet, threat related to vulnerabilities, threat related to spam, threat related to webpage defacement of government websites. Ahhh also to malwares, those are the threats. And when we get these things, when we get these threats, we try to analyse them and send advisory to all our stakeholders. (Participant 29, Head, ngCERT, 24/08/16)

This response was only repeated once. Also, when asked on why the national coordinator's office was relevant to addressing cybercrime in Nigeria, the participant spoke about the borderless nature of the crime and how issues of coordination and partnership could be better handled with one central authority in charge:

The Cybercrime Act categorically stated that ngCERT should be the point of contact for such kind of international cooperation. (Participant 29, Head, ngCERT, 24/08/16)

The participant also stated its capacity in the state of the art forensic laboratory and in training stakeholders such as law enforcement officers and judges as to why it was relevant in being the arrow head in fighting cybercrime in Nigeria.

So it is important, it is very important key because we have the forensic lab, we have some capacity, we do some analysis and we also do training of law enforcement once in a while and also we do train judges and tell judges look these is the way this crime happens. (Participant 29, Head, ngCERT, 24/08/16)

Legislative Support

There was only one participant from Organisation C which is the National Assembly

responsible for making laws in Nigeria. The Senator is a member of the Senate Committee on ICT & Cybercrime. The Committee is responsible for making cyber laws and amending existing laws that have to do with ICT and Cybercrime. The participant's answers were based on the oversight function the committee has on all MDAs that dealt with issues of ICT and Cybercrime. Also, the participant was asked on the relevancy of their role in addressing issues of computer-related offences in Nigeria.

> *The Committee we have started a review on the existing law that we believe is not full enough to tackle the present cybercrime that is happening all over the world because we have to sign a lot of pacts with other countries in other to make it work or make it effective.* (Participant 30, Member, Senate Committee on ICT & Cybercrime, 31/05/17)

The participant's answer emphasised the review of existing laws in order to make them more effective in tackling cybercrime in Nigeria. The interviewee's response to the relevancy of the Senate Committee in tackling cybercrime was:

> *Because it is the only Committee that would be able to relate with other Committees or other legislative Houses all over the world that for example the last time I went to Korea, our Committee on Cybercrime met with the Committee on Cybercrime in Korea and the same thing happened when we went to New York at the United Nations, when a seminar was organized on cybercrime. So these are some of the experiences you gather from such place and to come and use it amongst some of your Committee members and be able to implement on our system and for us to fight the criminals* .(Participant 30, Member, Senate Committee on ICT & Cybercrime, 31/05/17)

The response by the Senator emphasised how the Committee was the only parliamentary interface that related to local and international stakeholders in the global fight against cybercrime.

Telecommunications Regulation

There was only one participant from Organisation D which is the Nigerian Communications Commission that is responsible for regulating the telecommunications sector in Nigeria. The participant is from the cybersecurity division of the organisation and their responsibilities are based on their mandate to provide policies and cybersecurity strategies to the ISPs and Telecoms companies that provide the internet and communication services that are frequently abused by cybercriminals. Also, the participant was asked on the relevancy of their role in addressing issues of computer-related offences and breaches in Nigeria.

> *The cybersecurity unit of the Commission serves as the primary interface between the telecommunications agencies in Nigeria and Law Enforcement Agencies in the country in*

> *respect with crimes and investigations that have to do with telecommunications services.*(Participant 32, Telecoms Regulator, 13/06/17)

The participant stated that the unit served as the primary interface between law enforcement in respect of investigating cyber related offences. When asked about the relevancy of the unit in tackling cybercrime, the participant said:

> *First of all the unit is central to issue regulations in regulating the activities of telecoms company in Nigeria. Telecommunication is critical to Cybercrime Issues in Nigeria more especially since the Mobile telephony is the primary means of communication in the country and as you know the telecommunication industry are regulated by the Commission.(Participant 32, Telecoms Regulator, 13/06/17)*

The response given showed the importance of the telecommunications sector in addressing the issue of cybercrime in Nigeria and how the cybersecurity unit played an integral part.

ICT Regulation

There was only one participant from Organisation E which is the National Information Technology Development Agency that is responsible for regulating the ICT sector in Nigeria. The participant is from the cybersecurity division of the organisation and their responsibilities are based on their mandate to provide policies and cybersecurity strategies to the MDAs in tackling issues of cyber breaches and cyber related offences. Also, the participant was asked about the relevance of their role in addressing issues of computer-related offences and breaches in Nigeria.

> *We interface with other MDAs and our CERT has relationship with CERTs elsewhere like the Malaysian CERTs and the Canadian CERTs are all connected with us so we share information, we share expertise and all that so that is the way we handle cybersecurity issues.*(Participant 31, ICT Regulator, 05/06/17)

The ICT regulator's response emphasised the synergy of the department with international Computer Emergency Response Teams (CERT) in sharing information and expertise in handling cybersecurity issues. When asked about the importance of the department in investigating cybercrime in Nigeria, the participant said:

> *The role is very important we find that the first steps to tackling cybercrimes particularly the preventive and defensive aspects resolves around human beings. And it is of significance that the human beings whom are seen to be the weakest link in this whole setup are enlightened effectively so that they know when issues and requests to do this or that on the internet should be avoided. They know when to critically look at request before they accept it. (Participant 31, ICT Regulator, 05/06/17)*

The response was geared towards the preventative and defensive roles it played in

enlightening the public about the dangers of using the internet which most times created opportunities for criminals to easily target victims online.

7.8.3 Theme 3: Definition of Cybercrime

Definition of cybercrime is the third theme that emerged from the research study. All the thirty-four (34) interviewees were asked to define or state what they considered as cybercrime. Generally, there was not one definition of cybercrime but in order to analyse this theme, the participants' definitions were grouped into two broad definitions of cybercrime namely:

1. Cyber-Enabled Crimes;
2. Cyber-Dependent Crimes

McGuire & Dowling (2013b) state that cyber-enabled crimes are traditional crimes which can be increased in their scale or reach by use of computers, computer networks or other form of ICT. In contrast, cyber-dependent crimes can be committed without the use of ICT. Examples are financial fraud, 419, phishing, etc.

Cyber-dependent crimes or 'pure cybercrime' are offences that can only be committed using a computer, computer networks or other forms of ICT. Examples are malware, hacking, DDoS etc. (McGuire & Dowling, 2013a)

Therefore, 'Theme 3: Definition of Cybercrime' was analysed based on participants' participant answers provided, thus, two sub-nodes emerged from the definition of cybercrime and each is analysed below. Figure 7.7 shows the theme and the emergent outcomes

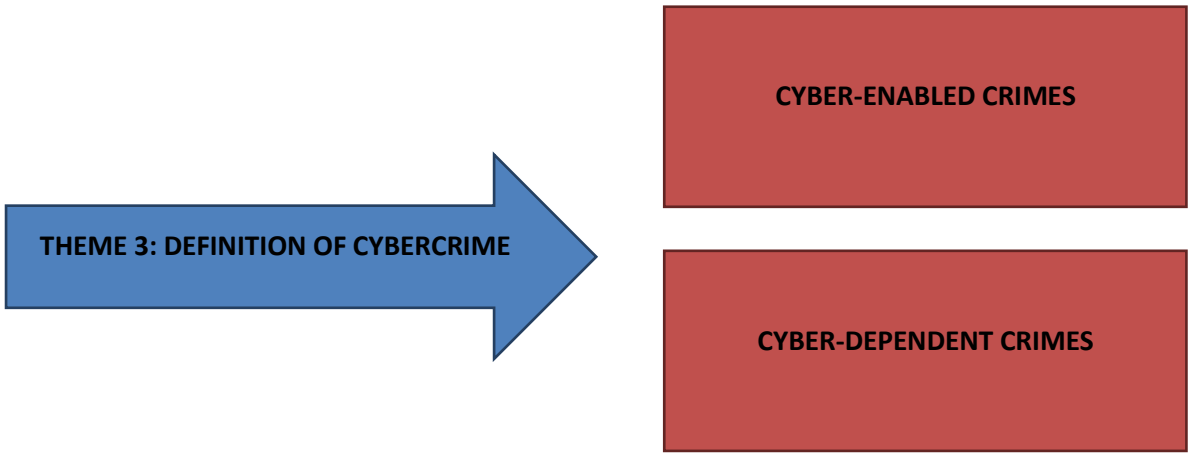


Figure 7.7: Theme 3: Definition of Cybercrime& Sub-Themes

Cyber-Enabled Crimes

Participants that defined cybercrime based on the definition by McGuire & Dowling (2013b) all stated that the use of ICT was important in committing the crime. Participant 23, thus, defined cybercrime as:

> *Cybercrime I believe is using technology to commit a crime be it financial, terrorism, be it child abuse, defamation of character, stealing of sensitize of information; so cybercrime is really a technology based crime* (Participant 23, ICT Team Lead, 18/08/16)

This response was repeated eighteen (18) times by different interviewees. However, since not all the participants were ICT proficient, the researcher noticed the participant answered the question mostly based on the department they worked in. For example, investigators defined cybercrime as:

> *Crimes that are considered as cybercrimes includes I can say marriage scam, OBT. The use of computers and electronic gadgets* (Participant 6, Cybercrime Investigator, 19/08/16)

This response was coded three (3) times while one of the participants from the UK refused to define cybercrime but referred the researcher to the Home-Office definition of cybercrimes which were categorised under cyber-enabled and cyber-dependent crimes respectively. The participant from the ICT Unit, however, defined cybercrime somewhat differently from the investigators by stating that:

> *It means the use of computers because we are talking about cyber, something in the space, something that you cannot see but can feel. So the use of computers can be considered as cybercrime, the use of electronic devices and other things like the use of the internet which is en-vouge and we have so many social media now. People can hide under it and commit crime.*(Participant 22, ICT Team Lead, 17/08/16)

This response that included the use of the internet was coded ten (10) times by different participants. However, it was only one participant from the 'Legal Department' who defined cybercrime within the scope of McGuire & Dowling (2013b) definition of 'cyber-enabled crime'; that participant stated:

> *Cybercrimes basically or simply are those crimes that are committed by computer, by the use of computer, by the use of network, internet.*(Participant 26, Cybercrime Prosecutor,19/08/16)

Cyber-Dependent Crimes

Participant who defined cybercrime based on the definition by McGuire & Dowling (2013a) all stated that such crimes could only be committed using a computer, ICT or the network. Participant 5, thus, defined cybercrime as:

> *Majorly, crimes that are, I can just narrow it down to crimes that has to do with IP, IPs related stuff, in order words most have passed through an internet facility, those are the things when you talk about cybercrime. Crimes that ordinarily exist or didn't pass through the internet, may have some attributes of the cybercrime but may not be cybercrimes.* (Participant 5, Cybercrime Investigator, 16/08/16)

This definition that involves the use of IPs and internet was repeated six (6) times by all the participants who defined cybercrime as cyber-dependent crimes. However, Participant 2 stated further that the crime must be committed by a digital device that is the target, tool and source in the commission of the crime:

> *Now in the context of work we do, we define cybercrime in very simple language. It is a crime in which a computer, computer network or any other digital device is the source, target or tool used in the commission of the offence.* (Participant 2, Cybercrime Investigator, 11/08/16)

Also, one of the participants added that the crime must target the confidentiality, integrity and availability for it to be termed as cybercrime:

> *We see crimes against computer systems and we see crimes by use of computer crimes as either as a tool and again as a target. So so again any crime I mean that's targeting the confidentiality, availability and integrity of computer systems we see it as a cybercrime.*(Participant 1, Cybercrime Investigator, 11/08/16).

This answer was only repeated once by all of the participants who answered the question.

7.8.4 Theme 4: Forms of Cybercrime

The fourth theme analysed was concerned with what form of cybercrime was more prevalent in the UK and Nigeria respectively. All the thirty-four (34) participants were asked this question and the emergent themes were categorised as follows:

1. Advance Fee Fraud and Financial Crimes
2. Digital Element
3. Hacking and Malware
4. Romance Scam
5. Scam Messages

Out of the thirty-four (34) participants, thirty-two (32) answered the question from the Nigerian perspective and two (2) from the UK perspective accordingly. Therefore, 'Theme 4: Forms of Cybercrime' was analysed based on the answers from the participants. Figure 7.8 shows the theme and the emergent outcomes

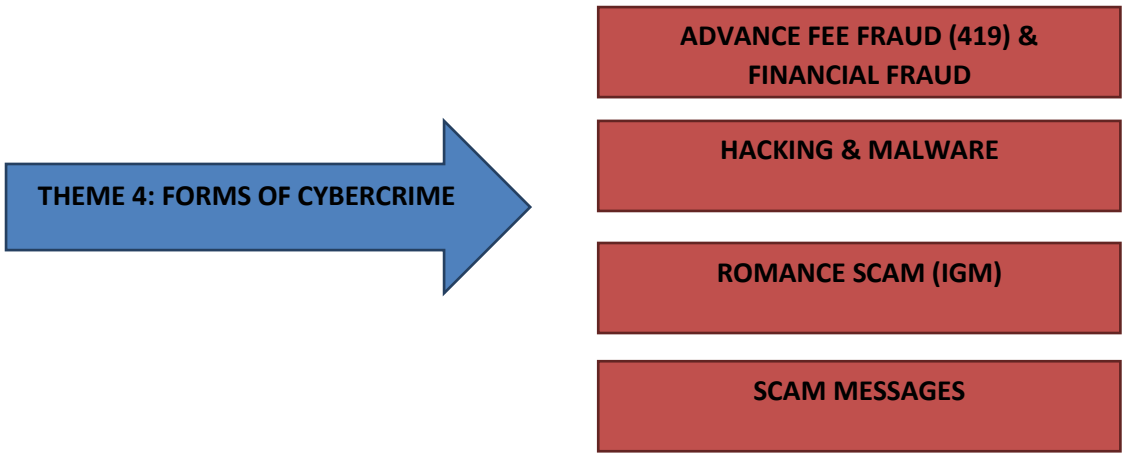


Figure 7.8: Theme 4: Forms of Cybercrime& Sub-Themes

Advance Fee Fraud and Financial Crimes

Fourteen (14) participants gave example of crimes such as advance fee fraud, 419 and obtaining under false pretence (OBT). One of the participants stated that the cybercrime most prevalent was:

> *It is usually Advance Fee Fraud. You know AFF is a kind of cybercrime. AFF is another form of 419 and cybercrime falls under it.*(Participant 16, Media Team Lead, 25/08/16)

Participant 20 further clarifies that the crimes ultimate aim is to get some financial gain. This response was repeated thirteen (13) times by various participants.

> *I think for me its financial fraud and a bit of identity theft with the aim of making some financial fraud.*(Participant 20, ICT Team Lead, 23/08/16).

Participant 25 also emphasised on the sending of fraudulent messages through the email in order to 'attain financial gain'.

> *Sending of false email. Sending of email that contains false information and mostly the send it to victims and in the process they gain financial, they attain financial gain.*(Participant 25, Cybercrime Prosecutor, 17/08/16)

This response was repeated in ten (10) times by the participants that there is one form of financial gain to be derived by these crimes.

Digital Element

However, one participant stated that the crime that was most prevalent must have a digital element and it affected most people.

> *Cyber-enabled crimes affect vast amount of people because it has got a digital element in the majority of crime that affect people.* (Participant 34, Cybercrime Investigator, 18/12/17)

Hacking and Malware

However, eight participants stated that the most common cybercrimes are hacking and the use of malicious software to commit crime. Participant 29 stated that with the advent of the digital currency called 'bit-coin', cybercrime has escalated to another level.

> *Recently with the advent of ah bitcoin exchangers in the country. You would find out the crime has escalated to people trying to to encrypt your data and tell you that you should pay Bitcoin but most of the crime now you see is defacement. Defacement of government websites, when people are not happy with government sometimes they go and deface it and stuffs like that.* (Participant 29, National Coordinator, 24/08/16).

This response showed the sophistication of the criminal to encrypt a victim's data was coded three (3) times, however, it was stated that the hacking of people's emails to commit crime was more prevalent. This response was repeated four (4) times by interviewees. Participant 24 stated that cybercriminals were:

> *Hacking into alarm systems on banks and they are hacking into things like that, they are hacking into MTN, telecommunications network, boycotting stuffs like that.*
> (Participant 24, Cybercrime Prosecutor, 18/08/16).

Romance Scam

Another variant of cybercrime that was considered to be common is romance scam. Participant 21 explained this form of cybercrime by stating:

> *Dating scams and romance scams which involve somebody taking up another man's identity to defraud a victim.*(Participant 21, ICT Officer, 30/08/16).

This response was coded three (3) times and Participant 5 further stated that a proposition of marriage was mostly made in order to entice the victims of such scams. He stated that:

> *IGM, has to do with these love scam, IGM, I go marry you. Those ones are prevalent and a lot of money loss in the process.*(Participant 5, Cybercrime Investigator, 16/08/16)

Scam Messages

Scam messages using SMS to send to members of the public were also a variant of cybercrime that was considered common. Participant 13 stated that:

> *The use of handsets to send text messages, text messages and then followed by phone calls, then scam mails, email. These are the three prevalent ones.* (Participant 13, Media Unit Head, 24/08/16)

This response was repeated three (3) times by interviewees and all agreed that the use of the mobile devices to send unsolicited SMS was a form of cybercrime that was prevalent in Nigeria.

7.8.5 Theme 5: Causes of Cybercrime

The fifth theme, 'Causes of Cybercrime' analysis was based on the causes of cybercrime in both the UK and Nigeria respectively. All the thirty-four (34) participants were asked this question and the emergent themes were categorised as follows:

1. Financial Gain
2. Greed
3. Lack of Awareness
4. Poverty
5. Unemployment
6. Vulnerability of Systems
7. Weak Laws

Each of these sub-nodes were analysed in relation to responses from the interviewees. Figure 7.9 shows the theme and the emergent outcomes.

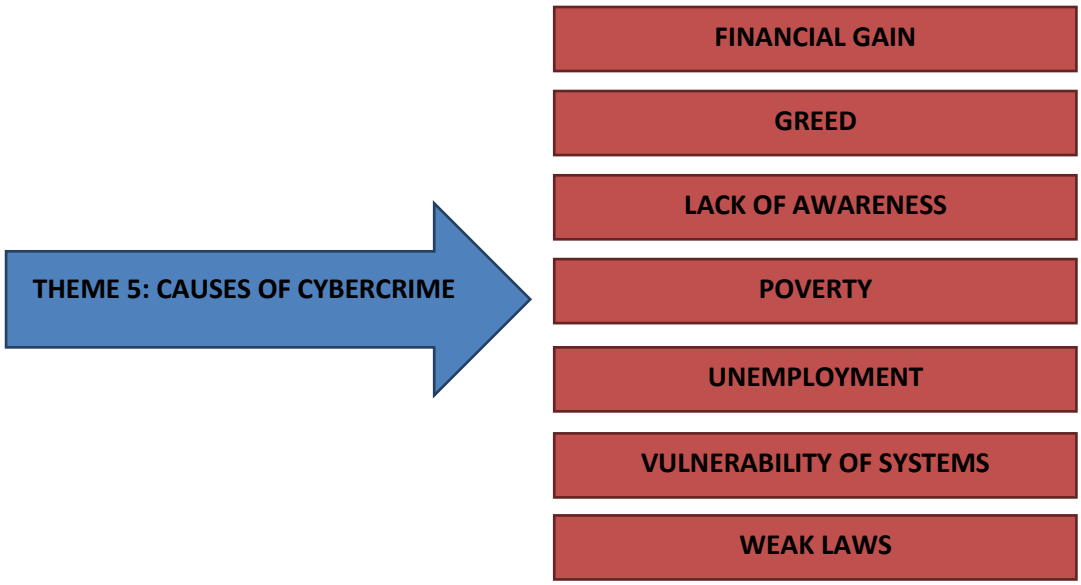


Figure 7.9: Theme 5: Causes of Cybercrime& Sub-Themes

Financial Gain

The participants that argued that financial gain was the main cause of cybercrime stated that:

> *Nigerian cybercrime cybercriminals are in need of the money so the ease to which they can gain financial gain is the main driving force for this.* (Participant 2, Cybercrime Investigator, 11/08/16)

A similar response was repeated amongst the three (3) interviewees that mentioned financial gain as a main reason for cybercrime. However, one of the participants also connected greed as the main factor of the criminals seeking financial gain:

> *Greed is a huge factor to get more than you bargain for through financial gain* (Participant 4, Cybercrime Investigator, 18/08/16)

Greed

About ten (10) participants argued that greed was the main factor that motivated people either to commit crime or to fall victims of cybercrime. Participant 23 categories the issue into two issues namely personal and government issues respectively. The participant explained further by stating:

> *First I would say there are some personal issues and there are some government issues. What I mean by personal issues mostly I would say greed. That is people want to make quick money, they don't want to work, they are lazy and they think they only way to make money is the quickest way of making money* (Participant 23, ICT Team Lead, 18/08/16)

This similar response that mentioned greed as the main motivating cause of cybercrime was coded ten (10) times, however, two (2) of the participants argued that greed and peer pressure were the main causes of cybercrime. Participant 16 stated that:

> *Mostly it is greed and peer pressure. You know youths are the people prevalent group that are susceptible to this kind of criminality and what is responsible is peer pressure. You would see your friend driving range rover jeep and before you know your friend is doing well in life and you ask him how he does it and he says "Yahoo Yahoo". So peer pressure, greed.*(Participant 16, Media Team Lead, 25/08/16)

The above response shows that youths are the people most likely to commit cybercrime and that greed and peer pressure were the main motivating causes of indulgence in cybercrime.

Lack of Awareness

Lack of awareness and poor education for both stakeholders that were involved in investigating cybercrime and members of the public was one of the factors that was responsible for the prevalence of cybercrime. Therefore, participant 34 clearly stated that:

> *Cyber-Enabled crime like a little bit about cyber-dependent crime is a lack of education, training and awareness both for staffs and also for the members of the public.*(Participant 34, Cybercrime Investigator, 18/12/17)

This response was repeated six (6) times as the main cause of cybercrime, however, one of the participants blamed the government for not making people aware about the dangers of cybercrime. The participant stated that:

And the second is from the other aspects, I mean government; I think there not many policies on security and cybercrime security awareness and another part there is ignorance as well. People are not really aware of certain security they should put in place to block or to prevent those kind of crimes. (Participant 23, ICT Team Lead, 18/08/16)

Poverty

Also, poverty was considered a motivating factor especially amongst the youth population in Nigeria as responsible for high prevalence of cybercrime in the country. Participant 17 stated that:

The majority of people committing these crimes are mostly youths; I think we are just going to peg it on poverty, even though poverty is not an excuse for anyone to commit a crime but we all know that a typical adolescent want what he wants and when he wants it so they likely chance is he is going to go ahead and do what he feels or what would bring money into his pocket one way or the other. (Participant 17, Media Team Lead, 16/08/16)

This response was repeated six (6) times and the participant identified poverty as the main factor that motivated the youths to commit cybercrime; however, two participants acknowledged poverty as the main cause for cybercrime but stated that it should not be an excuse for committing crime. The participant stated that:

I want quickly say that people say it is poverty, but that is very wrong. There is no excuse for criminality anywhere in the world that because you are looking for money to eat and you do not have a job is not a license to go into criminality. (Participant 16, Media Team Lead, 25/08/16)

Unemployment

Unemployment amongst the youths in Nigeria was considered as a main cause of cybercrime in the country. Eight (8) of the interviewees argued that unemployment was a main factor and some of the participants argued that:

If you look at the country today, 70% of our population is the youth so think of the youth without employment and they always devise a means of making money.And these are some of the factors that we see as being responsible for for the rise in cybercrime cases in the country. (Participant 1, Cybercrime Investigator, 30/08/16)

This response was repeated by eight of the participants, however, one of the participants argued that most of the perpetrators of cybercrime were students of tertiary institutions and unemployment was not a valid excuse for them to commit crimes. The participant argued that:

Unfortunately, Nigerians are highly intelligent people and I am not saying that because I am a Nigerian but we are highly resourceful in a lot of ways. There is high unemployment; there is high expectation in life for most Nigerians. You want to live a life; you don't want to start

> *From scratch, you just want to be there especially in tertiary institutions. If you look at a lot of the cybercriminals that are operating in Nigeria are operating from tertiary institutions. You cannot say it is joblessness as in lack of employment.*(Participant 19, ICT Team Lead, 11/08/16)

Vulnerability of Systems

Vulnerability of computer and ICT systems was also considered as one of the factors that caused cybercrime. Four (4) participants argued that most critical infrastructure especially in the financial sector were suitable targets for the cybercriminals. Participant 4 argued that another factor that caused cybercrime:

> *Is vulnerability of systems as well. I think the banks are kind of porous especially the financial institutions in terms of mobile banking.* (Participant 4, Cybercrime Investigator, 18/08/16)

This response was repeated four (4) times; however, one of the participants argued that the, *'availability and affordability of the internet' w*as also a factor that facilitated the criminals to have access to the internet easily to commit their nefarious activities.

Weak Laws

Weak laws and lack of enforcement of cybercrime related laws was considered as a factor in the high prevalence of cybercrime. Some of the participants argued that the punishment for the cybercriminals did not serve as a deterrence to crime; thus, there was a need for the laws to be amended. Participant 13 argued that:

> *The legal framework is there but the enforcement is not ah is not well carried out. And that and the punishment also does not serve as a deterrent. They are only jailed for maybe 7 years, 2 years, 5 years. I don't know what the new cybercrime Act says about the punishment, I don't know but I feel the punishment does not serve as a deterrent to check the use of internet to commit crime.* (Participant 13, Media Unit Head, 24/08/16)

This response was coded five (5) times; however, one of the participants also argued that even when the punishment was severe,the proceeds from crime was higher, then the offender would not hesitate to commit the crime even though the risk of being caught was high as long as they kept the proceeds of their criminal activities. Participant 19, thus, argued:

> *If the incentive is much higher and there is no chance of you getting caught and even if you would get caught the punishment does not outweigh the incentive in a very big way. It makes it easy for you to and there is a high motivation for you to commit those crimes.* (Participant 19, ICT Team Lead, 11/08/16).

7.8.6 Theme 6: Partnership

The sixth theme, 'Partnership' analysis was based on the role that partnership and collaboration between stakeholders play in addressing the issue of cybercrime. All the thirty-four (34) participants were asked this question and the emergent themes were as follows:

1. Internal Partnership
2. External Partnership

The sub-nodes are internal and external partnership. Internal partnership refers to internal departmental partnership within an organisation in tackling cybercrime while external partnership refers to the outside collaboration, regional and international collaborations between an organisation and other key stakeholders in addressing the issue of cybercrime. Figure 7.10 shows the theme and the emergent outcomes.

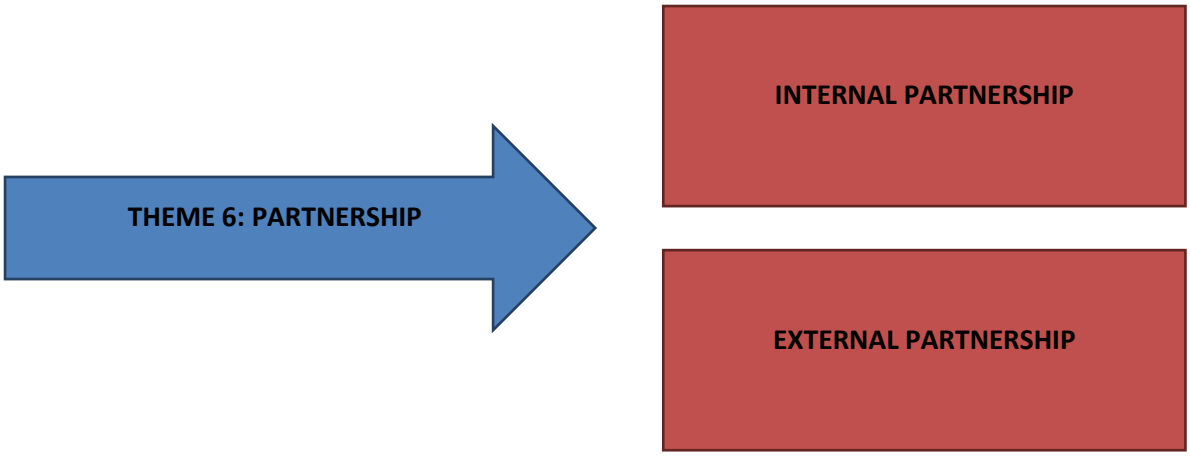


Figure 7.10: Theme 6: Partnership& Sub-Themes

Internal Partnership

About thirty-two (32) of the participants have one form of partnership with other departments and units within their organisation. According to Participant 21, the relationship was cordial and all units responsible for tackling cybercrime shared information. The participant stated that:

> *They have a very cordial relationship. All unit within the Commission they share information* (Participant 21, ICT Team Lead, 30/08/16)

This response was repeated ten (10) times amongst the participants. Another participant from

the ICT unit stated that the unit provided manpower support, ICT logistics and sometimes trained the investigators in investigating cybercrime. According to Participant 20, the ICT Unit did the following:

> *Basically it's in manpower provision and the ICT resource provision through computers, networks and internet, creating portals for service providers to give information and off course email is one of the important tools for fighting cybercrime and also what cybercriminals use to conduct the cybercrime. Also the ICT unit helps the public interface unit in terms of cybercrimes campaigns, so they give them the necessary information that they would use to feed the general public in order to fight cybercrimes and bring awareness.*(Participant 20, ICT Team Lead, 23/08/16)

This response of providing support and training to other units was coded twelve (12) times by participants mainly from the ICT and Forensics units. One of the participants who was a cybercrime investigator argued that in order to successfully investigate and prosecute a cybercrime incident, the evidence extracted from the suspect needed to be analysed by the forensics unit and legal charges drafted by the legal and prosecution department. The interviewee thus stated that:

> *Well you see in the commission so many departments and we do complement each other for us we are investigators. We investigate cases but we have a forensic department. Forensic department I mean assist in forensically examining all the recovered devices and they give us results and analysis of those things. We also have the legal department who now guide us into the work that we do. I mean because we operate within the ambit of the law ahh they look at our files at the end of our investigation to see if they can prefer charges against the accused or if they Act that is being committed contravenes any of the laws so I mean we have a very good working relationship with some of the departments.* (Participant 1, Cybercrime Investigator, 30/08/16)

This response was repeated by seven (7) of the participants who had worked in the investigations department of their respective organisations. However, a participant from the legal department of an organisation added that their role in investigating cybercrime was more advisory to the other units. The participant argued that:

> *The relationship I would say is basically that of playing an advisory role. Hitherto, prior to this time, we didn't really have enabling laws backing cybercrime so with the establishment, with the coming into law of the Cybercrimes Act, the legal and prosecution department has to go out there, advise those units, the teams saddled with the responsibility of investigating these things in line with the emerging trends, in line with global trends. Bringing out ways, techniques and bringing out the laws guiding these cybercrime offences and explaining the laws, the cybercrimes laws so to say to them.* (Participant 26, Cybercrime Prosecutor, 19/08/16)

This response was repeated four (4) times by all the lawyers and six (6) times by the ICT officers. However, one of the participants from the forensics unit argued that, the forensic

analysis they did in extracting evidence from the digital devices of the cybercriminals was pivotal to any successful investigation and prosecution of cybercrime. The participant thus argued that:

> *Well we are the centre of the investigative activities of the Commission because right now you can handle a circle of fraud or crime without passing through technology. We provide support in the areas of being able to get through technological devices, extracting data, extracting information that would be useful to the investigators. Getting the trail of what actually happened as the use these digital media. So we are centre, we deal with all the departments. ICT is there to provide support; the Operations department bring in the bulk of the cases that we work with. The training academy which is another arm of the Commission, it is one place which we have played a very active role, leverage on the training activities to provide awareness in these regards and basically that's it; we are almost at the centre of everything that is happening* (Participant 7, Forensic Examiner, 11/08/16)

The above mentioned response was similar to what five (5) forensic examiners stated.

External Partnership

About thirty-one (31) of the participants had one form of partnership with an external body or international organisation. According to participant 1, the relationship was necessary due to the transnational nature of cybercrime and how it involved the use of facilities that were regulated by an external body. The participant stated that:

> *Well cybercrime being that it is it is transnational in nature and also there are lots of facilities that are been used in which you would have to work with other external stakeholders. The cybercrime unit we have had a good working relationship. We have collaboration with so many stakeholders most especially the ISPs, the banks* (Participant 1, Cybercrime Investigator, 30/08/16)

Most of the cybercrime perpetrated was linked to the use of internet facilities provided by the ISPs and the loss of money that was stolen online from the banks. All the eight (8) investigators agreed that, the relationship was necessary in order to have a proper investigation done. However, one of participants argued that, the relationship was minimal and only done during training sessions or when other organisations need their expertise in investigating cybercrime. The participant argued that:

> *The relationship with other agencies now is minimal to the best of my knowledge. However, there have been attempts to make sure that this relationship is fostered. There have been joint training sessions which create an atmosphere for agencies, different agencies, law enforcement agencies to cross pollinate ideas, develop professional and informal relationships which enhance investigation of cybercrimes. There is also demand from sister agencies to the Commission to support in terms of investigating cyber related crimes.*(Participant 10, Forensic Examiner, 15/08/16)

This response was coded twice by other interviewees by agreeing that the relationship was based on what help they could offer to the requesting organisation. Also, some of the organisations had regional partnerships with other countries through their regional bloc organisation. For example, one of the participants stated that, their organisation had a partnership with ECOWAS, which is a regional West African body of West African countries. This partnership was due to the transnational nature of cybercrime and how some cybercriminals had left Nigeria to other West African countries that had no cybercrime laws in order to continue to commit their illegal activities. The participant stated that:

> *Particularly the West African region. There were. Because of the enforcement effort that we have been making on these cybercriminals. A lot of them migrated to these West African countries. Now these West African countries like Benin republic are becoming hub of these cybercriminals. If we have these bilateral agreements with all these countries. It would make it a lot easier for us to cooperate and then deal with this scourge.*(Participant 2, Cybercrime Investigator, 11/08/16)

However, most of the participants argued that they had international collaboration with international bodies and organisations such as the EU, UN and FBI. They argued that these relationships were necessary especially when it came to issues of jurisdiction, repatriation of funds and joint operations by different countries. Participant 12 argued that:

> *We have lots of partners when we talk about stakeholders, first and foremost I would want to mention the EU, the European Union, they provide support for the activities of the EFCC; UNODC, United Nations Office of Drugs and Crime, they provide grants for information technology and the development of forensic lab amongst others. The US government through the FBI provide trainings and in short lots of support from them* (Participant 12, Forensic Examiner, 16/08/16)

About twenty (20) members of an organisation mentioned they had an external partnership with international bodies and that it had greatly assisted in the investigation of cybercrime in Nigeria. Participant 3 further argued that these partnerships were very effective and came in the form of:

> *Treaties, multilateral and bilateral treaties and even regional arrangement with countries with tackling criminal cases, it's been very effective so far* (Participant 3, Cybercrime Investigator, 19/08/16)

7.8.7 Theme 7: Benefits of Partnership

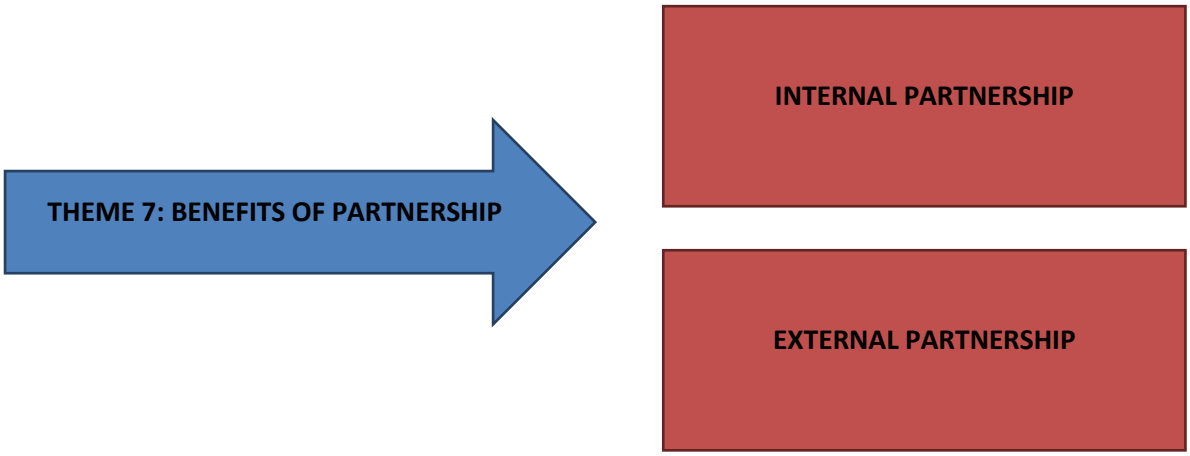
The seventh theme, 'Benefits of Partnership' was based on the role that partnership and collaboration between stakeholders played in addressing the issue of cybercrime. About twenty-three (23) out of the thirty-four (34) participants responded that the partnership was

necessary and was beneficial in the international efforts to tackle cybercrime globally. Two emergent themes were categorised as follows:

1. Internal Partnership
2. External Partnership

The sub-nodes were internal and external partnerships. The benefits of internal partnership with an organisation was analysed within the framework of how different departments collaborated and the benefits and necessity of those partnerships. In contrast, the benefits of external partnership an organisation had to local, national and international bodies were analysed within the scope of understanding how these partnerships benefited the organisations in their efforts to tackle the borderless nature of cyber related offences.

Figure 7.11 shows the theme and the emergent outcomes.



Theme 7.11: Benefits of Partnership& Sub-Themes

Internal Partnership

In analysing the benefits and relevance of partnership within key stakeholders in an organisation, twenty (20) participants agreed that there was one form of partnership with varying degrees of benefits to their organisations. Participant 1 argued that the partnership between forensics and legal department was very relevant and important to a successful investigation and prosecution of cybercrime in Nigeria. The participant stated that:

> *It is very very relevant. Very very relevant in the sense that if you make an arrest and you do investigation, if you recoveries you make you recover items in a scene of crime. I mean the forensic department are the people that would do the forensic analysis of those devices and that would further tell you the kind of criminal group that you are doing with yeah and the legal department too, if you dont prosecute, prosecution is a deterrent, so if you don't*

> *Prosecute so at the need the whole thing would become meaningless, it is very very important.* (Participant 1, Cybercrime Investigator, 30/08/16)

Fourteen (14) interviewees agreed with Participant 1 that there was a need for synergy and understanding between departments that were tasked with the investigation, prosecution and prevention of cybercrime. However, one of the participants from the ICT unit stated that ICT staff should be the ones investigating cybercrime and not investigators. The participant argued that:

> *I think it is very relevant. I think the ICT experts should be the one to be trained to be cybercriminal detectives or operatives.* (Participant 20, ICT Team Lead, 23/08/16)

This argument was supported by another ICT staff member who stated that the partnership was beneficial but not enough because the ICT unit should be the unit investigating cybercrime because of their skill sets and training. The participant stated that:

> *Very relevant but it is not enough. Basically the cybercrime unit of the Commission should if not resident in the department but I think they should have a synergy; I think they should always relate with us on the cybercrime cases.* (Participant 23, ICT Team Lead, 18/08/16)

The participant from the committee that had legislative oversight on cybercrime issues, however, argued that the synergy was not sufficient and most organisations or units within organisations worked at variance with each other. The participant argued that:

> *Well the truth of the matter is that we need to improve on it; there is a need for a synergy even amongst other committees. Apart from the Committee under me, there are other committees and agencies that are also protecting our cyber-space. But the truth of the matter is that there is no Synergy amongst all of them so we need to work out a situation where there would be a synergy and NSA that is in charge would be able to have access and control 3 or the 4 and 5 security agencies. But at the moment everybody works in variance, that is one of the roles my Committee is trying to play and that is the reason that we are even trying to call for the national conference that its coming very soon and it's on Cybercrime and Cyber-Attack.* (Participant 30, Senator, ICT & Cybercrime, 31/05/17)

Another participant spoke about the importance of the partnership through training as it helped in building cyber resilience within the staff of an organisation. The participant argued that:

> *Yes because when you are talking about cybercrime you are talking about cyber-resilience as well for the organisation. If people have training and awareness; if they have that awareness they are going to be more resilient so if there is an attack from criminality by organised crime….they staffs are going to be more empowered to recognise those threats and it increases our security levels. Also they are more likely to empower and pass on those protective preventive measures to members of the public.* (Participant 34, Cybercrime Investigator, 18/12/17)

External Partnership

In analysing the benefits of external partnerships with other local, national and international organisations, twenty (20) participants argued that there were some benefits in collaborations. However, not all the participants agreed on how beneficial the partnership was to their respective organisations. For example, Participant 21 argued that the partnership was beneficial as the sharing of information was key to a successful investigation of cybercrime. Participant 21 stated that:

> *Yes it is. Like I said earlier considering the nature of cybercrime, it is borderless so you would always need the help of external stakeholders when conducting cybercrime offences. They provide information which is necessary in the conclusion of cybercrime cases.* (Participant 21, ICT Team Lead, 30/08/16)

Fourteen (14) participants argued that there was a need to share information and synergise because of the borderless nature of cybercrime and, by sharing information with other stakeholders, it had made it easier to investigate cybercrime. However, participant 23 argued that the external partnership was not yielding any different results by stating that:

> *Honestly I don't think there are anything they are putting in place, it's just the existing things we have; nothing new is being implemented; even if it is honestly I am not aware of.*(Participant 23, ICT Team Lead, 18/08/16)

Participant 20 stated that there was a need to share more information because the synergy in place between organizations' needed to be strengthened through more collaboration in tackling cybercrime. The participant also argued about the need to have more training and support from external stakeholders in order to investigate cybercrime better.

> *That's a tricky question for me, but I think its ok but I think we can get more. Basically it is the collaboration, we could do more, we need financial support, we need more information, we need more, and basically we need to know more about the trends in cybercrime. For me I think we need to know more about the trends to be able to fight it and in fighting it we need more support from the external stakeholders.* (Participant 20, ICT Team Lead, 23/08/16)

7.8.8 Theme 8: Measures and Benefits of Measures

The eighth theme, 'Measure and Benefits of Measures', was analysed within the scope of what measures the organisations were using in tackling the issue of cybercrime. Also, participants were asked how beneficial the measures were in tackling cybercrime. Thirty-two (32) responded by mentioning different measures and approaches they were using to mitigate the activities of cybercriminals. Also, the benefits of the measures were analysed in order to

understand how suitable the measures were in tackling cybercrime. Eight (8) sub-themes emerged from the main themes. The emergent themes are:

1. Awareness Campaigns
2. Best Practices
3. Enforcement
4. Funding & Logistics
5. Partnership
6. Training and Manpower
7. Benefits of Measure

Figure 7.11 shows the theme and the emergent outcomes.

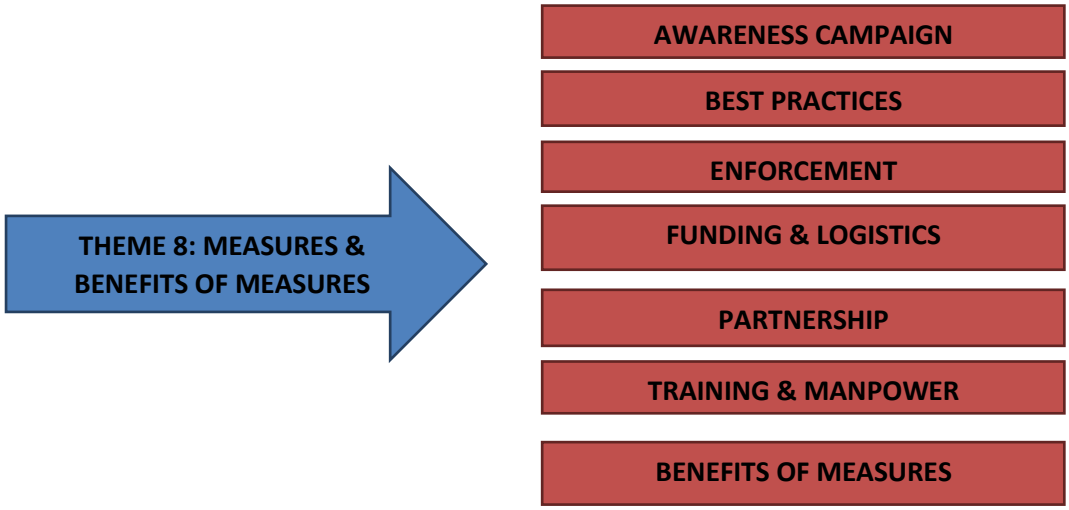


Figure 7.12: Theme 8: Measures, Benefits of Measures & Sub-Themes

Awareness Campaign

Fourteen (14) participants stated that raising awareness of the general public about the dangers of cybercrime was one of the measures they were using to tackle the activities of cybercriminals. Participant 27 argued that:

> *The measures that are being taken right now in order to address the issue of cybercrime in Nigeria primarily are on awareness, sensitization campaign, re-orientation. Nigerians need to know more on how those internet fraudsters operate.* (Participant 27, Cybercrime Prosecutor, 17/08/16)

Another participant argued that, they not only enlightened the public but also tried to inform them about the trends of cybercrime and how to avoid being a victim. Participant 6 stated that:

> *Right now we are being more proactive by enlightenment through the media section. So we try to tell the public the current and mode of techniques the hackers and fraudsters are using now and also we try to be proactive so anytime we get any alert of any scam, we swing into action.* (Participant 6, Cybercrime Investigator, 19/08/16)

This response was repeated nine (9) times by the participant that mentioned using awareness campaigns to sensitise the general public. Also, participant 15 stated that the organisation used the social media outlets to reach out more to the general public. The participant stated that:

> *Basically, it is educating them; we tend to talk to them a lot. We talk to them both verbally and non-verbally. We talk to them online, we put lots of adverts, and we have cartoons. We put cartoons showing them the ills of corruption or how cybercrime is being done and when they see something they would know that it is actually a fraudulent transaction or it is a shaky one, they shouldn't fall into it.* (Participant 15, Media Team Lead, 11/08/16)

Best Practices

Only one participant from the forensics unit stated that the measures they were using to curtail the activities of cybercrime was by adhering to international best practices in retrieving evidence from digital devices which was vital for a successful investigation of cybercrime. The participant stated that:

> *We adhere to the international best practice such as ACPO guideline, we ensure that we maintain the integrity of every evidence we are working on. Chain of custody, we ensure that we properly establish a chain of custody and we don't temper with the integrity of any evidence because this evidence has to be presented in the court of law the way it is.* (Participant 11, Forensic Examiner, 16/08/16).

Enforcement

The enforcement of cybercrime laws and other laws that criminalised the illegal use of computers to commit crime was one of the measures used by seven (7) participants in deterring criminals in committing crime. Participant 25, a lawyer with one of the organisations argued that:

> *We are enforcing the provision of the law, enforcing the provision of the Cybercrimes Prevention and Prohibition Act 2015.* (Participant 25, Cybercrime Prosecutor, 17/08/16)

The Cybercrime Act 2015 was an important legal instrument that when properly enforced would assist in addressing the activities of cybercriminals. However, another participant argued that by opening up more offices and having a dedicated forensic unit in each of these new offices, it had reduced the backlog of cases. The participant stated that:

> *We have been able to open offices in the 5 geopolitical zone including the headquarters which is the sixth one; forensic units have been created and personnel are manning them so the*

> *work load has reduced so it's more on those units in the zones.* (Participant 12, Forensic Examiner, 16/08/16)

However, another participant stated that, the organisation conducted cyber-raids on internet cafes that were being used to commit cybercrime offences even though the use of them had greatly reduced due to people using their mobile devices to commit such crimes. The participant argued that:

> *We do cyber raid but now it is a little bit difficult to do cyber-raids because most people have gadgets that they use unlike those days that you go to cyber-cafes and those days you go to cyber cafes and you raid them.* (Participant 6, Cybercrime Investigator, 19/08/16)

Funding and Logistics

The provision of funds and tools to conduct proper cybercrime investigation was a measure used for the successful investigation of cybercriminals. Three (3) interviewees stated that funding and logistical support of tools was a major way they were able to counter the activities of cybercrime. One of the participants stated that:

> *We do some intelligence, social media. We try to source information from social media because some of these fraudsters and trace emails as well. We are using of email and domain tracing tools to help us as well.* (Participant 4, Cybercrime Investigator, 18/08/16)

The participant commented on the importance of using software tools for investigation. Also, participant 9 argued that the use of these modern tools made the investigation timespan short and the analysis of the evidence even better. The participant argued that:

> *Well as I earlier said, this commission, this unit rather, the Forensic Accounting unit is a modern unit that use modern tools in its investigations so we are able to introduce new software's of doing very vibrant analysis that would take you before now would take you two days to do, would take you 5, 10 minutes you are done with your analysis and you connect the dots by using these technologies. It has been helping really.* (Participant 9, Forensic Examiner, 16/08/16)

Partnership

The partnership between organisations in investigating cybercrime was one of the measures used in tackling cybercrime. Seven (7) interviewees agreed that, having partnerships with relevant stakeholders had been beneficial in investigating cybercrime. The participant argued that:

> *The cybercrime unit has been holding a lot of meetings with different agencies like Microsoft. Recently we had some people from Facebook that were here to enlighten us on new trends of the offences that are being conducted through Facebook. Some like Facebook lottery. And some other agencies too.* (Participant 21, ICT Team Lead, 30/08/16)

Another participant made similar arguments by stating that due to the global nature of cybercrime, they collaborated with key stakeholders in proffering solutions to tackle cybercrime. The participant argued that:

> *Some of these measures is collaboration, intra and inter agency cooperation, we reach out to other stakeholders, other sister LEAs, and we robe minds, ideas, we strategize ways to forge ahead and we come back to the Commission and we table these before the Commission and then make them key in to the global fight against cybercrime.* (Participant 26, Cybercrime Prosecution, 19/08/16)

Training and Manpower

The training of staff and the recruitment of new staff was identified as one of the measures being undertaken to address cybercrime in Nigeria. These sub-themes were coded eight (8) times by different participants from different organisations. According to participant 10:

> *The Commission is making attempts to train more and more officers because the demand for digital forensic which provides digital evidence from cybercrime is huge. So the commission is currently training more and more people to increase the human capacity in investigating cybercrime. There is also an attempt to educate more and more officers on issues relating to cybercrime as well as also most judges are not well acquainted with cyber related crimes since they are intangible crimes so to speak, so the commission is making attempt to make sure more and more legal officers are educated.*(Participant 10, Forensic Examiner, 15/08/16)

Participants 10's argument was centred on the training of staff in digital forensics and the education of judges to be able to understand cyber related crimes. Also, another participant argued that because of their experience in retrieving evidence from digital devices, they acted as training facilitators in educating staff from other departments and other organisations as well. The participant argued that:

> *Well in the course of analysing digital devices, in the course of management of crime scenes. We get to pick up a lot of lessons and we share that we the investigators primarily through the avenues of training. So periodically we provide training for the operatives of the Commission, we also are actively involved as facilitators in the trainings that go on at the academy and these trainings goes beyond the training of EFCCs personnel's to even personnel's from other agencies.* (Participant 7, Forensic Examiner, 11/08/16)

Benefits of Measures

The benefits of the measures used in tackling cybercrime varied from participant to participant. While some argued that it was effective, others said they could not know the benefits of the measures. However, in general thirty-two (32) responded stating that there was some form of benefit in deploying certain measures to investigate cybercrime. One of the participants argued that having more offices and more staff across the country had made the workload less, thus, reducing delays in investigating cybercrime. The participant argued that:

> *It has been successful to a limit because the workloads of headquarters has reduced and cases coming from there no longer take a longer time unlike before that it is based on first come, first serve, you would have to take your time before you do them. But now because of the outlets, they don't bring the cases to the headquarters again. They give it to these outlets and to a large extent, raids are being carried out in these different outlets unlike before it takes a very long time before you start thinking of going to these places to carry out raid, you understand. Its time wasting and the logistics involved and what have you.*(Participant 12, Forensic Examiner, 16/08/16)

However, another participant from the Media department argued that they would not be able to know how beneficial the measures were until they got feedback from the public. The participant stated that:

> *Well we have just started so we wouldn't be able to access how successful they are until we get feedback from the communities.* (Participant 13, Media Unit Head, 24/08/16)

Also, one of the participants, argued that no matter what measures were used against the cybercriminals, it was very difficult to keep up with the criminals because of the evolution of ICT. The participant argued that:

> *So far so good there have been a few convictions but I think with the trend of IT being very fast and rapid and even the cybercrime being fast, then we need to buckle and do a lot more to be able to be at the same level with the cybercriminals.* (Participant 20, ICT Team Lead, 23/08/16)

Another participant argued that partnership with relevant stakeholders outside their organisation was helping in investigation and prosecution of cybercrime. The participant argued that:

> *Partnering with stakeholders like Microsoft and other organizations has really helped in conducting our investigations and prosecutions in court of law.* (Participant 21, ICT Team Lead, 30/08/16)

7.8.9 Theme 9: Laws

The ninth theme, 'Laws' was analysed within the scope understanding how adequate the laws were in investigating and prosecuting cybercrime. Nineteen (19) interviewees responded differently to how adequate the laws were in tackling cybercrime. Three (3) sub themes emerged from the ninth theme. The emergent themes are:

1. Amendment of Laws
2. Enforcement of Laws
3. Laws are Adequate

Figure 7.13 shows the theme and the emergent outcomes.

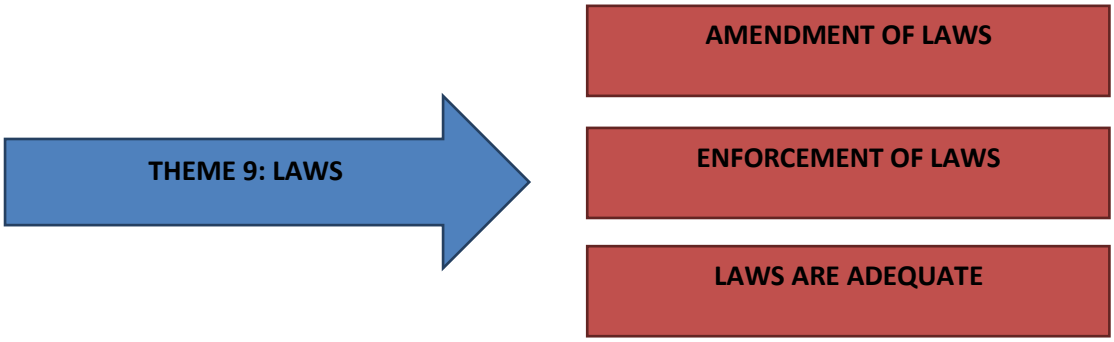


Figure 7.13: Theme 9: Laws & Sub-Themes

Amendment of Laws

This theme emerged from the response of five (5) interviewees who argued that, there was a need to amend some part of the cybercrime laws as it was not adequate for prosecuting cybercriminals in court. Participant 26 argued that:

> *I wouldn't say they are adequate, like I told you the enabling laws were very weak before, we didn't even have laws and the activities of these cybercrime offenders were affecting the country negatively and then the stakeholders sat and said what was the way forward? As a result of that, we now have the main and the substantive Act which was just passed year. As it is now, we just one or one and the half laws.* (Participant 26, Cybercrime Prosecution, 19/08/16)

However, participant 32 further argued that even with the new Cybercrime Act, there was still a need for amendments in order to make the law dynamic in tackling the menace of cybercrime, Participant 32 stated that:

> *I have attended a number of forums where calls for amendment are already coming up. There are issues like I said that are being put to use, they are already calling for amendments to various sections so there are inadequacies being pin pointed in the cybercrimes Act and like I said it has to be into use before we can start talking about amendment; it has to be a dynamic document anyway and a provision in it has a council, the Cybercrime Advisory Council which is actually charged with details of the implementation of the Act itself and as I speak with you the Council is still meeting.* (Participant 32, Telecoms Regulator, 13/06/17)

This response was repeated by a member of parliament who argued that a national conference on cybercrime had been organised to address issues within the cybercrime laws. The participant further argued that from the input of the Ministries, Departments and Agencies, the parliament would be able to know what part of the laws to amend. Participant 30 argued that:

> *The National Conference we would be able to gather what is called information and the thinking of the MDAs harnessed it together and it would help us in forming a policy and it*

> *would assist us in the amendment of the laws we are trying to do.* (Participant 30, Senator, ICT & Cybercrime, 31/05/17)

Enforcement of Laws

The enforcement of laws used in prosecuting cybercriminals is one of the emergent themes of the ninth theme. Nine (9) participants argued that the current cybercrime laws were adequate but there was a need to enforce the laws in curtailing the activities of cybercriminals. Participant 13 argued that, there was a need to enforce the law and make relevant stakeholders aware of the laws. The participant stated that:

> *They laws are there but it is the enforcement that is the problem. And then also if you look at the laws especially the current Cybercrimes Act, people don't know anything about it. There is lack of information about all these Acts. That or the Acts or the laws that are being used to address the issue of cybercrime in Nigeria.* (Participant 13, Media Unit Head, 24/08/16)

Also, participant 24 stated a similar response to participant 13 about enforcing the laws. The participant stated that:

> *I don't have problems with laws more to speak, my problem is enforcement of the laws. Because the laws can be there but they are not enforced and until you begin to work with the laws, you may not know that they have issues.* (Participant 24, Cybercrime Prosecution, 18/08/16)

However, participant 21 argued that the laws need to be implemented while judges and law enforcement officials should be adequately trained in enforcing the law. The participant stated that the law:

> *Is very effective but another issue is implementation. Now you have to talk about issues of training judges, LEAs. So it would take time but the laws are quite effective and they are very strict. So I believe if they are properly implemented, they would go a long way limiting the number of cybercrime offences that are committed in Nigeria.* (Participant 21, ICT Team Lead, 30/08/16)

Laws are Adequate

Seven (7) interviewees argued that the cybercrime laws were adequate in investigating and prosecuting cybercrime in their respective jurisdiction. Participant 33 from the UK argued that the laws used were inadequate in sentencing criminals but now the laws were better. The participant stated that:

> *They are getting better. We now have longer sentences because personally in my opinion the sentences were quite inadequate for some of the crimes taking place and you know they are at the adequate I would say.* (Participant 33, Cybercrime Investigator, 16/11/17)

Participant 1, argued similarly with participant 33 by stating that:

> *I think the current laws are adequate. We have the Cybercrime law now which was just in 2015. We have the Advance Fee Fraud Act even though it's not cyber as in but there are some sections which even proscribes some of these offences. So to me for now I think the laws are adequate.* (Participant 1, Cybercrime Investigator, 30/08/16)

However, participant 2 argued that the laws were adequate but there was a misapplication of the laws towards freedom of speech. Participant 2 stated that:

> *They current laws are adequate in curtailing cybercrime. And now my biggest challenge now is that the misapplication of some of these. Look at this issue of cyber stalking and the way it's like the office wants to apply it to gag media* (Participant 2, Cybercrime Investigator, 11/08/16)

7.8.10 Theme 10: Challenges

The tenth theme, 'challenges', was analysed within the scope of understanding what current challenges the relevant stakeholders were facing in tackling cybercrime. Five (5) sub themes emerged from the main theme. The emergent themes are:

1. Bureaucracy
2. Inadequate Funding and Tools
3. Laws and Jurisdiction
4. Technology
5. Inadequate Training and Education

Figure 7.14 shows the theme and the emergent outcomes.

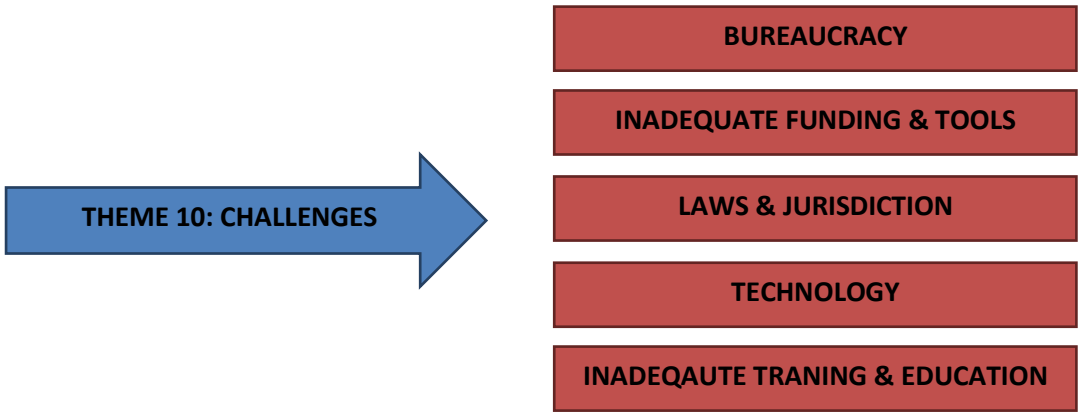


Figure 7.14: Theme 10: Challenges & Sub-Themes

Bureaucracy

The sub-theme of 'bureaucracy' emerged from the responses of five (5) interviewees. The bureaucratic bottlenecks within an organisation, according to Participant 32 were a major challenge in addressing the issue of cybercrime. The participant argued that:

> *The major challenge like I mentioned to you beginning is some kind of bureaucracy that you would always have to go through and for us what I realise even the communication challenge that you have to go through the ngCERT is a challenge and that is what like I have said the National Policy has put in place.* (Participant 32, Telecoms Regulator, 13/06/17)

Another participant argued that the challenge was not merely in dealing with internal stakeholders but also with external stakeholders such as large IT firms such as Google that did not give the relevant information needed by law enforcement agencies in investigating cybercrime. Participant 7 argued that:

> *The challenge in having to deal with the big companies, the big operators like the Googles, the Yahoos and all of these companies that provide platform for these people to operate; it's a big issue. I know from experience that dealing with Google is not easy; trying to get out information from Google and other big IT companies is not easy. So that's also a major constraint, it's a challenge to dealing in addressing the issue of cybercrime in Nigeria.* (Participant 7, Forensic Examiner, 11/08/16)

Participant 3 also complained that:

> *Basically, obviously we have issues of coordination and delays in the Ministry of Justice also hinder our work to a certain extent and manpower.* (Participant 3, Cybercrime Investigator, 19/08/16)

Inadequate Funding and Tools

The emergent theme of 'inadequate funding and tools' was a major challenge to tackling cybercrime and was argued by twelve (12) interviewees. One of the participants stated that, they were unable to sustain a rigorous public awareness campaign because of inadequate funding and tools. Participant 14 argued that:

> *Going by the empowerment we receive from Section 6 subsection p, I would read again, "carrying out and sustaining a rigorous", if we look at these two words, "sustaining", "rigorous", not just carrying out public relations activities. So you know discover that there is need for capital, there is need for resources to be able to carry out and sustain rigorous public enlightenment. Because if you look at Nigeria for instance, the population, the geography and culture of the people. You cannot use one message to reach to your vast messages, you need various messages.* (Participant 14, Media Team Lead, 12/08/16)

Participant 6 mentioned how the current tools they were using in the cybercrime lab were outdated and needed to be updated and replaced by more modern tools. The participant stated that:

> *Some of the challenges we have basically are equipment's but we try to use and manage the little we have. In the cybercrime lab we have it is not as modern as what is being obtainable now.* (Participant 6, Cybercrime Investigator, 19/08/16)

However, participant 16 argued that there was a need for more funding to procure vehicles to

transport officers to various locations for sensitisation campaigns and also, there was a need to pay allowances to staff to carry out their duties. Thus, participant 16 stated that:

> *Funding. When I say funding it covers a lot. For instance now there is a need for vehicular equipment, there is need for sensitization equipment's; Information Disseminating equipment. There is a need for vehicles, there is need for more computers, and there is need for even allowances for staff who have been assigned* (Participant 16, Media Team Lead, 25/08/16)

Laws and Jurisdiction

The different laws and jurisdiction involved in carrying out a proper cybercrime investigation was mentioned as a major challenge in tackling cybercriminals. Due to the transnational nature of cybercrime offences, differences in laws between countries could be a hindrance in cooperation between countries. Seven (7) participants stated that laws and jurisdiction was a major challenge in investigating cybercrime. Therefore, participant 1 argued that:

> *Some of the challenges that we do have, being that it is transnational in nature sometimes you would tend to have cases that we might need to reach out to other countries and other countries might not be cooperative. This is one. Secondly again you may have, that's jurisdictional issues*(Participant 1, Cybercrime Investigator, 30/08/16)

Also, another participant argued similarly to participant 1 by stating that cooperation and collaboration between law enforcement agencies in different countries was very challenging. The participant argued that:

> *This crime is not local, this crime have international dimension so there needs to be an active cooperation and collaboration between law enforcement agencies across different jurisdictions that's one key point and I think for now that is not there. If it's there it is still at a very minimal level; if I am investigating a breach in a Nigerian bank and money was moved to somewhere in eastern Europe, I should be able to reach out to a partner law enforcement agency in eastern Europe and say well, these are time bound, you need to move with speed also.* (Participant 7, Forensic Examiner, 11/08/16)

Technology

The evolution of technology and the adoption of new technology to commit cybercrime by the criminals was a major challenge for stakeholders responsible for either preventing, investigating or prosecuting cybercrime. Also, some of the investigators needed to update their technical skills and embrace the use of technology at a faster pace in investigating some of these computer related offences. Six (6) participants agreed that technology was a major challenge in addressing the issue of cybercrime. Participant 1 argued that:

> *Technology is growing at the speed in which it's going, it's going at a very high speed. We need to be up to date with the kind of things that are happening so the need to have dedicated*

> *and up to date skills and in tackling these kind of things.* (Participant 1, Cybercrime Investigator, 30/08/16)

Another participant stated that, the criminals were always a step ahead of law enforcement officers. Participant 17 mentioned that:

> *The challenges we are facing basically I think is that there always someone a step ahead, even though we normally and they are almost naturally going to make mistakes, we always catch them eventually but then I think the biggest challenge is that they are sometimes a step ahead because they have time while we are doing a lot of things.* (Participant 17, Media Team Lead, 16/08/16)

However, participant 33 argued that, affordability of storage devices made the forensic analysis of digital evidence more difficult and longer. The participant stated that:

> *From a forensic point of view is the amount of storage that people can have now. That the cost of storage is coming down now so we can see terabytes of data and it takes longer to process the data and to go through that it takes longer and longer and physically the amount of storage that we have to go through and we have shorter and shorter time now to deal with that because the procedures have changed* (Participant 33, Cybercrime Investigator, 16/11/17)

Inadequate Training and Education

Inadequate training on the part of the staff and lack of education on the part of the public were considered as major challenges, according to fourteen (14) participants that participated in this research. According to participant 19,

> *Lack of proper manpower because ICT is always changing, there are always new things. There is a certain level of training and re-training that has to take place, information dissemination and all those things are not readily available. The infrastructure in place sometimes is a bit outdated. Some of the softwares we are using, we have licensing issues. So all these things they make things very hard.* (Participant 19, ICT Team Lead, 11/08/16)

Also, participant 2 argued that even with the tools, most of the investigators lacked basic ICT knowledge in investigating cybercrime. According to participant 2,

> *Most of our investigators don't have the IT they need in order to investigate these cases. To investigate basically a cybercrime, first of all you have to be grounded in IT and many a times our investigators our investigators find it a bit and to be grounded in IT knowledge one has be make a lot of sacrifices to pursue knowledge on your own.* (Participant 2, Cybercrime Investigator, 11/08/16)

Another participant argued that even the judges and lawyers did not understand the basic terminologies in the Cybercrimes Act and that they should be trained as well. Participant 21 stated that:

> *Another issue is when you take these cases to the court, the judges and the lawyers too are not aware of some of these terminologies and some of the things of what you consider as evidence or cybercrime offences.* (Participant 21, Cybercrime Prosecutor, 30/08/16)

Participant 28, a cybercrime prosecutor also agreed with participant 21 that the judges needed to be fully aware of some of the basic cybercrime terms before they could begin to prosecute those criminals brought before them in a court. Participant 28 argued that:

> *I would say the awareness of the judiciary because the problem is that the judiciary are not so grasped in the issue of cybercrime. The nitty gritty of prosecuting or appreciate what we are trying to say in court in the sense of going to court and trying to prosecute this offences, they can't understand.* (Participant 28. Cybercrime Prosecutor, 19/08/16)

7.8.11. Theme 11: Recommendations

The eleventh theme, 'recommendation', was analysed after all the thirty-four (34) participants were asked, what recommendation they would suggest to tackle the challenges mentioned in theme 10. Five (5) sub themes emerged from the main theme. The emergent themes are:

1. Education and Awareness
2. Funding and Tools
3. Laws and Policy
4. Partnership
5. Training

Figure 7.15 shows the theme and the emergent outcomes.

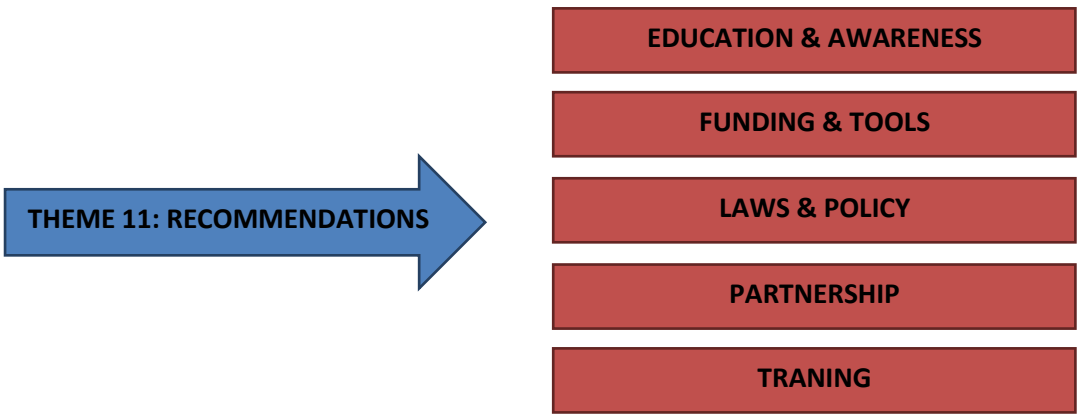


Figure7.15: Theme 11: Recommendations & Sub-Themes

Education and Awareness

Fifteen (15) participants argued that education and awareness of the public about cybercrime was one of the many ways to address the issue of cybercrime. Participant 10 argued that:

> *Recommendation is that each organization should realise that cybercrime, it's about the highest paid crime in the world and that should attract global attention. In a sense that agencies also should channel more of their resources into fighting crime. There is also the need to create awareness. A lot of people are still uneducated or unaware of cybercrime. So I think that some of the resources both NGOs, government agencies and ours should involve in advocacy, creating awareness, intimating people on cyber related crimes.* (Participant 10, Forensic Examiner, 15/08/16)

Furthermore, participant 13 argued that arrest and prosecution of the criminals would not solve the problem and that there was a need to increase awareness amongst the general populace. Participant 13 argued that:

> *It is not enough to go and start arresting people fah. Arrest would not work. It is creating awareness; they must explore all the platforms of advocacy, of public enlightenment, of ofahh creating of education, of civic public education to be able to address this issue of cybercrime. Arrest, prosecution would not solve the problem, it would only compound it.* (Participant 13, Media Unit Head, 24/08/16)

According to participant 22, the awareness should include our friends and family members because some people thought that there was nothing wrong in committing cybercrime. The participant stated that:

> *We need more public awareness because some people don't even know what crime is so we need acceptability from the public. We need a system that would reward whistle blower because we cannot do it alone and we need to educate our family and our friends so that we would be keeper of your next door neighbour just as it is done in the Britain.* (Participant 22, ICT Team Lead, 17/08/16)

Funding and Tools

Ten (10) participants argued that increased funding and provision of tools and equipment was one of the recommendations that should be embraced by relevant stakeholders. According to participant 21, the provision of these tools would assist law enforcement officers in being proactive rather than reactive in handling cybercrime cases. The participant argued that,

> *Commission has to provide equipment. What we should be having is a situation where we should be able monitor calls, emails and conversation between people so that we would ahead of these criminals because mostly what we do here is a reactive approach which is not proactive at all. Mostly the offences are been committed and most cases the offenders have gone with the Money or probably spending the loot.* (Participant 21, ICT Team Lead, 30/08/16)

Also, participant 6 mentioned the type of equipment needed such as:

> *Basic equipments like tracking device, access to network providers database at any given time without recourse to writing formal letters, then logistics.* (Participant 6, Cybercrime Investigator, 19/08/16)

In contrast, participant 12 argued that the internet services needs to be upgraded and the provision of high processing computers would assist in the analysis of digitally retrieved data. Participant 12 stated that:

> *Then the upgrade the internet service, we need high processing computers because the computers we have sometimes most times tend to crash because of the workload.* (Participant 12, Forensic Examiner, 16/08/16)

Laws and Policy

The response of ten (10) interviewees showed that there was a need to strengthen the existing laws and also create sound policies that would assist relevant stakeholders in tackling the issue of cybercrime. Participant 12 stated that the forensic lab should be autonomous and independent of any organisation. The participant argued that:

> *Autonomy of the forensic lab, what I mean is, the forensic lab should not be in the EFCC, because it is a problem for us when we go to court is like we take our instructions from other units, it's like they are telling us the evidences, they are telling us to implant evidences, it's like we are not giving them what we have in the device, we are planting them rather. So it would be good if the lab is autonomous, not in an organization.* (Participant 12, Forensic Examiner, 16/08/16)

However, participant 23, stated that the policies needed to be towards creating greater awareness. The participant stated that:

> *And from the government side there should be laws put in place and policies; formulate policies; there is not much awareness on cybercrime and cybercrime security.* (Participant 23, ICT Team Lead, 18/08/16)

Furthermore, participant 10 stated that some of the laws needed to be reviewed in order to reflect the current realities of cybercrime. According to participant 10:

> *I think that the cybercrime law in Nigeria has got some issues which need to be reviewed and adjusted to fit into the current realities at the moment.* (Participant 10, Forensic Examiner, 15/08/16)

Partnership

According to sixteen (16) interviewees, the use of partnerships and collaborations between the government, private sector and international organisations needed to be implemented. Participant 10 argued that:

> *Commission should also collaborate with private agencies in cybercrime so that there would be this synergy with government and the private sector. I believe that if these things are implemented there would go a long way in tackling cybercrime.* (Participant 10, Forensic Examiner, 15/08/16)

Also, participant 20 argued that greater collaboration between the private sector and external stakeholders should take place to improve the information sharing mechanism between stakeholders. Participant 20 argued that:

> *I would say collaboration particularly with the private and external stakeholders; to proactively identify future or features communication technologies which are liable to criminal exploitation and also we need to able to harness the intelligence of network and information security stakeholders for effective and timely response*. (Participant 20, ICT Team Lead, 23/08/16)

However, participant 30 argued that in order to have a proper partnership between stakeholders, the ONSA should coordinate all activities of MDAs. Participant 30, thus argued that:

> *Coordination and everybody should agree that the Commander in Chief of Cybercrime Security is the NSA. NSA should have a department where these other agencies can report to him.* (Participant 30, Senator, ICT & Cybercrime, 31/05/17)

Training

According to nineteen (19) interviewees, training of staff of relevant stakeholders was the most important suggestion in the fight against cybercrime. Participant 16 argued that:

> *There is need for the Commission to specifically train special officers in the fight against cybercrime. Right in the Commission has thankfully a department dedicated solely to cybercrime. We now have a cybercrime unit in operations that is targeted in fighting or investigating purely cybercrime cases. So there is a need for the Commission to train these guys to the teeth because in fighting cybercrime is not an area for the novice.*(Participant 16, Media Team Lead, 25/08/16)

Another participant further argued that the investigators needed to be properly trained to investigate cybercrime before the prosecutors could file legal charges against the criminals. The participant argued that:

> *The recommendation I would suggest is not from the legal because the legal and prosecution department is the end unit; from the investigative stage, the investigators need to be trained and retrained especially as it has to do with investigating cybercrime* (Participant 26, Cybercrime Prosecutor, 19/08/16)

7.9 Conclusion

In conclusion, the chapter presents the research participants and discusses the function of the interviewer and how the interviews were administered. The chapter further explains the interview transcription and thematic analysis processes. Also, the coding of the interview data for thematic analysis is discussed in detail and an overview of the demographic of the interview findings are elaborated. Finally, the chapter presents all the research findings based on the literature review themes and emergent themes that were found during the thematic analysis process.

CHAPTER 8: DISCUSSION

8.1 Introduction

This chapter presents a detailed discussion of the qualitative findings in relation to the literature. This research study was undertaken with the aim of identifying any improvements required in the international efforts to tackle cybercrime within the scope of law enforcement agencies in the UK and Nigeria. In order to achieve the aim of the study, a qualitative research method was adopted. Data was collected from relevant stakeholders LEAs, Telecoms Regulator, ICT Regulators, Parliament and the ONSA.

This research was guided by a number of research objectives and the findings from the qualitative research. The quantitative study explored the different roles members of the Cybercrime Advisory Council play in tackling cybercrime in Nigeria. It highlighted the different definitions of cybercrime and the form of cybercrime that is most prevalent in Nigeria. It also identified the causes of cybercrime and how stakeholders both within organisations and outside are collaborating in order to tackle cybercrime. Additionally, it explored the measures used by LEAs and relevant stakeholders in addressing cybercrime. Finally, it identified the challenges faced by LEAs and relevant stakeholders and also examined the improvements required to tackle cybercrime.

This discussion is divided based on the research questions with a focus on different aspects of the phenomenon under investigation. These research questions are restated in the following section (8.2).

As mentioned earlier in chapters 1 & 3, previous studies have focused on different aspects of causes and effects of cybercrime in Nigeria (Hassan et al., 2012; Adesina, 2017); laws penalising the misuse of computers (Olusola et. al., 2013b; Saulawa& Abubakar, 2014) have mainly focused on financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et. al., 2012). Even though some studies have attempted to explore cybercrime from the perspective LEAs in UAE and Jordan (Maghairah, 2009; Alkaabi, 2010), none has been comprehensively conducted from the perspectives of LEAs and stakeholders in Nigeria. This study has attempted to understand cybercrime from the perspectives of LEAs and relevant stakeholders in order to provide a more holistic and richer narrative to enable an understanding of what challenges are limiting their investigations and how they can improve in order to tackle cybercrime globally.

This chapter discusses the major findings from the data analysis carried out in Chapter 7. Results suggest that the EFCC, NITDA, NCC, ONSA and Parliament in Nigeria face some form of challenges in tackling cybercrime as discussed by Walls (2007) in his study of the role of the public police. The results also show that poverty is a major cause of cybercrime in Nigeria confirming the earlier findings of Adesina (2017). However, some of the stakeholders did have some partnerships and collaboration in tackling cybercrime, even though there is still a need to develop a more holistic approach to tackling cybercrime.

8.2 Research Question

The aim of this research was to identify any improvements required in the international effort to tackle cybercrime globally within the scope of LEAs in the UK and Nigeria. In order to achieve this aim, the researcher addressed the research questions from the perspective of Routine Activity Theory. The reasons for using RAT have been explained within the theoretical framework in Chapter 4.

The chapter highlights the similarities and contradictions between the research findings (Chapter 7) and the literature review (Chapter 3). The structure of this chapter is based on the research questions which were:

1. How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?
2. Are Law Enforcement Agencies in Nigeria capable guardians in tackling cybercrime and explored in relation to Routine Activity Theory?
3. To what extent are the current laws adequate in investigating cybercrime in Nigeria?
4. How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?
5. What improvements are needed in the International efforts in tackling cybercrime globally?

8.3 Research Question Analysis

8.3.1. Research Question 1

How are the causes of cybercrime motivating people to commit cybercrime and explored in relation to Routine Activity Theory?

In order to discuss how the causes of how cybercrimes opportunities are motivating offenders to commit crime, it is important to separate and discuss two components of RAT namely the suitability of a target and a motivated offender.

8.3.1.1: Part One: Suitable Target

The suitability of a target is discussed from the viewpoint of understanding the main causes of cybercrime in the findings of the research. Figure 8.1 shows the causes of cybercrime in relation to suitability of target

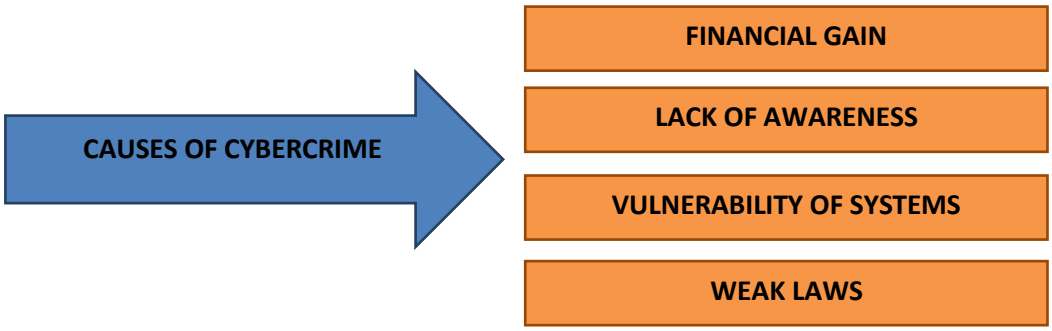


Figure 8.1: Causes of Cybercrime (Suitability of Target)

Figure 8.1 shows four emergent themes from theme 5 in Chapter 7 (Data Analysis). The four emergent themes were financial gain; lack of awareness; vulnerability of systems and weak laws. These are discussed further vis a vis the suitability of targets. These four factors constitute humans or otherwise suitable targets. Each of these factors are discussed further in relation to the research question.

Vulnerability of Systems

As shown in the findings of the research, some of the participants argued that the vulnerability of ICT systems and the internet has made it a suitable target for cybercriminals. Also, some of the participants argued that the 'availability and affordability of the internet' has given criminals the tools and means to commit their criminal activities. This argument aligns the UNODC (2013) which argued that as internet penetration continued to increase in developing countries, the number of targets and offenders also increased daily. Also, it would be very difficult to estimate how many users on the internet are using it for illegal activities. These findings also support Cohen and Felson (1979) RAT assertion that for crime to take place, three requirements must be present namely: a motivated offender, a suitable target and the absence of a capable guardian. The findings also align to the argument by Yar (2005) that targets were more visible and prone to an attack in the public domain such as on the internet.

Furthermore, some of the findings revealed that the financial sector and e-commerce platforms were more vulnerable to criminals. This finding is consonant with the argument by ITU (2012) that existing ICT infrastructure had known weaknesses that could be exploited by an offender. Table 8.1 summarises the findings in the current research, literature review and Routine Activity Theory.

The Current Research	Literature	Routine Activity Theory
Vulnerability of systems was repeated four times as a cause of cybercrime	• Reliance on ICT makes people vulnerable (UNODC, 2013). • Internet usage and penetration on the increase (UNODC, 2013) • Criminals embracing ICT (Yar, 2005; Wall, 2005)	Suitability of vulnerable targets online makes a motivated offender likely to commit crime
New Insight: Vulnerability of systems is a cause of cybercrime. This adds to existing literature and supports routine activity theory		

Table 8.1: Summary of Vulnerability of Systems findings and literature

Lack of Awareness

Odumesi (2015) argued that, lack of cybersecurity awareness in Nigeria was a motivating factor for cybercrime because it made it easy for fraudsters to operate leading to huge financial losses and a negative impact on the credibility and reputation of the country. This argument was confirmed by the research findings that lack of awareness by members of the public was a contributing factor to rendering them targets of attacks by cybercriminals. Also, the findings agree with Oluwu (2009) who asserted that the lack of awareness also extended to ICT companies operating in Africa as most decision makers were now fully aware of the cybercrime problem. Also, the findings of the research show that members of the public were not fully aware that their routine activity on the internet made them suitable targets. This finding confirms Yar's (2005) argument that there was a connection between the target visibility and suitability as the potential offender knew of the existence of the target.

Table 8.2 summarises the findings in the current research, literature review and Routine Activity Theory.

The Current Research	Literature	Routine Activity Theory
Lack of awareness was coded six times by interviewees	• Lack of awareness making businesses and individuals lose money	An unaware victim that is a suitable target because he is visible and has some sort of value to the criminal
New Insight: Lack of awareness of a suitable target (i.e. human) is a factor in understanding why a motivated offender would commit a crime and it supports routine activity theory		

Table 8.2: Summary of Lack of Awareness findings and literature

Weak Laws

According to Hassan et al. (2012) the lack of enforcement of some weak laws governing cybercrime was prevalent in Nigeria and most law enforcement agencies lacked the sophisticated hardware tools to track down an online criminal. This argument aligns with the similar findings of the current research that highlighted how weak laws or enforcement of laws had made offenders to target victims and businesses easily. Furthermore, the UNODC (2013) states that with the exception of the United States and Europe, the rest of the world has insufficient investigative powers to investigate cybercrime. Thus, the Nigerian government over the recent decade has enacted various laws and policies for the sole purpose of improving their curtailment of cyber-related offences (Chawki et al. 2015). However, law-makers must continuously respond to ICT and Internet development so as to measure the effectiveness of existing laws and provisions (ITU, 2012). This argument aligns with findings from the research that has shown how the laws in Nigeria have continued to change and progress based on the evolution of ICT technologies. Table 8.3 compares the current research findings and literature

The Current Research	Literature	Routine Activity Theory
Weak laws was coded five times as a cause of cybercrime	• Lack of adequate laws • Lack of enforcement of laws • Weak laws do not deter cybercriminals	Weak Laws is not part of RAT three elements; however, an offender may be motivated to commit a crime if the laws penalising that crime are weak.
New Insight: Current research supports the existing literature but does not support routine activity theory		

Table 8.3: Summary of Weak Laws findings and literature

Financial Gain

Felson (1998:55) argues that the valuation of the target varies according to the shifting value attached socially and economically to particular goods at particular times. Also, factors such as scarcity and fashion determine the value placed on the target by offenders and others. However, the offender's rationale for selecting a particular target rests upon whether the target is for 'personal pleasure, for sale,' or to be used in committing another crime (Yar, 2005). These arguments resonate with the findings of the current research that showed that financial gain attached to the target was a motivating factor to commit crime.

With a high unemployment rate in Nigeria, especially amongst the youths, Hassan et al. (2012) argued that the quest for financial gain of ill-gotten wealth coupled with the minimal risk of committing crime online all contributed to cybercrime which offered offenders in Nigeria a suitable avenue to perpetrate their illegal activities. These arguments align with findings of the research, as it shows that offenders are motivated and most likely to commit crime based on a financial gain they perceive they might get from the value of the target.

Table 8.4 compares the current research findings and literature

The Current Research	Literature	Routine Activity Theory
Financial gain was coded three times	• Major cause of cybercrime • Cybercrime costs in Nigeria are mostly financial	Financial gain attached to the value of the suitable target is a motivating factor
New Insight: Current research supports and adds to the existing literature by stating that most Nigerian cybercriminals are financially motivated and supports routine activity theory		

Table 8.4: Summary of Financial Gain findings and literature

8.3.1.2: Part Two: Motivated Offender

Clarke and Felson (2008:2) argued that there were three minimal elements for direct-contact predatory crime which were a likely offender, a suitable target, and the absence of a capable guardian against crime. They further stated that a likely offender was anybody who for any reason might commit crime. Lopez (2014) maintains that in RAT, a crime can only take place if there is a motivated offender, thus, meaning that there must be a motive to begin with. The motive varies based on the objective of the offender, and most often motivated offenders as elements of crime were very difficult to control or foresee in the prevention of crime.

The motivation of an offender to commit cybercrime especially in Nigeria is discussed from the viewpoint of understanding the main causes of cybercrime in the findings of the research. Figure 8.1 shows some of the causes of cybercrime from the current research that are related to a motivated offender.

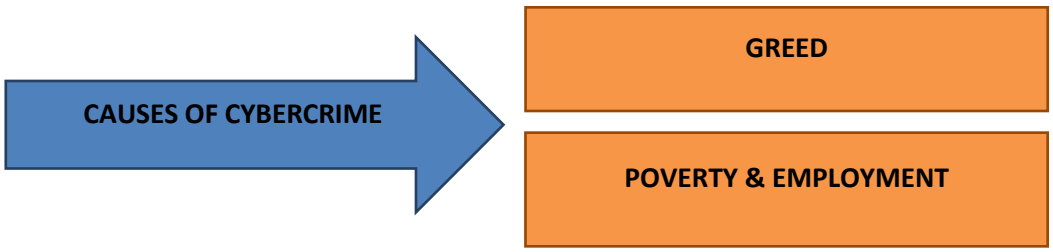


Figure 8.2: Causes of Cybercrime (Motivated Offender)

Greed

Cyber criminality and cyber victimisation are crimes associated with the exploitation of human weaknesses such as greed, gullibility and the quest for getting rich syndrome and not crimes that are necessarily influenced by poverty or unemployment (Adesulu, 2017). This aspect of cybercriminality was found in the current research and most participants agreed that greed was a major reason that motivated offenders to commit cybercrime. However, some of the interviewees argued that greed and peer pressure from society and friends played a role in motivating offenders to commit crime. The peer pressure factor was not found in the literature even though, Jacinta (2017) argued that, the offender did not necessarily have what it took to sustain their livelihood but rather preferred an easy and often illegitimate way of getting money. Also, Hassan et al. (2012) argued that high unemployment amongst the youth was a motivating factor as cybercrime offered them minimal risk of getting caught. Table 8.5 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Greed was coded ten times	• Greed as a motivating factor for offenders • Get rich syndrome common amongst youth • Some arguments links Unemployment and peer pressure	Greed as a motivating an offender to commit crime
New Insight: Current research both supports and contradicts the existing literature and supports Routine Activity Theory		

Table 8.5: Summary of Greed findings and literature

Poverty and Unemployment

Hassan et al. (2012) argued that cybercrime in Nigeria was associated with high rates of unemployment, poverty and an ineffective educational system. However, Adesina (2017) stated that high rate of unemployment and poverty was a paradox in Nigeria since the country was a leading oil-producing nation and rich in mineral resources. This argument aligns with the findings of the current research as it has shown that most people commit cybercrime because of poverty and unemployment. Furthermore, statistics have shown that the unemployment is high amongst university graduates that have high levels of computer and internet competency (Oluwu, 2009). This point expressed by Oluwu (2009) correlates with the current research findings but contradicts some of the findings that show that unemployment is not an excuse to commit crime as there are many unemployed youths not partaking in an illegal activity to make a living. However, some of the findings also show that some of the cybercriminals are still in university and are being sponsored by their parents; so they are not necessarily unemployed but just looking for an illegal means to gain financial independence. This contradicts the existing literature and argument of Adesina (2017) which argued that the cocktail mix of idleness on the side of the offender and availability and affordability of the internet made the youth more prone to commit cybercrime. Table 8.6 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Poverty repeated six times & Unemployment coded eight times	• High poverty and unemployment especially amongst youth • Likely offender are mostly youths • Youths from university with some computer skills are more prone to be offenders	Poverty and unemployment as motivating an offender to commit crime.
New Insight: Current research both supports and contradicts the existing literature and supports routine activity theory.		

Table 8.6: Summary of Poverty and Unemployment findings and literature

8.3.2. Research Question 2

Are Law Enforcement Agencies in Nigeria capable guardians in tackling cybercrime and explored in relation to Routine Activity Theory?

In order to discuss whether LEAs were capable guardians in preventing and investigating cybercrime, it was necessary to discuss the RAT element of absence of a capable guardian. Finally, the challenges facing LEAs and the measures used by LEAs in tackling cybercrime was discussed in relation to the literature review.

8.3.2.1. Absence of a Capable Guardian

A guardian refers to anyone or anything that creates a protection for the target victim. The motivated offender is discouraged from committing an offense when they know that the target has a guardian. Therefore, capable guardians as elements of crime can be controlled, modelled or changed to prevent crime (Lopez, 2014). This research question is discussed from the viewpoint of stakeholders' role in tackling cybercrime and how the routine challenges they faced in the discharge of their duties limited them in being capable guardians in cyberspace. Figure 8.3 shows the challenges faced by LEAs and other stakeholders in tackling cybercrime.

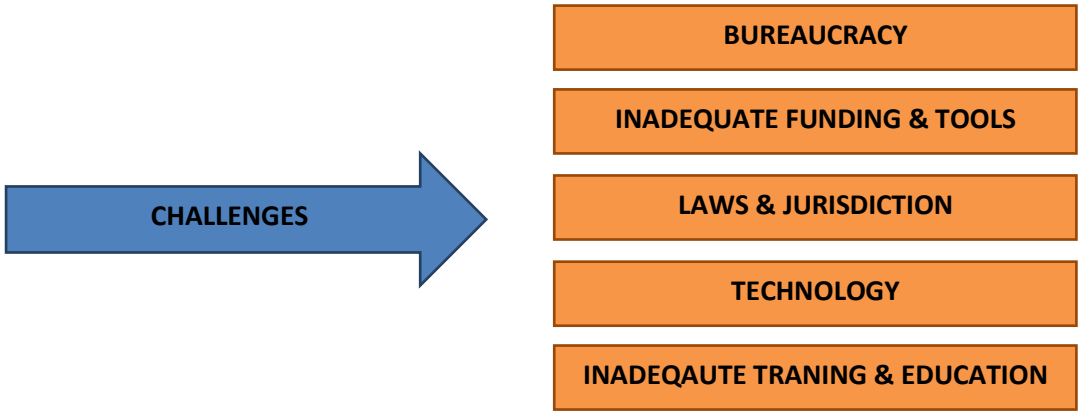


Figure 8.3: Challenges of Tackling Cybercrime (Capable Guardianship)

Bureaucracy

As shown in the research findings, bureaucratic bottlenecks within LEAs and other organisations hindered capable guardians such as the police in their endeavours for crime detection or prevention. Participants argued that bureaucracies in their organisation and other external large IT firms such as Google and Facebook made them incapable of protecting

victims from cybercrime. This argument contradicts Yahaya's (2009) position that shows the Nigerian government as having a robust partnership especially with Microsoft with the aim of tackling cybercrime and software piracy in Nigeria. The findings also show that there is an issue in coordinating policies and practices in mitigating the activities of cybercrime. This finding contradicts Owens (2014) argument that places the blame on the traditional Nigerian police as having structural constraints which rendered it vulnerable to interference by the political elite, thus, limiting the police in effectively enforcing the law. Table 8.7 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Bureaucracy was coded five times	• Government and organisations have MoU and partnership with relevant stakeholders • Few literature to support bureaucracy.	Bureaucracy as a variable hindering the capability of a guardian to prevent crime.
New Insight: Current research contradicts the existing literature and supports routine activity theory		

Table 8.7: Summary of Bureaucracy findings and literature

Laws and Jurisdiction

As shown by the research findings, the multiplicity of laws and different jurisdictions is a major challenge to stakeholders especially LEAs in tackling cybercrime globally. Participants argued that due to the transnational nature of cybercrime, it made it difficult to conduct a proper investigation without an existing legal instrument and agreement with other countries to back it up. This finding aligns with the UNODC (2013) argument that with the exception of Europe and America, most developing countries had insufficient powers to investigate and prosecute cybercrime. Furthermore, the finding aligns with Yar's (2007) argument of 'jurisdictional disparities' which could be problematic especially with policing or prosecuting deviant behaviours. The finding also shows that cooperation and collaboration between different countries on cybercrime issues is very challenging. The finding confirms Smith's (2013) argument that the harmonisation of laws and adoption of international conventions on cybercrime would make prosecution easier and improve the mutual assistance and extradition of criminals between countries. These findings also support Cohen and Felson's (1979) argument that lack of a capable guardian was a necessary condition for crime to take place. Yar's (2005) argument, that where the capable guardian was a person, their mere presence

served as a gentle reminder that someone was looking. This aligns with the findings of the current study because the jurisdictional limitation of conventional police to deter crime from taking place was much more evident in cyberspace than in terrestrial space.

Table 8.8 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Laws and jurisdiction was coded seven times	• Different laws and jurisdiction hinders • Similar laws, existing MLATs and adoption of international convention makes investigation and prosecution easier	Different laws and Jurisdiction as a variable hindering the capability of a guardian to prevent and investigate crime.
New Insight: Current research supports and adds to existing literature and supports the understanding of routine activity theory capable guardianship		

Table 8.8: Summary of Laws and Jurisdiction findings and literature

Technology

The finding from the research shows that the evolution of technology and the adoption of new technology to facilitate the commission of cybercrime by the criminals is a major challenge for stakeholders responsible for preventing, investigating or prosecuting cybercrime. This finding resonates with Chukkol (2014) who pointed out that Nigeria had witnessed the acceleration of crimes at a faster rate due to criminals embracing ICT to commit crimes. The finding also shows that some of the cybercrime investigators are playing 'catch up' in terms of their skillsets and training for investigating cybercrime. This finding aligns with Smith's (2003) argument that the investigation of cross-border cybercrime required adequate technical and forensic skills and knowledge. Also the finding aligns with Tiv's (2006) observation that the investigation of advance fee fraud required some computer knowledge which the criminals knew were beyond the skills of the traditional Nigerian Police Force. However, some of the findings especially from the 'Forensic Analyst' shows that the affordability of storage devices makes the acquisition of evidence from a digital artefact more difficult and time consuming because of low levels of qualified staff available to extract the information. This finding contradicts the ITU (2012) position which stated that even though the low cost of digital storage had increased, the number of digital sources of evidence, the digitisation and the use of such technologies had a great impact on procedures related to the

collection of evidence and its use in court. The finding aligns with Cohen and Felson's (1979) argument that lack of a capable guardian was a necessary condition for crime to take place.

Table 8.9 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Technology was coded six times	• Criminals embracing ICT (Chukkol, 2014) • AFF requires technical knowledge (Tiv, 2006)	Technology as a variable hindering the capability of a guardian to prevent and investigate crime.
New Insight: Current research supports and contradicts existing literature and supports the understanding of routine activity theory capable guardianship		

Table 8.9: Summary of Technology findings and literature

Inadequate Funding and Tools

The findings from the research show that inadequate funding for the procurement of tools and other logistical equipment needed to prevent and investigate cybercrime is a major challenge in fighting cybercrime. Some of the findings showed that the tools were either outdated or non-existent for investigating the ever evolving nature of cybercrime. This finding is in alignment with Smith (2013) who pointed out that the level of funding required for training and upgrading of equipment was inadequate. The finding also agrees with Dalton's (2012) assertions that cyber investigations were costly and that consequently, governments were reluctant to free up the funds. Also, the finding is in alignment with Cohen and Felson (1979) who pointed out that the lack of capable guardianship was a necessary condition for crime to take place in addition to the presence of a suitable target and a motivated offender. Table 8.10 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Inadequate funding and tools was coded twelve times	• Funding of LEAs critical to cyber investigation • Cyber investigations and tools are expensive	Inadequate funding and tools as a variable hindering the capability of a guardian to prevent and investigate crime.
New Insight: Current research supports existing literature and supports the understanding of Routine Activity Theory capable guardianship		

Table 8.10: Summary of Inadequate Funding and Tools findings and literature

Inadequate Training and Education

The findings of the research shows that inadequate training on the part of the investigators and lack of awareness on the part of the general public is a major challenge in tackling cybercrime. This aligns with Odumesi (2015) who pointed out that lack of cybersecurity training especially amongst LEAs had made it easy for fraudsters to operate in Nigeria leading to huge financial losses. The finding also aligns with Wall (1998) that public policing practices have been shaped by the time honored tradition of policing and could not respond to such rapid changes of ICT. The finding also shows that some of the lawyers and judges have inadequate knowledge about cybercrime, thus, making prosecution of cybercrime very difficult. This aligns with Buono's (2010) assertion that the current lack of adequate training on cybercrime for judges and prosecutors does not afford them the level of training required to deal with cybercrime and electronic evidence. Also, the finding is in alignment with Cohen and Felson (1979) arguments that lack of capable guardianship provided by either LEAs or a judge is needed for crime to occur.

Table 8.11 compares the current research findings and literature.

The Current Research	Literature	Routine Activity Theory
Inadequate training and education was coded fourteen times	• Inadequate training more evident in law enforcement and judges • Inadequate education with the public	Inadequate training and education as a variable hindering the capability of a guardian to prevent and investigate crime.
New Insight: Current research supports and adds to existing literature and supports the understanding of routine activity theory capable guardianship		

Table 8.11: Summary of Inadequate Training and Education findings and literature

8.3.3 Research Question 3

To what extent are the current laws adequate in investigating cybercrime in Nigeria?

Proper legislation is the bedrock for the investigation and prosecution of cybercrime. However, lawmakers in different jurisdictions must continue to respond to internet developments and monitor the effectiveness of existing legal instruments, most especially due to the fast evolution in digital and internet technologies (ITU, 2012). Grabosky (2012) argued that one of the greatest challenges faced by the advent of digital deviant behaviours is that it has greatly enhanced the potential for transnational crime. He stated further that, 'a degree of

common legal ground is required in order to mobilize the law of a foreign state on one's behalf'. The adequacy of laws in investigating cybercrime is discussed from the findings and emergent outcomes of the current research. Figure 8.4 shows the theme and emergent sub-themes to be discussed.

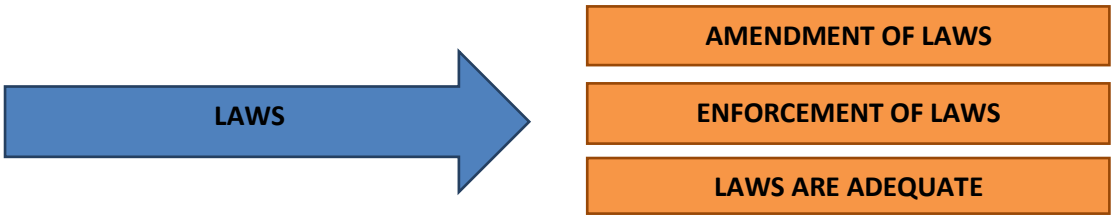


Figure 8.4: Adequacy of Laws

Amendment of Laws

The finding of the current research shows that there is a need to amend some parts of the law due to their inadequacy for prosecuting criminals. This finding is in alignment with Chawki et al. (2015) who argued the Nigerian government had enacted various laws and policies for the sole purpose of curtailing the activities of cybercriminals. Such laws included the Criminal Code Act, Economic and Financial Crimes Commission Act 2004, Advance Fee Fraud and other Fraud Related Offences Act 2006. In regards to the Criminal Code Act of 1990, Oriola (2005) pointed out its limitations in enforcement by LEAs and the lack of restitution for the victim of the crime. This was confirmed by the findings of the current research. Also, some of the findings showed that even the recently enacted Cybercrime Act 2015 needed to be amended as there was no section showing who would enforce the many offences listed in the law. Adaramola's (2015) argument also aligns with the findings of the current research because it contended that the definitions provided in the Act were 'too specific' and might give scope for offenders to use other means of committing crimes outside the specific definitions of the law. Table 8.12 compares the current research findings and literature.

The Current Research	Literature
Amendment of laws was coded five times	• Laws are constantly amended to reflect the current changes in ICT and internet technologies. • Amendment of laws take time to be concluded
New Insight: Current research adds to literature as it has shown that the current Cybercrime law needs significant amendments as it was passed without various stakeholder participation.	

Table 8.12: Summary of Amendment of Laws findings and literature

Enforcement of Laws

The findings of the current research show that the current laws are adequate and need to be properly enforced in order to investigate and prosecute cybercrime. Also, the finding show that judges and lawyers need to be adequately trained to enforce the laws. The finding is in alignment with Hassan et al. (2012) who showed how the lack of enforcement of some fragile laws regarding cybercrime was prevalent in Nigeria and most law enforcement agencies lacked the necessary tools to investigate cybercrime. However, the findings contradict Olowu's (2009) position that links lack of enforcement to lack of training and tools to investigate cybercrime. The findings are also contrary to Ajayi (2016) who argued that challenges to enforcement of cybercrimes were usually necessitated by jurisdictional differences and identifying the cybercriminal. He further argued that the extradition process was lengthy and difficult and that the lack of effective reporting of crime was detrimental to the enforcement of cybercrime laws. Table 8.13 compares the current research findings and literature.

The Current Research	Literature
Enforcement of laws was coded nine times	• Laws are adequate but need enforcement. • Enforcement challenges are mostly from lack of skillsets to enforce the law or jurisdictional issues
New Insight: Current research supports literature by showing the connection between training of judges and LEA officers and enforcement of the law	

Table 8.13: Summary of Enforcement of Laws findings and literature

Laws are Adequate

The finding of the current research showed that the laws are adequate and properly enforced. However, some of the findings showed that there is a misapplication of the current law towards freedom of speech. The finding aligns with Oke's (2015) argument that the Cybercrime Act 2015 was adequate as it addressed the inadequacies of previous laws such as the Economic and Financial Crimes Act 2004, Advance Fee Fraud and Other Fraud Related Offences Act 2006 in regulating cybercrime. The finding is also in alignment with Nkanga (2016) who states that since the Cybercrime Act was passed into law it has been used to muzzle the press and online bloggers through the application of a controversial clause on cyber-stalking. Table 8.14 compares the current research findings and literature.

The Current Research	Literature
Laws are adequate was coded seven times	• Laws are adequate and created due to inadequacies of previous laws • Misapplication of Laws by the political elite against freedom of speech in Nigeria
New Insight: Current research adds to literature on how the misapplication of cyber laws is targeted at freedom of speech in Nigeria.	

Table 8.14: Summary of Laws are Adequate findings and literature

Table 8.15 compares the various laws with the emergent themes

S/N	LAWS	Emergent Outcomes		
		Amendment of Law	Enforcement of Law	Law is Adequate
1	Criminal Code 1990	√		
2	EFCC Act		√	
3	Advance Fee Fraud Act 2006		√	
4	Cybercrime Act 2015	√	√	√

Table 8.15: Summary of Laws and Correlation with Emergent Themes

8.3.4 Research Question 4

How are the different definitions of cybercrime appropriate in understanding cybercrime in Nigeria?

The absence of a consistent current definition amongst law enforcement agencies mandated to tackling cybercriminals is one of the major problems of cybercrime (NHTCU/NOP 2002:3). The term 'has no specific referent in law' still dominates the political, criminal justice, public and academic discourse of many nations (Wall, 2002:2). The research question is discussed based on the definition of cybercrime by all the interviewees and subsequently grouped into two emergent themes of the current research. Figure 8.5 shows the theme and emergent sub-themes to be discussed

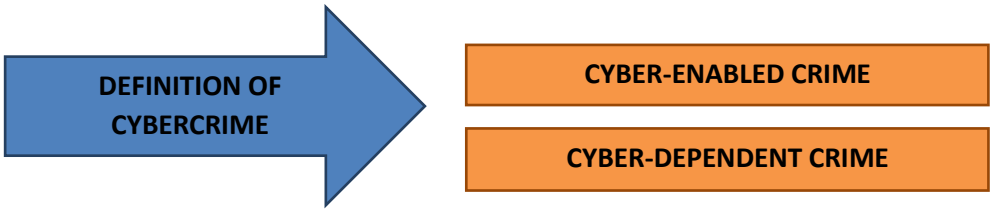


Figure 8.5: Definition of Cybercrime

Cyber-Enabled Crime

One finding of the research shows that the majority of the interviewees defined cybercrime in terms of traditional crime but which could be increased in scale by the use of ICT or the internet. The finding aligns with McGuire & Dowling's (2013b) definition of cybercrime as traditional crimes such as financial fraud, 416 and phishing that are increased in their scale or reach 'by use of computers, computer networks or other form of ICT'. Also, the findings are consonant with the UK Government (2016) National Cyber Security Strategy that categorises cybercrime in the context of two interrelated forms of criminal activity of cyber-dependent and cyber-enabled crimes. However, the finding contrasts with Pati's (2007) definition that categorises cybercrime based on the victims of the crime. The finding also contradicts the Council of Europe (2001) definition on cybercrime which differentiates between four types of offences, namely; offences against the confidentiality, integrity and availability of computer data and systems; computer – related offences; content-related offences; and copyright-related offences. Table 8.16 compares the current research findings and literature.

The Current Research	Literature
Cyber-Enabled Crime was coded eighteen times	• Definition varied considerably (See Table 8.18)
New Insight: Current research adds to literature as it showed how ICT officers, Investigators and Prosecutors defined cybercrime differently within the scope of cyber-enabled crimes	

Table 8.16: Summary of Cyber-Enabled Crime findings and literature

Cyber-Dependent Crime

The findings of the research also showed that some of the interviewees defined cybercrime as crime that can only be committed using a computer, ICT or the network. The finding agrees with McGuire & Dowling's (2013a) definition of cybercrime as offences that can only be committed using a computer, computer networks or other forms of ICT. Examples are

malware, hacking, DDoS etc. The finding also aligns with the UK Government's (2016) National Cyber Security Strategy definition as crimes which are committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime and the target of the crime. However, the finding contradicts Pati (2007) definition that categorises cybercrime based on victims of the crime as well as the Council of Europe (2001) categorisation of cybercrime. One of the cybercrime investigators, however, defined cybercrime as crime targeting the confidentiality, integrity and availability of a computer which aligns with the Council of Europe (2001) categorisation of cybercrime. Table 8.17 compares the current research findings and literature.

The Current Research	Literature
Cyber-Dependent Crime was coded six times	• Definition varied considerably (See Table 8.18)
New Insight: Current research adds to literature as it showed how ICT officers, Investigators and Prosecutors defined cybercrime differently within the scope of cyber-enabled crimes	

Table 8.17: Summary of Cyber-Dependent Crime findings and literature

Table 8.18 is a matrix showing how the findings of the current research are either in alignment or contradiction with existing literature on the definition of cybercrime.

S/N	SOURCE/AUTHOR	CATEGORISATION	CURRENT STUDY	
			ALIGNS	CONTRADICTS
1	**Council of Europe (2001)**	• Offences Against CIA • Computer-related offences • Content-related offences • Copyright-related offences		✕
2	**Pati (2007)**	• Against Individual • Against Individual Property • Against Organisation • Against Society		✕
3	**Wall (2003,2005)**	• Cyber-Assisted • Cyber-Enabled • Cyber-Dependent	✕	
4	**Home Office (2016) McGuire & Dowling (2013a,b)**	• Cyber-Enabled • Cyber-Dependent	✕	

Table 8:18 Showing Alignment and Contradiction of Literature with Current Research

8.3.5 Research Question 5

What improvements are needed in the International efforts in tackling cybercrime globally?

The improvements needed in the international effort to tackle cybercrime globally are discussed from the findings and emergent outcomes of the current research. Figure 8.6 shows the theme and emergent sub-themes to be discussed.

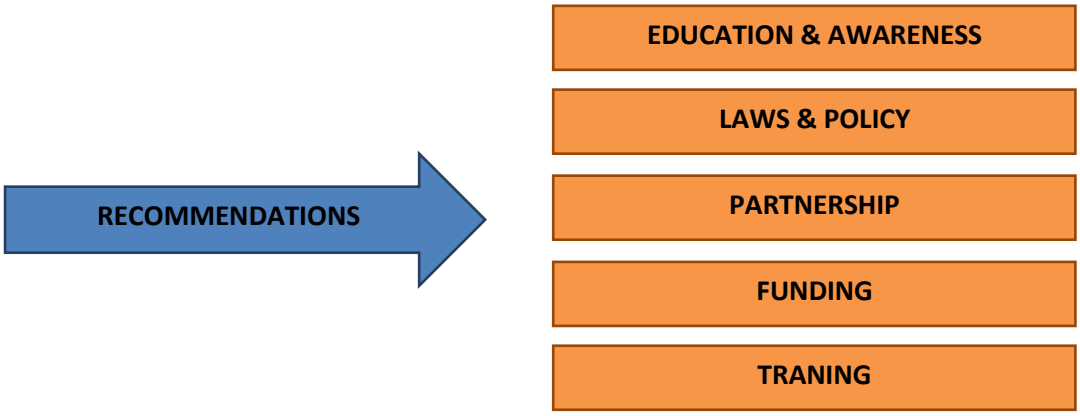


Figure 8.6: Improvements & Recommendations

Education and Awareness

The findings of the research showed that the education of the public and raising awareness about cybercrime and cybersecurity is one of the major ways of improving the international efforts in tackling cybercrime. This finding aligns with Kortjan and Solms (2014) argument that education and awareness can facilitate individuals to become knowledgeable about the risks that are present online. The finding also shows that the arrest and prosecution of cybercriminals is not adequate in deterring crime but would rather compound the problem. This finding contradicts Abubakar's (2009) statement that through collaboration with foreign police and organisations, the Nigerian government has been able to effectively investigate and prosecute the activities of scammers. The finding also contradicts Kortjan and Solms (2014) in their stance that education rather than arrest played an important role in developing a culture of secure behaviours amongst users in the cyber domain. Furthermore, the findings underline the need to include family and friends as some individuals consider their deviant

behaviours online to be legal. This finding amplifies the argument of Dix (2017) stating that a comprehensive national security education campaign in all sectors was mandatory for raising public awareness of the risk and impact of some cyber activities; hence the need to deploy basic protective measures in using online digital devices. The finding also supports Aloul's (2012) argument that different groups have to be involved in order to produce IT security-aware residents.

Table 8.19 compares the current research findings and literature.

The Current Research	Literature
Education & awareness was coded fifteen times	• Education of the public vital to cybersecurity and online hygiene • Cybersecurity awareness is low amongst online users and government official • Different sectors involved in raising awareness (i.e. government, LEAs, NGOs, schools & individuals)
New Insight: Current research adds to literature as it states that, the arrest and prosecution is not adequate to tackle cybercrime.	

Table 8.19: Summary of Education & Awareness findings and literature

Laws and Policy

The findings of the research highlight the need to strengthen and enforce existing laws and policies to assist the activities of relevant stakeholders in investigating cybercrime. The finding supports Olusola et al. (2013b) in their proposition that governments should work together in strengthening the legal frameworks for cybersecurity. The finding also aligns with Hassan et al. (2012) who argued that the Nigerian government must enforce laws regarding cybercrime in order to deter cybercriminals from their nefarious activities. However, the findings reveal that many have commented that forensic laboratory used to analyse digital evidence in cybercrime cases should be made independent of their organisations as the current situation amounted to a conflict of interest in the court. This finding contradicts Aloul's (2012) recommendation that law enforcement agencies such as the police should have dedicated forensics teams that are specialised in rendering professional support to investigators in the investigation of cybercrime.

Table 8.20 compares the current research findings and literature.

The Current Research	Literature
Laws & policy was coded ten times	• Common laws and policies needed to fight cybercrime globally (Grabosky, 2001) • Multi-stakeholder engagement required to educate and raise awareness (Aloul, 2012) • Enforcement of existing laws necessary in investigating cybercrime (Hassan et al., 2012)
New Insight: Current research adds to literature as it states that, forensic units should be autonomous rather than domiciled within an organisation.	

Table 8.20: Summary of Laws & Policy findings and literature

Partnership

The findings elaborate on the importance of partnership with the public and private sector in order to share information that is vital in investigating, prosecuting and preventing cybercrime. This finding aligns with Binns (2017) who emphasised the importance of collaboration in a successful police investigation. Her argument further aligns with the current findings, as she states that, partnerships help to foster the flow of information and that there is an information sharing gap between stakeholders which can provide an avenue for cybercriminals. The finding also aligns with the WEF (2016) recommendation that the public and private sectors should work to create platforms that enhance information-sharing and improve investigation and prosecution of cybercrime. However, some of the findings also indicated that a central organisation, namely the Office of the National Security Advisor, should coordinate all collaboration and partnership between the private and public sector.

Table 8.21 compares the current research findings and literature.

The Current Research	Literature
Partnership was coded sixteen times	• Partnership needed for successful police investigation (Binns, 2017) • Standard police practice not enough to curtail cybercrime (WEF, 2016)
New Insight: Current research adds to literature as it states that, there should only be one organisation (i.e. ONSA) to coordinate collaboration between the public and private sector.	

Table 8.21: Summary of Partnership findings and literature

Funding

The findings recommended that there should be an increase in funding to train law enforcement officers and purchase tools in tackling cybercrime. This finding corroborates

that of Barej (2017) who holds the view that there is an urgent need to increase the budgetary allocation of law enforcement agencies to tackle cybercrime. The finding, however, did not share the opinion of WEF (2016), which argued that the funding gap could be addressed through a public private partnership of stakeholders rather the finding enumerated the kinds of devices and equipment that needs to be purchased by the government so as to tackle the cybercriminals. The finding also showed that the current equipment used in investigating cybercrime are outdated and not at a par with international best practices. Table 8.22 compares the current research findings and literature.

The Current Research	Literature
Funding was coded ten times	• Shortages in expertise and resources in African States (Tamarkin, 2015) • Need to increase budgetary allocations for LEAs (Beraj, 2017) • Funding gap could be bridged through public-private partnerships (WEF, 2016)
New Insight: Current research adds to literature as it states that, due to the workload of analyzing digitally retrieved evidence, the current ICT systems used in investigation cybercrime needs to be upgraded to assist in investigating cybercrime effectively.	

Table 8.22: Summary of Funding findings and literature

Training

The finding showed that there is a need to train law enforcement officials in the investigation of cybercrime because most of the cybercriminals are better skilled than the investigators. The finding corroborates that of Ajayi (2016) that most of the cybercriminals are better educated, trained and have more resources compared with law enforcement officers. The finding correlated with the WEF (2016) recommendation that the public sector should collaborate with the private sector in sharing best practices in IT education and training. Also, the finding showed that investigators need training more than other stakeholders, as the tools and processes they use in investigating a cybercrime incident would affect how the investigation of such an incident would be prosecuted in court.

Table 8.23 compares the current research findings and literature.

The Current Research	Literature
Training was coded nineteen times	• Cybercriminals are better skilled than most law enforcement officers (Ajayi, 2016) • Challenges in recruitment and retention of skilled law enforcement officials (Saunders, 2017) • Training gap could be bridged through public-private partnerships (WEF, 2016)
New Insight: Current research adds to literature as it states that, investigators need more training than prosecutors and analyst.	

Table 8.23: Summary of Training findings and literature

8.4 Overall Theme Conclusion

Having provided discussions to each of the five questions, which meet the aim and objectives of this research study, conclusions can be made based on the eleven themes from the literature review. Therefore, the following conclusions can be made for each of the eleven themes which are presented as follows:

8.4.1 Theme 1: Function of Office

The research finding differentiated the various stakeholders and the general function of their offices. The finding showed that majority of the stakeholders were from a law enforcement organisation with a mandate to investigate and prosecute cybercrime in Nigeria and the UK. This finding corroborated that of the EFCC (2004) stating that the mandate of the EFCC and the National Crime Agency and West Yorkshire Police law enforcement roles respectively (NCA, 2017b; West Yorkshire Police, 2017a). The finding also showed that the National Communications Commission had a mandate in regulating the telecommunications sector in Nigeria, while the National Information Technology Development Agency had a role in regulating the ICT sector. This resonates with the mandates of NITDA (NITDA, 2017b) and the mandates of the NCC (NCC, 2017b). The finding showed that the Senate has an oversight function on cybercrime matters in Nigeria which aligns with Adebusiyi's (2008) views on the legislative functions of the National Assembly; while the finding showed that the Office of the National Security Advisor was the overall coordinator of the Cybercrime Advisory Council which aligns with the dictates of the Cybercrime Act (2015) on the functions of the ONSA.

8.4.2 Theme 2: Role in Fighting Cybercrime

The finding showed that within the EFCC, five departments and units namely the operations, legal, ICT, Forensics and public affairs department had specific roles in tackling cybercrime in Nigeria. While the operations and legal department dealt with the investigation and prosecution of cybercrime, the ICT and forensics unit provided technical and scientific support in the retrieval and analysis of digital evidence. The finding showed that the public affairs department dealt with the prevention and awareness role in mitigating the activities of cybercrime. These findings align with the different roles and responsibilities of these departments and units as argued in the EFCC (2014) annual report stating the general roles and function of each of the research stakeholders. Equally, the finding showed that the Nigerian Computer Emergency Response Team (ngCERT) is the focal point in managing all cyber incidents in Nigeria. This finding aligns with Council of Europe (2017) that states, the ngCERT was created to effectively manage and coordinate the management of cybersecurity incidents. The finding also showed the specific roles played by the NCC and NITDA through their cybersecurity departments in addressing cybercrime. The finding enumerated the various function of the National Cyber Crime Unit (NCCU) which is domiciled within the National Crime Agency. This finding aligns with the NCA (2017a) statement that the NCCU is in charge of the overall capability to tackle cybercrime in the UK. Finally, the finding aligns with West Yorkshire Police (2017b), that highlights the specific function of the cybercrime and digital forensic unit in tackling cybercrime in West Yorkshire.

8.4.3 Theme 3: Definition of Crime

The finding established that cybercrime was defined within two distinct categories namely cyber-enabled and cyber-dependent crimes. Theme 3 was discussed in detail in ***'8.3.4 – Research Question 4'.*** The finding aligns with McGuire and Dowling (2013b) who defined cyber-enabled crime as traditional crimes that were increased in scale by ICT and cyber-dependent crime that could only be committed with the use of computers or computer networks (McGuire and Dowling, 2013a)

8.4.4 Theme 4: Forms of Cybercrime

The research findings established the forms of cybercrime that were more prevalent in Nigeria and the UK. The finding enumerates the forms of cybercrime as advance fee fraud and financial crimes, hacking and malware, romance scams and scam messages. This finding aligns with the argument of Ribadu (2007) and WITFOR (2005) which states that crime

perpetuated against Nigerian information and telecommunications systems are related to mail scam, credit card fraud and financial fraud. However, this finding contradicts Akuta et al. (2011) that cybercrime activities actually committed by Non-Nigerians but were made to look like '419' crimes and mostly originating from Cameroun.

8.4.5 Theme 5: Causes of Cybercrime

The finding established that there are seven main causes of cybercrime namely financial crime, greed, lack of awareness, poverty, unemployment, vulnerability of systems and weak laws. Theme 5 was discussed in detail in ***'8.3.1 – Research Question 1'***. The findings corroborates Hassan et al. (2012) argument that unemployment and poverty are the main causes of cybercrime and aligns with Adesulu's (2017) views that, greed and the quest for financial gain are the main causes of cybercrime in Nigeria. The finding also aligns with Odemesi (2015) who argued that low cybersecurity awareness in Africa was the reason for high prevalence of cybercrime in many African states.

8.4.6 Theme 6: Partnership

Overall, all the departments and units have both internal and external partnership and collaboration in tackling the cybercrime. The EFCC for example has five departments and units that collaborate in order to tackle cybercrime. A detailed illustration can be found in '***Chapter 2: Research Context Figure 2.2'.***The finding showed that the EFCC has external partnerships with relevant stakeholders such as Microsoft and other law enforcement agencies. This finding aligns with BBC (2009) and EFCC (2014) that the EFCC is partnering with Microsoft by using smart technology rather than cyber raids on internet cafés to tackle the activities of scammers.

8.4.7 Theme 7: Benefit of Partnership

Overall, a series of reasons were presented across the findings on the benefits of both the internal and external partnership. While most agreed that the internal partnership was relevant within departments and units within an organisation, the findings were equally divided in the benefits of the external collaborations. While some of the findings enumerated the many benefits of collaboration such as information sharing and training, some of the findings showed that, lack of synergy and sharing of information was detrimental to investigating cybercrime.

8.4.8 Theme 8: Measures & Counter-Measures

The finding established that there were various measures and initiatives used in tackling cybercrime in Nigeria and the UK. The measures are awareness campaign, adherence to international best practices, enforcement and partnership, training and funding amongst others. The findings align with BBC (2009) views on how partnership is used by LEAs to fight crime. Equally, the finding agreed with Abubakar (2009) argument that, enforcement of relevant cybercrime laws and prevention and education are measures used by the EFCC and other stakeholders in addressing the issue of cybercrime.

8.4.9 Theme 9: Laws

The research findings showed that the laws needed to be amended, enforced or were adequate and properly enforced. Theme 9 was discussed in detail in ***'8.3.3 – Research Question 3'***. The findings aligns with the arguments of Grabosky (2001) on the need to have common laws across all countries and Hassan et al. (2012) notion on the need of the Nigerian government to enforce all the laws regarding cybercrime. The finding also corroborated Olusola et al. (2013b) argument on the need of governments to work together in strengthening their legal frameworks for cybersecurity.

8.4.10 Theme 10: Challenges

Overall, the research found and categorised five main challenges facing stakeholders in tackling cybercrime. These challenges are bureaucracy, inadequate funding and logistics, laws and jurisdiction, technology and inadequate training and education. Theme 10 was discussed in detail in ***'8.3.2 – Research Question 2'***. The findings corroborates Smith's (2003) argument that cybercriminals embracing of technology poses further issues around the inadequate training of law enforcement officers. The finding also aligns with Ajayi (2016), that the lack of common laws and jurisdictional issues is a major challenge in information sharing in the global fight against cybercrime.

8.4.11 Theme 11: Recommendations

Generally, the findings showed that education and awareness, better funding, enforcement of laws and policies and partnership and training were recommended in the global effort to tackle cybercrime. Theme 11 was discussed in detail in ***'8.3.5 – Research Question 5'***. The findings aligned the following arguments that better education and awareness is required (Aloul, 2012); common laws and collaboration between nations is needed (Grabosky, 2001;

Binns, 2017), and adequate provision of funding and training are needed in the global effort to tackle cybercrime effectively (WEF, 2016; Barej, 2017; Saunders, 2017).

8.5 Emergent Themes – Not in Literature

The following is a summary of the emergent themes that were not found in the literature review: The themes are:

Theme 2: Role in Fighting Cybercrime: The specific roles of each of the departments and units of most of the Nigerian stakeholders were not available in the literature review, thus, were collected during the interview process.

Theme 6: Partnership: The internal partnerships and collaboration within organisations that participated in the research were not available in the literature review and was found during the interview process

Theme 7: Benefits of Partnership: Some of the benefits of the partnership were not found in the literature review. For example all the internal partnership benefits within the EFCC, NCC, NCA, WYP, NITDA, ONSA and the Senate were not available in the literature.

Theme 8: Recommendations: Some of the recommendations discovered in the research differs with the recommendations suggested in the literature review.

These emergent themes not found in the literature will be discussed further in *'Chapter9: Conclusion'* under research contributions.

8.6 Summary of Discussions

In summary, table 8.24 illustrates the correlation between the emergent themes with the literature review and findings. The table shows all the themes and the emergent themes with the literature review and findings. The table also correlates all the stakeholders that participated in the research with the literature and findings.

8.7 Conclusion

In conclusion, this chapter discusses all the research questions and gives a brief discussion of all the research themes. Equally, the chapter highlighted the emergent themes that were not found in the literature and summarises all the findings with a correlation table (Table 8.24).

S/N	THEMES	SUB-THEMES	LIT. REV.	FINDING	CASE STUDY						
					Tick where appropriate (×)						
					EFCC	ONSA	NCC	NITDA	NA	NCA	WYP
1	FUNCTION OF OFFICE	ICT Regulation	×	×				×			
		Law Enforcement	×	×	×					×	×
		Legislation	×	×					×		
		National Coordinator	×	×		×					
		Telecoms Regulation	×	×			×				
2	ROLE IN FIGHTING CYBERCRIME	Investigation		×	×					×	×
		Forensics Support		×	×					×	×
		Legal & Prosecution		×	×						
		ICT Support		×	×						
		Media & Prevention		×	×						
		National Coordinator	×	×		×					
		Telecoms Regulation	×	×			×				
		ICT Regulation	×	×				×			
		Legislative Support	×	×					×		
3	DEFINITION OF CYBERCRIME	Cyber-Enabled Crimes	×	×	×	×	×	×	×	×	×
		Cyber-Dependent Crimes	×	×	×	×	×	×	×	×	×
4	FORM OF CYBERCRIME	AFF & Financial Fraud	×	×	×	×	×			×	×
		Hacking & Malware	×	×	×	×	×	×	×	×	×
		Romance Scam	×	×	×						
		Scam Messages	×	×	×						
5	CAUSES OF CYBERCRIME	Financial Gain	×	×	×	×	×	×	×	×	×
		Greed	×	×	×	×	×	×	×		
		Lack of Awareness	×	×	×			×		×	×
		Poverty	×	×	×						
		Unemployment	×	×	×						
		Vulnerability of Systems	×	×	×	×	×				
		Weak Laws	×	×	×						
6	PARTNERSHIP	Internal Partnership		×	×		×	×		×	×
		External Partnership	×	×	×	×	×	×	×		×
7	BENEFITS OF PARTNERSHIP	Internal Partnership		×	×		×	×		×	×
		External Partnership	×	×	×	×	×	×	×		×
8	MEASURES AND COUNTER-MEASURES	Awareness Campaign	×	×	×				×	×	×
		Best Practices	×	×	×					×	×
		Enforcement	×	×	×	×					
		Funding & Logistics	×	×	×	×		×		×	
		Partnership	×	×	×	×	×	×	×	×	×
		Training and Manpower	×	×	×	×	×	×	×		
		Benefit of Measures		×	×		×		×	×	×
9	LAWS	Amendment of Laws	×	×	×				×		
		Enforcement of Laws	×	×	×	×	×				
		Laws Are Adequate	×	×	×		×	×		×	×
10	CHALLENGES	Bureaucracy		×	×		×	×	×		
		Inadequate Funding & Tools	×	×	×			×			
		Laws & Jurisdiction	×	×	×				×		
		Technology	×	×	×	×					
		Inadequate Training and Education	×	×	×	×		×		×	×
11	RECOMMENDATIONS	Education & Awareness	×	×	×						
		Funding & Tools	×	×	×					×	×
		Laws & Policy	×	×	×						
		Partnership	×	×	×	×	×	×	×	×	×
		Training	×	×	×	×	×	×			

Table 8.24: Themes and Sub Themes Correlation with Literature Review and Findings

CHAPTER 9: CONCLUSION

9.1 Introduction

This conclusion chapter revisits the research rationale and reviews how the research was conducted. The chapter reviews the contributions to knowledge, theory, practice and policy. Also, this chapter explains how Klein and Myers' (1999) principles of interpretive field research was used to evaluate the research. Finally, the chapter focuses on limitations and the potential future directions for the research.

9.2 Research Summary

As discussed in the introduction and literature review, there is a paucity of literature on law enforcement and the roles of members of the Cybercrime Advisory Council in tackling cybercrime collaboratively. Most of the previous studies focused on the causes and effects of cybercrime in Nigeria (Hassan et al., 2012; Adesina, 2017); laws penalising the misuse of computers (Olusola et. al., 2013b; Saulawa and Abubakar, 2014) and have focused relatively on financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et. al., 2012). The current study brings all these different factors together and attempts to understand cybercrime from a Nigerian law enforcement viewpoint such as the studies Maghairah, (2009) and Alkaabi (2010) have done.

Furthermore, the research adopts a classical criminological framework of Routine Activity Theory, in examining the applicability of the theory to cyberspace, which Yar (2005) has argued can be considered in understanding cybercrime. The justification for selection of the theory was discussed in detail in Chapter 4. The research was framed based on an interpretivist paradigm and a relativist philosophical view, which accommodates the methodology to the exploratory and explanatory nature of the current research. Due to the social nature of the research topic, a qualitative approach was used in collecting data through interviews. Interviews were conducted with thirty four participants mostly from a law enforcement agency. Evidence in the research suggested that members of the Cybercrime Advisory Council have attempted to overcome challenges in investigating cybercrime through partnership, training and enforcement of relevant laws and policy. Finally, the finding extends the criminological view of online deviant behaviour and further the current discussion on the role of law enforcement in policing cybercrime in Nigeria. The contributions of the study are categorised as follows:

9.3 Theory Contribution

The study addresses the gap in the application of Routine Activity Theory (RAT) to deviant online behaviors such as advance fee fraud in Nigeria by extending the criminological understanding of the suitability of a target, a motivated offender and the absence of a capable guardian within the scope of law enforcement. This study added to the understanding of the three RAT elements as follows:

Suitable Target: Yar (2005) argued that, 'the greater the target's accessibility, the greater the suitability', and the offenders rationale in picking a suitable target is based upon whether the target is for 'personal, pleasure, for sale' or to be used in committing another crime. This study has added to the argument by Yar (2005), as it has found that the vulnerability of computer systems in Nigeria was enabling cybercriminals to target individuals and organisations. The study has also contributed to RAT suitability of target as it found that the lack of awareness of a suitable target (i.e. humans) was a contributory factor to making an individual susceptible to becoming a target of an online crime. However, the finding also contributed to theory by contradicting RAT assumptions of the convergence of the three elements for crime to take place, by adding the presence of weak laws in a country as a factor in making a target suitable for a motivated offender.

Motivated Offender: Grabosky (2001) 'old wine in new bottles' assumptions about the motives of a cybercriminal as human factor to commit crime does not change. This study has contributed to Grabosky's (2001) assumption, as it has found that Nigerian cybercriminals are motivated by greed and the financial gain they can acquire in committing crime. The study contributed to RAT, by stating that high levels of poverty and unemployment among skilled youths in Nigeria are motivating factors for them to indulge in the activities of cybercrime.

Absence of a Capable Guardian: The policing of crime in both terrestrial and cyberspace has become a 'pluralistic endeavour' as responsibilities are shared between law enforcement officers, information security specialists and individual users (Grabosky, 2001). This study contributes to RAT, but expands the understanding of a capable guardian by including issues such as that inadequate funding and tools, training and education of law enforcement officers in Nigeria as rendering them unable to be capable guardians of potential victims of cybercriminal. Furthermore, the study contributes to RAT, by adding that the continuous evolution of technology has made law enforcement officers play 'catch up' to the criminals, while the borderless nature of cybercrime has made the application of laws and jurisdictions a

cumbersome issue for policing cybercrime in Nigeria. Table 9.1 summarises the theoretical contributions.

S/N	Contribution	Summary
1	**Theory contribution**	Extends the RAT understanding of suitable target, motivated offender and capable guardianship within the Nigerian and law enforcement context.

Table 9.1: Summary of Theoretical Contributions

9.4 Knowledge Contribution

This research investigation has contributed to the field of cybercrime policing of cyber-enabled crimes especially in Nigeria. The identification of the eleven themes which emerged from the findings of this study is a contribution as they form a conceptual framework, allowing for the understanding of the intricate relationships and associations between the various factors. Previous studies (Hassan et al., 2012; Maghairah, 2009 and Sesan et al., 2012) focused on some of these themes but the eleven themes have not been considered comprehensively. The identified themes provide a holistic framework for future research in cybercrime policing in Nigeria.

As the research investigation progressed, fifty-one sub-themes (Table 7.6) were developed, based on the eleven themes, specific to the field of cybercrime investigation and policing in Nigeria. This contribution provides an expanded understanding of cybercrime investigation from the scope of law enforcement which other members of the Cybercrime Advisory Council (CAC), such as the telecommunications and ICT regulators can adopt in order to improve on their mandate in tackling cybercrime. Therefore, the fifty-one emerging outcomes can be applied by policy makers and regulators in a practical sense, as they develop their own measures in curtailing the activities of cybercrime. The research has added a unique dimension to the policing knowledge by researching cybercrime in a Nigerian and Cybercrime Advisory Council context, rather than a generalisation of all the stakeholders. This was achieved by including five participants from members of the Cybercrime Advisory Council.

The development of the cybercrime investigation timeline in Nigeria (1990-2016) (Table 3.7 & Figure 3.2) is a contribution to knowledge as it identified and correlated all the variables involved in understanding the evolution of cybercrime investigation from 1990 to 2016. The

timeline serves as a novel contribution to current and future researchers in conducting studies of cybercrime in Nigeria. The current research adds to existing literature on the specific roles of members of the Cybercrime Advisory Council in tackling cybercrime in Nigeria (Figure 7.6). This is a major contribution as there are currently few or even no literature on the specific roles these participants play in tackling cybercrime in Nigeria. The current research also adds to existing knowledge on the benefits of the internal and external partnership (Figure 7.11) members of the CAC have amongst themselves and with external stakeholders. Furthermore, the measures (Figure 7.11) used by members of CAC to investigate and prosecute cybercrime is an addition to existing knowledge on the approaches used to deter activities of cybercriminals in Nigeria. Also, the current research contributes to knowledge as it has shown the different definitions of 'cybercrime' (Figure 7.7) by investigators, prosecutors, regulators and members of parliament. This adds to the literature on the definitions and categorizations' of cybercrime.

Finally, the study contributes to knowledge by making recommendations for (Figure 7.15) tackling cybercrime. The study extends the current literature by asserting that the education of law enforcement agencies and increased awareness of the public together can be a good approach in both crime control and crime prevention. Table 9.2 summarises the knowledge contributions

S/N	Contribution	Summary
1	**Knowledge contribution**	• Themes & emergent themes • Cybercrime investigation timeline • Nigerian context (LEA & CAC) • Specific roles in investigating cybercrime • Novel recommendations

Table 9.2: Summary of Knowledge Contributions

9.5 Practice and Policy Contribution

New insights from the current study regarding policy were raised in the research. The evidence suggested that the arrest and prosecution of criminals was not enough to serve as a deterrent to criminals. The issue of provision of education through specialised training of stakeholders involved in investigation, prosecution and prevention of cybercrime was greatly emphasised by the findings of the research. The improvement of the awareness level of

individuals and the general public in protecting themselves was recommended. Furthermore, some crucial issues were raised in the misapplication of one of the provisions of the Cybercrime Act (2015), namely 'Cyber-Stalking', in targeting freedom of speech in Nigeria. The provision of the law has been used to arrest and prosecute online bloggers who write about public officials. This was due to other evidence that suggested that the law needed significant improvement as it was passed into law without the participation of various stakeholders.

The current study appeals to practitioners in the law enforcement community. Forensic analysts, who stand as expert witnesses in a court of law, are responsible for presenting digitally retrieved evidence. They suggested that the forensic unit of organisations should be autonomous. This is so that the issue of the integrity of the evidence, due to tampering, would not be disputed in court during cross-examination. Also, the forensic analyst argued that due to the workload and outdated computer systems, it was affecting the progress and quality of cybercrime investigation in Nigeria. Their suggestion would assist policy makers and managers in either increasing the workforce of skilled staff or procuring sophisticated systems that are capable of producing quality end results of a cybercrime investigation. The study also showed that the inadequate training of judges and investigators is negatively impacting on the enforcement of the Cybercrime Act (2013). Evidence suggested that, investigators needed more training than prosecutors and analysts as they were responsible in the beginning of any cybercrime investigation. Finally, the evidence suggested that there should only be one organisation namely the Office of the National Security Advisor (ONSA) to coordinate between the public and private sector. Currently, all organisations coordinate with other stakeholders without a central authority even though the provision of the Cybercrime Act (2015) stipulates the ONSA as the central authority. This suggestion when implemented would effectively improve synergy between the public and private sector. Table 9.3 summarises the practical policy contributions

S/N	Contribution	Summary
1	**Practical and policy contribution**	• Review and misapplication of laws • Central coordination of efforts • Autonomous and upgraded forensic lab • Training for judges & investigators

Table 9.3: Summary of Practice & Policy Contributions

9.6 Research Evaluation

As discussed in Chapter 5 (Section 5.15), the research integrity was maintained by adhering to the seven principles set out by Klein and Myers' (1999) that are used in evaluating an interpretivist field research. Table 9.4 summarises the principles and reflection in the research.

S/N	Principles for Interpretive Field Research	Reflection in Current Research
1	**Hermeneutic Circle:** The principle suggests that all human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form.	Data analysis process was an iterative process as the data gathered were read multiple times in order to make the right correlation and meaning of the whole problem.
2	**Principle of Contextualisation:** Requires critical reflection of the social and historical background of the research setting in order for the intended audience to see how the current situation under investigation emerged.	This principle was achieved by a detailed research context chapter (Chapter 2) that gives an overview of the research topic within the Nigerian and law enforcement context in understanding cybercrime.
3	**Principle of Interaction between the Researcher and the Subject:** This principle requires critical reflection on how the research materials were socially constructed through the interaction between the researchers and participants.	In the current study, the researcher avoided presenting preconceptions to the respondents. Interview participation was voluntary and in order to avoid bias throughout the data collection process, a detailed description of the data collection process and the analysis was documented to minimise this.
4	**Principle of Abstraction and Generalisation:** This principle requires relating the idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action.	A detailed description and illustration of interviewee statement were categorised. The principle of generalization is met through discussion of the research results in relation to the ideas and concepts originating in previous research papers, thus, the research results will apply to multiple situations.
5	**Dialogical reasoning principle:** Requires sensitivity to possible contradictions between the theoretical preconceptions guiding the research design and actual findings with subsequent cycles of revision	The researcher's background, assumptions and experience was well documented (Section 5.17). Also, the researcher explained in detail philosophical approach, literature and a concise explanation of the data analysis and coding process to make it transparent.
6	**Principle of Multiple Interpretations:** Requires sensitivity to possible differences in interpretations among the participants as are typically expressed in multiple narratives or stories of the same sequence of events under study.	Multiple interpretations were detailed in the analysis chapter. Interview transcript were analysed iteratively following the interviews.
7	**Principle of Suspicion:** Requires sensitivity to possible 'biases' and systematic 'distortions' in the narratives collected from the participants.	The main aim was to avoid possible biases. This was done by collecting and analysis data from different sources. The researcher's background was documented in *section 5.17*. Description of data collection and analysis process in detail guided the researcher in avoiding biases.

Table 9.4: Research Evaluation Summary

9.7 Research Limitations

There are limitations within all research investigations. Even though, careful consideration was put in the design, data collection and analysis stages of this research study, there are some overall limitations. The limitations are categorised as follows:

Theoretical Limitation: This theoretical framework of this research was limited to only one criminological theory of Routine Activity Theory. Other theories such as General Deterrence Theory and General Theory of Crime were considered and reviewed in Chapter 5: Theoretical Framework but not used in this study.

Methodological Limitation: The research was limited to an interpretivist paradigm with a relativist philosophical assumption. The research approach was inductive and strictly qualitative through the collection of data through interview and documentation. However, the research limited the use of NVivo to organising findings, while manual coding was also used. The interviews occurred as a longitudinal; however, a cross-sectional study may have produced different outcomes

Research Scope Limitation: The scope of the research was limited to activities of law enforcement agencies especially the Economic and Financial Crimes Commission as a member of the Cybercrime Advisory Council. The research is also limited to specifically cyber-enabled crime of advance fee fraud.

Research Context Limitation: The research context is focused primarily in Nigeria with most of the participants from the law enforcement community. However, two of the participants are from the UK.

Logistical Limitations: Though, the intention of the researcher was to conduct mixed methods research with qualitative data from the law enforcement agencies and quantitative data from the public, due to logistical constraints, the research was limited to a qualitative approach.

Accessibility Limitations: The research had limitations in collecting data from some stakeholders especially the Judges due to their tight schedules. Also, the research was limited to the number of participants from the UK, therefore, the research context was mainly based in Nigeria.

9.8 Future Research

The future research potential in cybercrime is varied and diverse. This is due to the evolution of technology and crime itself. Since this research was limited by its scope, context and other limitations enumerated above, future research could be conducted based on the following categorisations:

Context: The context of the research could be extended to further investigations of cybersecurity in the UK to examine how the law enforcement agencies are tackling cybercrime. A comparative analysis of different stakeholders could be done to understand their respective roles in fighting cybercrime.

Topology of Crime: Research on a different variant of crime such as online grooming or cyber-terrorism could be done to find out what challenges are faced by cyber security professionals.

Scope: Research on the victims of cybercrime rather than of law enforcement agencies could be done to find out their perceptions about the activities of both cybercriminals and police officers. This could be done through survey and interviews or focus groups and the richness of the data could be used to support this current research study.

Theory: Future research could use General Deterrence Theory to find out whether the laws used in penalising cybercriminals is a deterrent to criminals. Future research could also apply Routine Activity Theory to another form of cybercrime such as cyberstalking or cyberbullying as these are traditional crimes which are further enabled by technology.

9.9 Conclusion

In conclusion, this chapter summarises the research study and presents the theoretical, knowledge, practical and policy contributions of the research. Furthermore, a detailed explanation is provided for the research evaluation. Finally, the limitations of the research are enumerated and potential subject matters for future research were identified.

REFERENCES

Abdulfatai, B. (2017). *Legislative Commitment and Cybercrime in Nigeria*. Paper presented at the Law Week of Faculty of Law of Lead City University Ibadan. Retrieved from http://nationalinsightnews.com/2017/03/08/legislative-commitment-cyber-crime-nigeria-sen-fatai-buhari-ph-d/

Abdullahi, R., Mansor, N. (2015). Concomitant Debacle of Fraud Incidences in the Nigeria Public Sector: Understanding the power of Fraud Triangle Theory. *International Journal of Academic Research in Business and Social Sciences,* 5(5), 312-326

Abubakar, A.S (2009) *Investigating Fraud Schemes in Nigeria.* Paper presented at International Conference on Cooperation against Cybercrime. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2643

Adams, P. (1998). Network topologies and virtual place. *Annals of the Association of American Geographers*, 88, 88-106

Adaramola, Z. (2015). Nigeria's cybercrime law and its 'loopholes'. *Daily Trust.* Retrieved 29 November, 2017, from https://www.dailytrust.com.ng/news/it-world/nigeria-s-cybercrime-law-and-its-loopholes/110593.html

Advance Fee Fraud and other Fraud Related Offences (AFF) Act 2006

Adebusuyi, A. (2008) "The Internet and Emergence of Yahoo Boys Sub culture in Nigeria", International Journal of Cyber Criminology Vol. 2(2) 368- 381.

Adesina, O.S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science* 13 (4)

Adesulu, D. (2017). Greed, cause of cybercrime – Don. *Vanguard News.* Retrieved 30 November, 2017 from https://www.vanguardngr.com/2017/06/greed-cause-cyber-crime-don/

Adomi, E., Igun, S. (2008) 'Combating cybercrime in Nigeria'. The Electronic Library 26 (5), 716-725

African Union (2014). African Union Convention on Cyber Security and Personal Data Protection. Retrieved 30 November, 2017, from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Aibieyi, S., Oyemwinmina, C. (2016). Analysis towards Effective Policing in Nigeria. *African Research Review*. Vol. 10(1), 61-72

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

Ajayi, G.O. (2003). NITDA and ICT in Nigeria. Retrieved from https://tpa.abu.edu.ng/www.devcomlibrary.com/Articles%20folder/ICT%20in%20Nigeria-Ajayi.pdf

Ajayi, O. (2011). An Overview of Salient provisions in the Evidence Act 2011. Retrieved from

http://www.olaniwunajayi.net/clientalert/Overview%20of%20the%20Evidence%20Act%202011.pdf

Ajers, R.L., Sellers, C.S. (2004). *Criminological theories: Introduction, evaluation and application*. 4th Ediction. Los Angeles: CA: Roxbury

Akintoye, O. (2008). EFCC is out to arrest internet fraudsters. *The Nation.* Retrieved from http://www.thenationonlineng.net/archive2/tblnews_Detail.php?id=66624

Alamika, E.E.O., Chukwuma, I.C. (2003). Analysis of Police and Policing in Nigeria. Retrieved 10 October, 2017, from, http://www.cleen.org/policing.%20driver%20of%20change.pdf

Alkaabi, A.O.S. (2010). *Combating Computer Crime: An International Perspective*. (PhD Thesis), Queensland University of Technology, Queensland. Retrieved from http://eprints.qut.edu.au/43400/

Aloul, F.A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology,* 3(3), 176-183

Arksey, H., Knight, P. (1999). *Interviewing for Social Scientists.* London: Sage

Babafemi, F. (2011). Placing EFCC mandate in proper perspectives. *Daily Trust.* Retrieved from http://www.dailytrust.com.ng/sunday/index.php/comment-debate/6126-placing-efcc-mandate-in-proper-perspectives

Baker, T.L. (1994). *Doing Social research. 2nd Edn.* New York: McGraw-Hill Inc.

Bansal, P., Corley, K. (2011). The coming age of qualitative research: Embracing the diversity of qualitative methods. *Academy of Management Review,54(2), 233-237*

Barnard, J. (2014, 12 November). Global economy loses $445 to cybercriminals a year; now they are gunning for Africa's easy money. *Mail & Guardian.* Retrieved from http://mgafrica.com/article/2014-11-12-global-economy-loses-445bn-to-cyber-criminals-a-year-now-they-are-gunning-for-africas-easy-money

Basit, T. H. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational Research, 45*(2), 145-154.

Barej, A (2017). Boost police budget to tackle cyber crime, says Reform. *Public Finance.* Retrieved 10 September, 2017 from http://www.publicfinance.co.uk/news/2017/08/boost-police-budget-tackle-cyber-crime-says-reform

Bazeley, P. (2007). *Qualitative data analysis with NVivo*. Los Angeles, Calif. ; London : SAGE.

BBC. (2009). Nigeria in big scamster crackdown. Retrieved from http://news.bbc.co.uk/1/hi/world/africa/8322316.stm

BBC. (2013). National Audit warns UK needs more skilled cyber-crime fighters. Retrieved 30 November, 2017, from http://www.bbc.co.uk/news/uk-politics-21414831

Bell, E., Bryman, A. (2007). The ethics of management research: An exploratory content analysis. *British Journal of Management*, 18(1), 63-77.

Bendiek, A., Metzger, T. (2015). Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review. *German Institute for International and Security Affairs.* Retrieved 30 December, 2017, from https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Bennett, R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces*, 70, 147-63

Binns, C. (2017). Law Enforcement Partnership Enhance Cybercrime Investigations. *PA Times.* Retrieved 20 November, 2017, from https://patimes.org/law-enforcement-partnerships-enhance-cybercrime-investigations/

Blaikie N. (2010) *Designing Social Research* (2nd ed.) Cambridge: Polity.

Blumberg, B., Cooper, D.R., Schindler, P.S. (2011) *Business Research Methods.* London: McGraw-Hill Education

Bossler, A.M., Holt, T.J. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behaviour*, 35:1, 20-40

Bossler, A.M., Holt, T.J. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, 30:1, 1-25

Boyatzis, R.E. (1998). *Transforming qualitative information: thematic analysis and code development.* London, & New Delhi: SAGE Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3* (2), 77-101.

Brenner, S. (2007). *Law in an Era of Smart Technology.* Oxford: Oxford University Press

Bringer, J. D., Johnston, L. D., & Brackenridge, C. D. (2004). Maximising transparency in a doctorial thesis; the complexities of writing about the use of QSR*NVIVO within a grounded theory study. *Qualitative Research, 4* (2), 247-265.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of police Strategies and Management,* Vol. 29(3), 408-433

Bryman, A. (1988). *Quantity and Quality in Social Research.* London: Routledge

Bryman, A., & Bell, E. (2015). *Business Research Methods* (4th ed.). New York: Oxford University Press.

Bryman, A., & Bell, E. (2007*). Business Research Methods* (2nd ed.). New York: Oxford University Press.

Buchanan, J., & Jones, M. (2010) The efficacy of utilising Nvivo for interview data from the electronic gaming industry into two jurisdictions. *Review of Management Innovation and Creativity, 3* (5), 1-15.

Budding, T., & Cools, M. (2008). Using computer software to analyze qualitative data: Accounting versus other disciplines.

Buerger, M.E., Gartin, P.R., Sherman, L.W. (1989). Hot Spots of Predatory Crime: Routine Activities and the Criminology of Place. *Criminology*, Vol. 27(1), 27-55.

Buono, L. (2010). Investigating and prosecuting crimes in cyberspace: European training schemes for judges and prosecutors. *ERA Forum*, 11, 207-218

Burke, R.H. (2009). *An Introduction to Criminological Theory*. 3rd Edition. London: Routledge.

Cabinet Office. (2016). *The UK Cyber Security Strategy 2011-2016 Annual Report*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

CDT (2011). International Issues: Cybercrime. Retrieved 10 December, 2017, from https://cdt.org/insight/international-issues-cybercrime/

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social Legal Studies, 10, 229-242*

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis.* Thousand Oaks, California: Sage Publishers.

Chatham House (2006). *Nigeria-Related Financial Crime and its Links with Britain*. London: The Royal Institute of International Affairs

Chawki, M., Darwish, A., Khan, M.A., Tyagi, S. (2015). 419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria. *Studies in Computational Intelligence, 593, 129-144*

Christou, G. (2017). The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities.* Retrieved 20 December, 2017, from http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf

Clarke, R.V. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research*, 10, 55-63.

Clarke, R.V., Felson, M. (2008). *Routine Activity and Rational Choice.* New Jersey: Transaction Publishers

Clarke, R.V., Felson, M. (1979). Opportunity makes the thief: Oractical theory for crime prevention. *Policing and Reducing Crime Unit: Research, Development and Statistics Directorate, 98, 1-36*

Clarke, R.V., Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 52, 170-183

Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press

Clough, P., Nutbrown, C. (2012) *A Student's Guide to Methodology* (3rd ed.). London: Hutchinson

Choo, K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 30(2011), 719-731

Cobb, S. (2016). *Mind this gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a critical analysis.* Paper presented at Virus Bulletin Conference, USA. Retrieved from https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf

Cohen, L.E., Felson, M.K. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44(4), 588-608.*

Coffey, A., & Atkinson, P. (1996). *Making sense of qualitative data*. London: Sage Publishers.

Collis, J. & Hussey, R. (2003). *Business research: a practical guide for undergraduate and postgraduate students* (2nd ed.). New York: Palgrave McMillan

Collis, J. & Hussey, R. (2009). *Business research: a practical guide for undergraduate and postgraduate students* (3rd ed.). New York: Palgrave McMillan.

Collis, J. & Hussey, R. (2014). *Business research: a practical guide for undergraduate and postgraduate students* (4th ed.). New York: Palgrave McMillan.

Collins, H. (2010). *Creative research: the theory and practice of research for the creative industries*. London: AVA Publishers.

Computer Misuse Act 1990

Council of Europe. (2017). *Nigeria: Cybercrime policies and strategies.* Retrieved from https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/nigeria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=hu_HU

Council of Europe (2001). *Convention on Cybercrime.* Retrieved 10 January, 2016, from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Council of Europe (2018). *Charts of signatories and ratifications of Treaty 185*. Retrieved 10 January, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=false

Corbetta, P. (2003). *Social research: theory, methods and techniques*. London: Sage Publishers

Cornish, D. and Clarke, R. (1986). The reasoning criminal: Rational choice perspectives on offending New York: Springer-Verlag.

Cornish, D. and Clarke, R. (1987). 'Understanding crime displacement: An application of rational choice theory.' Criminology, 25(4), 933-947.

Council of Europe. (2001). Convention on Cybercrime CETS No: 185. Retrieved 13 June, 2015, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Criminal Code Act (1990).

Creswell, J.W. (2014) *Research Design* (4th ed.). CA: Thousand Oaks

Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage.

Cross, C., Blackshaw, D. (2014). Improving the Police Response to Online Fraud. *A Journal of Policy and Practice 9 (2), 119-128.*

Crotty, M. (1998). *The foundations of social research: the meaning and perspective in the research process*. London: Sage Publishers.

Cybercrime Prohibition, Prevention Act 2015.

Cyber Sphere (2017). First Plenary Conference. Retrieved from https://www.ictcybersecurityweek.com/

Dalton, W. (2012). Cyber-crime policing completely inadequate, says ex-Scotland Yard detective. *IT Propotal.* Retrieved 15 November, 2017, from https://www.itproportal.com/2012/11/22/cyber-crime-policing-completely-inadequate-says-ex-scotland-yard-detective/

Daniel, S. (2013, 20 June). How EFCC uses mobile phones to get evidence. *Vanguard*. Retrieved from http://www.vanguardngr.com/2013/06/how-efcc-uses-mobile-phones-to-get-evidence/

Data Protection Act 1998

Dembowski, S., Hanmer-Lloyd, S. (1995). Computer applications – A new road to qualitative data analysis. *European Journal of Marketing*, 29(11), 50-62.

Denzin, N., & Lincoln, Y. (2000). The discipline and practice of qualitative research. In *Handbook of qualitative research.* (2nd ed., pp. 1–28). Thousand Oaks, CA: Sage.

Denzin, N. K., & Lincoln, Y. S. (2003). The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.). *The Sage Handbook of Qualitative Research* (4th ed.). London: Sage

Denzin, N. K., & Lincoln, Y. S. (2011). Introduction: The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.). *Collecting and interpreting qualitative materials* (2nd ed.). Thousand Oaks, California: Sage Publishers.

Dix, R.B. (2017). 5 Strategies for addressing cybercrime. *GCN*. Retrieved 10 March, 2017,

from https://gcn.com/articles/2017/01/11/strategies-addressing-cybercrime.aspx

Dotzauer, E. (2014). African Union Convention on Cyber Security and Personal Data Protection. Retrieved 30 October, 2017, from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/african-union-convention-cyber-security-and-personal-data-protection-0

Drinkwater, Doug. (2015). FBI, Europol and NVA want global approach to fight cyber-crime. *SC Magazine.* Retrieved from http://www.scmagazineuk.com/fbi-europol-and-nca-want-global-approach-to-fight-cyber-crime/article/418365/

Easterby-Smith, M., Thorpe, R., & Lowe, A. (2008). *Management research: theory and practice* (3rd ed.). London: Sage Publishers.

Economic and Financial Crimes Commission Establishment (EFCC) Act 2004

Economic and Financial Crimes Commission – EFCC (2009). *EFCC, Microsoft Sign MOU to Curb Internet Crime, Piracy* Retrieved 10 June, 2015, from http://www.efccnigeria.org/jm15/index.php/information-center/news/613-efcc-microsoft-sign-mou-to-curb-internet-crime-piracy

Economic and Financial Crimes Commission EFCC (2012). *2012 Annual Report.* Abuja: Sidwell Productions.

Economic and Financial Crimes Commission EFCC (2013). *2013 Annual Report.* Abuja: Sidwell Productions.

Economic and Financial Crimes Commission EFCC (2014). *2014 Annual Report.* Abuja: Sidwell Productions.

Economic and Financial Crimes Commission EFCC (2015). *Red Alert on Scams.* Abuja: Sidwell Productions.

Economic and Financial Crimes Commission EFCC (2016). *100 Frequently Asked Questions About the EFCC. Abuja: Sidwell Productions*

Economic and Financial Crimes Commission EFCC (2017). *Wikipedia.* Retrieved 10 December, 2017, from, https://en.wikipedia.org/wiki/Economic_and_Financial_Crimes_Commission

Ehimen, O.R., Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal, 3(1), 93-97.*

Eisenhardt, K.M. (1989). Building theories from case study research. *Academy of Management Review, 14(4), 532-50.*

Elebeke, E. (2015). Why is UK prosecuting war against cybercrime in Nigeria. *Vanguard.* Retrieved 27 April, 2017, from https://www.vanguardngr.com/2015/12/why-uk-is-prosecuting-war-against-cybercrime-in-nigeria/

Evidence Act (As Amended) 2011.

Eyitemi, M. (2011). Regulation of Cybercafes in Nigeria. *Information Resource Management Association, doi: http://www.irma-international.org/viewtitle/45411/*

Ezeoha, A,E. (2006). Regulating Internet Banking in Nigeria: Some Success Prescriptions – Part 2. *Journal of Internet Banking and Commerce, 11(1)*

Fabi, R. (2009). Nigeria, software firms to halt Internet crime. *Reuters.* Retrieved from http://af.reuters.com/article/topNews/idAFJOE59M0AH20091023

Felson, M. (1998). *Crime and everyday life,* 2nd Edn. Thousand Oaks, CA: Pine Forge Press.

Flanagan, Anne. (2005). The Law and computer crime: Reading the Script of Reform. *International Journal of Law and Information Technology, 13(1), 98-117.*

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law and Security Review,* 26, 298-303

Gilbert, L.S. (2002). Going the distance: Closeness in qualitative data analysis software. *International Journal of Social Research Methodology*, 5(3), 215-228

Gill, J., Johnson, P. (2010). *Research Methods for Managers* (4th ed.). California: SAGE

Gomm, R. (2009). *Key Concepts in Social Research Methods.* Stroud: Palgrave MacM.

Gottfredson, M., Hirschi, T. (1989). A propernsity-event theory of crime. *In Advances in criminological theory,*Vol. 1,eds. W. Laufer and F. Adler. New Brunswick, NJ: Transaction Publishers

Gottfredson, M., Hirschi, T. (1990). *A general theory of crime.* Stanford, CA: Stanford University Press

Grabosky, P. (2001). Virtual criminality: Old Wine in New Bottle. *Social and Legal Studies,* 10(2), 243-249

Grabosky, P., Broadhurst, R. (2015). *The future of cyber-crime in Asia.* University of Hong King Press: Hong Kong

Hakmeh, J. (2017). Building a Stronger International Legal Framework on Cybercrime. *Chatham House.* Retrieved 30 November, 2017, from, https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime?gclid=EAIaIQobChMIiZW82tu52AIViRbTCh3e5Qj-EAAYASAAEgJXm_D_BwE

Halfpenny, P. (1979). The Analysis of Qualitative Data. *Sociological Review, 27, 799-825*

Hammersley, M. (1992). *Deconstructing the Qualitative-Quantitative Divide,* in Hammersley, What's Wrong with Ethnography. London: Routledge

Hammersley, M. (2013). An outline of methodological approaches. Retrieved from June 15th, 2015 from http://www.tlrp.org/capacity/rm/wt/hammersley/hammersley4.html

Hardy, M., Bryman, A. (2004). *Introduction: Common Threads among Techniques of Data Analysis.* In M.Hardy and A.Bryman(eds), Handbook of Data Analysis. London: Sage

Hassan, A.B., Lass, F.D., Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology,* 2(7), 626-631.

Hayward, K. (2007). Situational Crime Prevention and its Discontents: Rational Choice Theory versus the 'Culture of Now'. *Social, Policy and Administration,* Vol. 41 (3), 232-250

Holt, T.J. (2013). *Cybercrime and Criminological Theory: Fundamental Reading on Hacking, Piracy, Theft and Harassment.* First Edition. San Diego: Cognella.

Holtfreter, K., Pratt, T.C., Reisig, M.D. (2010). Routine Online Activty and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267-296.

Huczynski, A., & Buchanana, D. (2007). *Organizational behavior: an introductory text.* London: Financial Times Prentice Hill.

Hundley, V., Teijlingen, E.R. (2001). The importance of pilot studies. Sociology at Surrey. Retrieved 30 November, 2017, from http://aura.abdn.ac.uk/bitstream/handle/2164/157/SRU35%20pilot%20studies.pdf?sequence=1&isAllowed=y

Hinton, P. (2012). Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. *Public Money and Management,* 32(3), 225-232

Internet Crime Complaint Center (2010). 2010 Internet Crime Report. Retrieved 23 July, 2016, from https://pdf.ic3.gov/2010_IC3Report.pdf

Internet Crime Complaint Center (2014). 2014 Internet Crime Report. Retrieved 23 July, 2016, from https://pdf.ic3.gov/2014_IC3Report.pdf

International Compliance Association ICA (2017). What is Financial Crime? Retrieved 28 December, 2017, from, https://www.int-comp.org/careers/a-career-in-financial-crime-prevention/what-is-financial-crime/

Internet World Stats (2017). Africa. Retrieved 2 January, 2018, from http://www.internetworldstats.com/africa.htm

Internet World Stats (2016). Top 20 Countries with the Highest Number of Internet Users. Retrieved 23 July, 2016 from http://www.internetworldstats.com/top20.htm

ITU (2012). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved 20 July, 2016 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Jacinta, O.J. (2017). The Rapid Growth of Internet Fraud in Nigeria, Causes, Effect and Solution. *Inner Temple OOU*. Retrieved 30 December, 2017 from https://innertempleoou.wordpress.com/2017/03/07/the-rapid-growth-of-internet-fraud-in-nigeria-cause-effect-and-solution-by-nweke-oluchi-jacinta/

Johnson, P., & Clark, M. (2006). Editors introduction: mapping the terrain: an overview of business and management research methodologies. In P. Johnson & M. Clark (eds.). *Business and Management Research Methodologies*. London: Sage, pp. xxv-lv.

Jones, D. W. (2008) Understanding criminal behaviour: Psychosocial approaches to criminality. Devon: Willan Publishing.

Jones, H. (2017). Cybercrimes reach epidemic proportions as fraud becomes most common crime in UK. *Express.* Retrieved 30 October, 2017, from https://www.express.co.uk/finance/personalfinance/846157/Cyber-crime-epidemic-fraud-UK

Kafoi, S. (2016). Nigeria Cybercrime Act 'weighs down Federal High Court'. *Technology Times.* Retrieved 30 December, 2017, from http://technologytimes.ng/nigeria-cybercrime-act-weighs-down-federal-high-court/

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–93.

Kortjan, N., Solms, R.V. (2014). A conceptual framework for cyber-security awareness and education in Nigeria. *SACJ*, 52, 29-41

Kshetri, Nir (2015). India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership. *IEEE Security and Privacy, 16-23*

Kuhn, T. S. (1962). *The structure of scientific revolution*. Chicago, IL: University of Chicago Press.

Kumar, R. (1999). *Research Methodology: A Step-By-Step Guide for Beginners.* London: Sage Publications.

Ladan, M.T. (2015). Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria. Retrieved from http://dx.doi.org/10.2139/ssrn.2680299

Lee, B. (2012). *Using documents in organizational research, in G. Symon and C. Cassell (eds) Qualitative Organizational Research Core Methods and Current Challenges*. London: Sage

Li, X. (2007). International Action against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*,4(3)

Longe, O., Mbarika, V., Ngwa, O., Wada, F. (2009). Crimincal Uses of Information and Communications Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact, Vol. 9 (3), 155-172*

Lopez, A. (2014). Routine Activity Theory of Crime. Retrieved 30 November, 2017, from http://lemoncenter.com/routine-activity-theory-elements-crime

Lyles, M.A., Salk, J.A. (1996). Knowledge acquisition from foreign parents in international joint ventures: an empirical examination in the Hungarian context. *Journal of International Business Studies, Special Issue, 27, 877-903*

Magnin, C.J. (2001). *The 2001 Council of Europe Convention on cybercrime: an efficient tool to fight crime in cyber space?* (MSc Thesis), Santa Clara University, Santa Clara. Retrieved from http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf

Maghaireh, A.M.S. (2009). *Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence.* (PhD Thesis), University of Wollongong. Retrieved from http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses

Malgwi, C.A. (2005). Fraud as Economic Terrorism: The Efficacy of the Nigerian Economic and Financial Crimes Commission. *Journal of Financial Crime, Vol. 12(2), 144-164*

Maier, B. (2010). How has the Law Attempted to Tackle the Borderless Nature of the Internet? *International Journal of Law and Information Technology, 18(2), 142-175*

Marsh, I., Melvile, G., Morgan, K., Norris, G., Walkington, Z. (2006). *Theories of crime. London: Routledge.*

Maxwell, J. A. (2005). Qualitative research design: an interactive approach. Thousand Oaks, California, Sage Publications.

Mertens, D. M. (2009). *Transformative research and evaluation*. New York: Guilford.

McCracken, G. (1998). *The long interview*. London: Sage Publishers.

McConnell (2000). Cybercrime and Punishment? Archaic Laws Threaten Global Information. Retrieved from http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

McGuire, M., Dowling, S. (2013a). Cyber-dependent crimes. *Cybercrime: A review of the evidence*

McGuire, M., Dowling, S. (2013b). Cyber-enabled crimes – fraud and theft. *Cybercrime: A review of the evidence*

McQuade, S.C. (2006). *Understanding and Managing Cybercrime.* New York: Allyn and Bacon.

Mertens, D. M. (2003). Mixed methods and the politics of human research: the transformative-emancipatory perspective. In A. Tashakkori & C. Teddlie (eds.). *Handbook of mixed methods in social and behavioural research* (pp.135-164). Thousand Oaks, CA: Sage Publishers.

Mertens, D. M. (2010). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods* (3rd ed.). Thousand Oaks, CA: Sage

Miles, M.B., Huberman, A.M. (1984). *Qualitative Data Analysis: A Sourcebook of New Methods.* (3rd ed.). California: Sage Publications.

Miles, M., & Huberman, A. (1994). *An expanded sourcebook: qualitative data analysis* (2nd ed.). London: Sage Publishers.

Miles, M.B., Huberman, A.M. (2014). *Qualitative Data Analysis: A Methods Sourcebook.* Beverly Hills: Sage Publications.

Money Laundering (Prohibition) Act 2012.

Money Laundering (Prohibition) (Amendment) Act 2012.

Morgan, D. (2007). Paradigms lost and pragmatism regained. *Journal of Mixed Methods Research, 1*, 48-76.

Morse, J.M. (1994) *Emerging From the Data: The Cognitive Processes of Analysis in Qualitative Inquiry*. In Morse, J.M. (e.d.) *Critical Issues in Qualitative Research Methods.* Thousand Oaks: Sage

Myers, M. D. (2013). *Qualitative research in business and management*. Sage.

National Assembly of Nigeria (2017a). *About the Senate.* Retrieved from http://www.nassnig.org/page/about-the-senate

National Assembly of Nigeria (2017b). *Constitution of the Federal Republic of Nigeria 1999.* Retrieved from http://www.nassnig.org/document/download/5820

National Assembly of Nigeria (2017c). NASS. Retrieved 30 December, 2017 from http://www.abuja-ng.com/NASS-ABUJA.html

National Crime Agency (NCA) (2017a). *National Cyber Crime Unit.* Retrieved from http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

National Crime Agency (NCA) (2017b). *What we do.* Retrieved from http://www.nationalcrimeagency.gov.uk/about-us/what-we-do

National Information Technology Development Agency (2018). *Common Wealth Network.* Retrieved 03 January, 2018, from http://www.commonwealthofnations.org/partner/national-information-technology-development-agency/

National Information Technology Development Agency NITDA Act (2007. Retrieved 20 November, 2017, from http://www.nassnig.org/document/download/5940

National Information Technology Development Agency (2017a). *About NITDA.* https://nitda.gov.ng/about-nitda/

National Information Technology Development Agency (2017b). *Mandate.* Retrieved from *https://nitda.gov.ng/mandate/*

National Population Commission (NPC) (2017). 2006 PHC Priority Tables. Retrieved 30 November, 2017, from http://population.gov.ng/core-activities/surveys/dataset/2006-phc-priority-tables/

National Security Advisor (Nigeria) (2017). *Wikipedia.* Retrieved 29 December, 2017, from https://en.wikipedia.org/wiki/National_Security_Advisor_(Nigeria)

National Security Agencies (1986) Act. Retrieved 20 November, 2017, from http://lawsofnigeria.placng.org/print.php?sn=336

NHTCU/NOP (2002). Hi-tech crime: The impact on UK business. London: NHTCU

Nigerian Communications (2013) Act. Retrieved 20 November, 2017, from https://www.ncc.gov.ng/data/html/NCA2003.html?ml=1

Nigerian Communications Commission (NCC) (2017a). *About the NCC.* Retrieved from https://www.ncc.gov.ng/about-ncc/who-we-are

Nigerian Communications Commission (NCC) (2017b). *Mandate of the NCC.* Retrieved from *https://www.ncc.gov.ng/about-ncc/mandate*

Nigerian Communications Commission (NCC) (2016). *Subscriber Statistics.* Retrieved from http://www.ncc.gov.ng/index.php/2015-10-12-15-28-34/statistics-reports/subscriber-data#quarterly-subscriber-operator-data

Nigeria. Economic and Financial Crimes Commission. (2015). *Landmark Achievements in the Fight against Economic and Financial Crimes 2012-2015. Abuja: Siddwell Production*

Nigerian Financial Intelligence Unit (2015). *About NFIU.* Retrieved 6 April, 2016, from http://www.nfiu.gov.ng/index.php/nfiu#_ftnref1

Nigeria Inter-Bank Settlement System. (2014). 2014 E-Payment Fraud Landscape in Nigeria. Retrieved from http://www.nibss-plc.com.ng/wp-content/uploads/2015/03/Fraud-Landscape-2014.pdf

Nigerian Police Force (2017a). *Vision and Mission.* Retrieved 30 November, 2017, from, http://www.npf.gov.ng/vision_mission.php

Nigerian Police Force (2017b). *Wikipedia.* Retrieved 30 November, 2017, from, https://en.wikipedia.org/wiki/Nigeria_Police_Force

Nigeria – The 419 Coalition Website. Retrieved 30 July, 2016 from http://www.419coalition.org/

NgCERT (2014a). *National Cyber Security Policy*. Retrieved from https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf

NgCERT (2014b). *National Cybersecurity Strategy.* Retrieved from https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf

Nkanga, P. (2016). How Nigeria's cybercrime law is being used to try to muzzle the press. *Committee to Protect Journalists.* Retrieved 25 November, 2017, from https://cpj.org/blog/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t.php

Oates, B.J. (2012). *Researching Information Systems and Computing.* Los Angeles: Sage.

Obuah, E. (2010). Combatting Corruption in Nigeria: The Nigerian Economic and Financial Crimes (EFCC). African Studies Quarterly, 12 (1)

Odekunle, F. (1986). The legal order, crime and crime control in Nigeria: Demystification of flase appearances. *Nigerian Journal of Policy and Strategy*, 1, 78-100

Odumesi, J.O. (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja. Nigeria

Oke, O.O. (2015). An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act 2015. *Social Sciences Research Network.* doi: http://dx.doi.org/10.2139/ssrn.2655593

Okeshola, F.B., Adete, A.K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3(9), 98-114.*

Oladipo, D. (2012). Undergraduate jailed for cyber fraud inside senator's café. *The Eagle Online.* Retrieved from http://theeagleonline.com.ng/undergraduate-jailed-for-cyber-fraud-inside-senator-s-cafe/

Olayemi, O.J. (2014a). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology,* 6(3), 116-125.

Olayemi, O.J. (2014b). Combating the Menace of Cybercrime. *International Journal of computer Science and Mobile Computing,* 3(6), 980-991.

O'Leary, Z. (2007). *The social science jargon buster: the key terms you need to know.* London: Sage Publishers.

Olowu, D (2009) Cybercrimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa" Journal of Information, Law and Technology (1) 1- 18

Olusola, M., Samson, O., Semiu, A., Yinka, A. (2013a). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science,* 2(4), 45-51.

Olusola, M., Samson, O., Semiu, A., Yinka, A. (2013b). Cyber Crimes and Cyber Laws in Nigeria. *The International Journal of Engineering and Science,* 2(4), 19-25

Omotor, D.G. (2009). Socio-Economic Determinants of Crime in Nigeria. *Pakistan Journal of Social Sciences, 6 (2), 54-59*

Onyeozeli, E.C. (2005). Obstacles to Effective Policing in Nigeria. *African Journal of Criminology and Justice Studies,* Vol. 1(1), 32 - 53

Oremewe, I. (2011). What's New about the 21011 Evidence Act 2011. Retrieved from http://dx.doi.org/10.2139/ssrn.2111157

Oriola, T.A. (2005). Advance fee fraud on the Internet: Nigeria's regulatory response. *Computer Law & Security Report,* 2005 (21), 237-248.

Ozeren, S. (2005). *Global Response to Cyberterrorism and Cybercrime: A Matrix for International Cooperation and Vulnerability Assessment.* (PhD Thesis), University of North Texas, Texas. Retrieved from http://nsl.cse.unt.edu/cae/attachments/Ozerendissertation.pdf

Paradigm Initiative Nigeria (2013a). Economic Cost of Cybercrime in Nigeria. Retrieved 10 June, 2015, from https://pinigeria.org/downloads/research-reports/

Paradigm Initiative Nigeria (2013b). Nigeria: Making a Case for Enduring Internet Freedom. Retrieved 10 June, 2015, from https://pinigeria.org/downloads/research-reports/

Paradigm Initiative Nigeria (2014). Cybersecurity in Nigeria: Need for a Paradigm Shift. Retrieved 10 June, 2015, from https://pinigeria.org/downloads/research-reports/

Patton, M. (1990). *Qualitative evaluation and research methods*. Beverly Hills, CA: Sage Publishers.

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, California: Sage Publishers.

Paul, D. (2015). Cybercrime Act: Fostering Sanity in ICT Sub-Sectors. Retrieved 14 March, 2016, from https://www.cert.gov.ng/news-events/details/153

Pati, P. (2003) 'Cybercrime. Retrieved 20th July, 2016, from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

Pati, P. (2007) Cybercrime: Hardships to curb it. Retrieved 20th July, 2016, from http://www.naavi.org/pati/cyber_crimes1.html

Phillips, D. C., & Burbules, N. C. (2000). *Postpositivism and educational research*. Lanham, Maryland: Rowman and Littlefield.

Polit, D.F., Beck, C.T., Hungler, B.P. (2001). *Essential of Nursing Research: Methods, Appraisal and Utilization.* 5th Ed., Philadelphia: Lippincott Williams & Wilkins

Prior, L. (2007). *Documents, in C. Seale, G.Gobo,J.F Gubrium and D. Silverman (eds) Qualitative Research Practice*. London: Sage

Provos, N., Rajab, M.A., Mavrommatis, P. (2009). Web-based malware attacks are more insidious than ever. What can be done to stem the tide? Cybercrime 2.0: When the cloud Turns Dark. *Communications of the ACM*, 53(4), 42-47

Regulatory of Investigatory Powers Act 2000

Reisig, M.D., Marenin, O. (1995). "A General Theory of Crime" and Patterns of Crime in Nigeria: An Exploration of Methodological Assumptions. *Journal of Criminal Justice, 23(6), 201-518*

Remenyi, D., Williams, B., Money, A., & Swartz, E. (2005). *Doing research in business and management: an introduction to process and method*. London: Sage Publishers.

Reyns, B.W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offences. *Journal of Research in Crime and Delinquency*, 50(2), 216-238

Robson, C. (2002). *Real world research: a resource for social scientists and practitioner-researchers* (2nd ed.). Massachusetts: Blackwell Publishers Inc.

Robson, C. (2011). *Real World Research.* Chichester: Wiley

Rojon, C., & Saunders, M. N. K. (2012). Formulating a convincing rationale for a research study. Coaching: *An International Journal of Theory, Research and Practice*, 5(1), 1–7.

Ryan, B., Scapens, R.W., Theobald, M. (2002). *Research Method and Methodology in Finance and Accounting,* (2nd ed.). London: Thomson.

Saulawa, M.A., Abubakar, M.K. (2014). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. *Journal of Law, Policy and Globalization, Vol. 32, 23- 33*

Saunders, J. (2017). Tackling cybercrime – the UK response. *Journal of Cyber Policy,* 2(1), 4-15

Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research methods for business students* (3rd ed.). Harlow: Pearson.

Saunders, M., Lewis, P., Thornhill, A. (2007). *Research Methods for Business Students.* Essex: Pearson.

Sekaran, U., & Bougie, R. (2013). *Research methods for business*. (6th ed.). Chichester: John Wiley and Sons Ltd.

Sesan, G., Soremi, B., Oluwafemi, B. (2013). Economic Cost of Cybercrime in Nigeria. Retrieved 10 June, 2015, from https://pinigeria.org/downloads/research-reports/

Shehu, A.Y., (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research,* 3(7), 169-180.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75.

Smith, J.K (1983). Qualitative v quantitative research: An attempt to classify the issue', Educational Research, March, 6-13

Smith, R.G. (2003). *Investigating Cybercrime: Barriers and Solutions*. Paper presented at the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney. Retrieved from http://www.aic.gov.au/media_library/conferences/other/smith_russell/2003-09-cybercrime.pdf

Smith, R.G., Grabosky, P., Urbas, G. (2004). *Cyber Criminals on Trial.* Cambridge: Cambridge University Press.

Shavers, B. (2013). *Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects.* Massachusetts: Elsevier.

Stevens, A. (2006). *"419": The Story of Advance Fee Fraud*

Steele, R. (2016). How offenders make decisions: Evidence of rationality. *British Journal of Community Justice,* 13(3), 7-20

Sutherland, E. and Cressey, D. R. (1974) Criminality (7th Ed.). Philadelphia, PA: Lippincott.

Tamarkin, E. (2015). The AU's cybercrime response: A positive start, but substantial challenges ahead. *Institute For Security Studies*. Retrieved 20 December, 2017, from, https://www.africaportal.org/publications/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead/

Tech UK (2015). Partners against crime: How can industry help the police to fight cybercrime? Retrieved 26 October, 2017, from file:///C:/Users/BNS382/Downloads/Cyber_Crime_Paper.pdf

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioural Sciences*. Thousand Oaks, CA: Sage Publishers.

The Commonwealth (2018). Member countries. Retrieved 10 December, 2017, from http://thecommonwealth.org/member-countries

Tive, C. (2006). *419 Scam: Exploits of the Nigerian Con Man.* New York: iUniverse Inc.

Tseloni, A., Wittebrood, K., Farrell, G., Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology, 44, 66-91*

Tuckett, A. (2005). Applying thematic analysis theory to practice: a researcher's experience. *Contemporary Nurse, 19,* 75-87.

Ukanwa, O.E. (2015). *Economic and Financial Crimes Commission, Its Policies and Corruption in Nigeria, 2003 To 2010.* (MSc Thesis), University of Nigeria, Nsukka. Retrieved from http://196.222.5.9:8080/xmlui/handle/123456789/742

UK Government. (2017). *National Crime Agency.* Retrieved from https://www.gov.uk/government/organisations/national-crime-agency

UK Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved 30 November, 2017, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

UK Government. (2016b). *International MLA & Extradition Agreements the UK is party to.* Retrieved 30 March, 2017, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=false

UN. (2011). Cybersecurity: A global issue demanding a global approach. Retrieved 20 August, 2015, from http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

United States Department of States. (1997). *Nigerian Advance Fee Fraud.* Retrieved from http://www.state.gov/documents/organization/2189.pdf

UNODC (2017). Corruption in Nigeria. Bribery: Public Experience and Response. Retrieved 15 November, 2017, from https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Nigeria/Corruption_Nigeria_2017_07_31_web.pdf

UNODC (2013). Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Ultrascan AGI (2014). 419 Advance Fee Fraud Statistics 2013. Retrieved 10 July, 2015, from http://www.ultrascan-agi.com/public_html/html/pdf_files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf

US Legal (2016). Law Enforcement Agency: Law and Legal Definition. Retrieved 10 March, 2017, from, https://definitions.uslegal.com/l/law-enforcement-agency/

Owen, O. (2014). The Nigerian Police Force: Predicaments and Possibilities. Retrieved 30 December, 2017, from, http://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/nrn-wp15.pdf

Oxford Dictionary (2018). Definition of Law Enforcement Agency. Retrieved 10 January, 2018, from https://en.oxforddictionaries.com/definition/law_enforcement_agency

Vanguard. (2015). NSA, Microsoft team up to tackle cybercrime in Nigeria. Retrieved from http://www.vanguardngr.com/2015/12/nsa-microsoft-team-up-to-tackle-cybercrime-in-nigeria-2/

Van Maanen, J. (1983) *Qualitative Methodology*. London: Sage.

Wall, D.S. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law, Computers and Technology, 12:2, 201-218*

Wall, D. (2004). What are Cybercrimes? *Criminal Justice Matters,* 58(1), 20-21

Wall, D.S. (2005). The Internet as a Conduit for Criminal Activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system (pp. 77-98). Thousand Oaks, CA:Sage.*

Wall, D.S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research,* 8:2, 183-205

Wall, D.S. (2008). Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology, 22:1-2, 45-63*

Wall, D.S. (2017) 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in R. Brownsword, E. Scotford and K. Yeung (eds) The Oxford Handbook on the Law and Regulation of Technology, Oxford: Oxford University Press.

Walsh, M. (2001) *Research Made Real: A guide for students*. United Kingdom: Nelson Thornes

Waziri, F. (2009). *The Fight against Money Laundering and Corruption in Africa: A Key Issue for Foreign Investment and Economic Development*. Paper presented at the International Summit on Transnational Crime, Paris, France. Retrieved from http://www.cmf.ch/wp-content/uploads/waziri.pdf

We Are Social (2016). Digital in 2006. Retrieved 20 August, 2016 from, http://wearesocial.com/uk/special-reports/digital-in-2016

Weitzman, E., & Miles, M. (1994). *Computer programmes for qualitative data analysis*. Thousand Oaks, California :Sage.

Wengraf, T. (2011). *Qualitative research interviewing*. London: Sage Publishers.

West Yorkshire Police (2017a). *County Profile*. Retrieved 20 December, 2017, from https://www.westyorkshire.police.uk/about-us/our-profile/county-profile/county-profile

West Yorkshire Police (2017b). *Cybercrime.* Retrieved 20 December, 2017, from https://www.westyorkshire.police.uk/advice/online-crime-safety/online-safety/cyber-crime

West Yorkshire Police (2017c). *Wikipedia.* Retrieved 20 December, 2017, from, https://en.wikipedia.org/wiki/West_Yorkshire_Police

Welsh, E. (2002). Dealing with data: using NVivo in the qualitative data analysis process. Qualitative Social Research *3* (2): 1-7.

Wengraf, T. (2011). *Qualitative research interviewing*. London: Sage Publishers.

Willig, C. (2009). *Introducing qualitative research in psychology.* New York: McGraw Hill and Open University Press.

WITFOR (2005) Social, Ethical and Legal Aspects. Retrieved 10 July, 2015, from http://www.witfor.org/2005/themes/social-projrct3.htm

World Bank (2017) The World Bank in Nigeria. Retrieved 14 December, 2017, from http://www.worldbank.org/en/country/nigeria/overview#1

World Economic Forum (WEF) (2016). Recommendations for Public-Private Partnership against Cybercrime. Retrieved 20 May, 2016, from, http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf

World Information Technology Forum (WITFOR) (2005). Social, Ethical and Legal Aspects. Retrieved 13 June, 2015, from http://www.witfor.org.bw/themes/social-projrct3.htm

Yahaya, F. (2009). EFCC, Microsoft tackle scammers, signs MoU. Retrieved 10 June, 2015, from, http://thenationonlineng.net/web2/articles/2031/1/EFCC-Microsoft-tackles-scammers-signs-MoU-/Page1.html

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4)407-427

Yar, M. (2006). *Cybercrime and Society.* London: SAGE

Yin, R.K. (1994) *Case Study Research: Design and Methods* (2nd ed.). California: SAGE

Yin, R.K. (2009) *Case Study Research – Design and Methods* (4th ed.). CA: Thousand Oaks, SAGE.

Yin, R.K. (2014) *Case Study Research – Design and Methods* (5th ed.). London: SAGE.

APPENDIX A: **ACTION PLAN 2017-2018**

S/N	JANUARY 2017 – MAY 2018												
	ACTION PLAN	**TASK**	**TIMESCALE**										
		1ST PHASE											
1	**TASK 1: POST- INTERVAL EVALUATION**	**SUB-TASK**	**JAN**	**FEB**	**MAR**	**APR**	**MAY**	**JUN**	**JUL**	**AUG**	**SEP**	**OCT**	**NOV**	**DEC**
		1. Incorporate Feedback From IE	√											
		2. Registration	√											
		3. Supervision Team Feedback		√										
		4. Pilot Study: Analysis		√										
		5. Collect Primary Data (UK)		√									√	
		2nd PHASE												
2	**TASK 2: DATA ANALYSIS & THESIS WRITING**	**SUB-TASK**	**JAN**	**FEB**	**MAR**	**APR**	**MAY**	**JUN**	**JUL**	**AUG**	**SEP**	**OCT**	**NOV**	**DEC**
		1. Analysis of Data		√	√	√	√							
		2. Submit Draft Data Analysis Chapter						√	√					
		3. Thesis Write Up		√	√	√	√	√	√					
		4. Validation of Data: Conference Paper						√	√	√				
		5. Complete Thesis Write Up									√	√	√	√
		3rd PHASE												
3	**TASK 3: THESIS SUBMISSION & VIVA PRESENTATION**	**SUB-TASK**	**JAN 2018**	**FEB 2018**	**MAR 2018**	**APR 2018**	**MAY 2018**	**JUN 2018**	**JUL 2018**	**AUG 2018**	**SEP 2018**	**OCT 2018**	**NOV 2018**	**DEC 2018**
		1. Submit First Draft of Thesis	√											
		2. Feedback and Corrections	√	√										
		3. Submission of Final Thesis		√										
		4. Preparation for Viva			√	√								
		5. Attend Viva					√							
		6. Feedback & Correction of Viva					√							
		7. Final Submission					√							

APPENDIX B: **WORKSHOPS 2017-2018**

SN	NAME	TYPE	DATE	TIME	VENUE	STATUS
JANUARY						
1	The Use and Design of Questionnaires	PhD Training	18/01/17	2:00pm	Maxwell 822	**Missed**
2	The Future of Cyber Security 2017	Conference	24/01/17	8:00am	Old Trafford	**Missed**
3	Interviewing: Methods and Process	PhD Training	25/01/17	2:00pm	Maxwell 822	**Attended**
FEBRUARY						
4	Case Study Research	PhD Training	01/02/17	2:00pm	Maxwell 822	Attended
5	Mixed Methods	PhD Training	08/02/17	2:00pm	Maxwell 822	**Missed**
6	Qualitative Data Analysis	PhD Training	15/02/17	2:00pm	Maxwell 822	**Missed**
7	Statistical Analysis of Research	PhD Training	22/02/17	2:00pm	Maxwell 822	**Missed**
MARCH						
8	Using Nvivo QSR – Theory and Practice for Qualitative Data Analysis	PhD Training	01/03/17	2:00pm	Maxwell 822	Attended
9	Home Office – Security and Policing 2017	Conference	07/03/17	8:00am	Farnborough	Missed
10	Business Analytics	PhD Training	08/03/17	2:00pm	Maxwell 822	**Attended**
11	Representativeness, Reliability and Validity in Research	PhD Training	15/03/17	2:00pm	Maxwell 822	**Missed**
12	Critical Thinking and Writing	PhD Training	22/03/17	2:00pm	Maxwell 822	**Missed**
13	PGR Symposium	Symposium	23/03/17	9:00am	Think Lab	**Attended**
14	Research Ethics and the Ethical Approval Process	PhD Training	29/03/17	2:00pm	Maxwell 822	**Missed**
APRIL						
15	UKAIS 2017 Doctoral Consortium	Conference	03/04/17	8:00am	Oxford	**Attended**
16	5TH International Conference on Cybersecurity, Cyber Welfare & Digital Forensics	Conference	22/04/17	8:00am	Addis Ababa	**Missed**
17	Referencing, Citation and Plagiarism	PhD Training	26/04/17	2:00pm	Maxwell 822	**Missed**
MAY						
18	Using Social Media in Your Research and Career	PhD Training	03/05/17	2:00pm	Maxwell 822	**Missed**
19	Cyber Secure Nigeria 2017	Conference	16/05/17	8:00pm	Abuja	**Attended**
20	Preparing for the Viva	PhD Training	17/05/17	2:00pm	Maxwell 822	**Missed**
21	Academic English and Academic Writing	PhD Training	31/05/17	2:00pm	Maxwell 822	Missed
JUNE						
22	Planning for a Full-time Academic Writing	PhD Training	07/06/17	2:00pm	Maxwell 822	**Missed**
23	Writing a Manuscript for Journal Submission	PhD Training	14/06/17	2:00pm	Maxwell 822	**Missed**
24	SPARC 2017	Conference	27/06/17	8:00am	Media City	**Missed**
JULY						
25	Rethinking Cybercrime	Conference	03/07/17	8:00am	UCLAN	**Attended**
26	5th International Conference on Cybercrime & Computer Forensics	Conference	16/07/17	8:00am	Gold Coast, Australia	**Missed**

APPENDIX C: **PARTICIPANT INFORMATION SHEET**

Research Topic: INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY

Dear Sir/Madam:

I am writing to seek your consent to participate in a research seeking to do a comparative study on investigating cybercriminals in Nigeria for my PhD research at Salford School of Business, University of Salford, UK.

The research aims to do a comparative analysis of the Law Enforcement Agencies in Nigeria and the UK in regards to the effectiveness of their laws, legislation, policies and approaches in investigating cybercriminals and what improvements are needed in the international efforts to tackle the menace of cybercrime.

The duration of the interview would last about **45 minutes** or less.

The research is conducted in accordance to the guidelines and Code of Practice and Procedure of Integrity in Academic Research, which means all answers that you give, are strictly confidential and anonymous. Participation in this research is voluntary.

The responses of all participants taking part will be combined into a report and used during the research subsequently.

If you wish to verify or check the authenticity of the research, you can contact the Researcher Supervisor on email through (m.griffiths@salford.ac.uk).

Yours Sincerely,

Name: *Muktar Bello*
Role: Researcher
Email: m.bello@edu.salford.ac.uk
Contact: [redacted]
Mobile: [redacted]

Name: *Dr. Marie Griffiths*
Role: Supervisor
Email: m.griffiths@salford.ac.uk
Contact: [redacted]

APPENDIX D: **PARTICIPANT INFORMATION LETTER**

TITLE: *INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY*
RESEARCHER: *Muktar Bello*
SUPERVISOR: *Dr Marie Griffiths*

I, ***Muktar Bello*****,** a PhD Candidate from Salford Business School at the University of Salford, Manchester invites you to participate in a research project titled *"Investigating Cybercriminals in Nigeria: A Comparative Study".*

I am conducting a research on the activities of law enforcement agencies both in the UK and Nigeria in Investigating Cybercriminals in Nigeria for the partial fulfilment of a Doctor of Philosophy degree.

If you decide to participate in this research, an interview would be conducted at a time and place of your convenience.

The duration of the interview would last about 45 minutes or less. Participation in this research is completely voluntary and you may choose to withdraw from the research at any time or not give an answer to any question that you may not be comfortable with.

The ***participant information form***, ***participant recruitment material*** and ***participant consent form*** have been attached for your information and consideration.

This study has been reviewed and received ethics clearance through the University of Salford Ethics Panel ***with ethics reference No: SBS16.08***

If you have any questions about your rights as a research participant, please contact the Research Supervisor, Dr Marie Griffiths at the below listed details.

If you have any questions, please feel free to contact the following details provided below:

Name: *Muktar Bello*
Role: Doctoral Researcher
Email: m.bello@edu.salford.ac.uk
Contact: [redacted]
Mobile: [redacted]

Name: *Dr Marie Griffiths*
Role: Supervisor
Email: m.griffiths@salford.ac.uk
Contact: [redacted]

APPENDIX E: **CONSENT FORM**

CONSENT FORM

Title of Research: Investigating Cybercriminals in Nigeria: A Comparative Study

Ethics Ref No: *SBS16.08*

Name of Researcher: MUKTAR BELLO

S/N	CONSENT	YES	NO	NA
1	I confirm that I have read and understand the information sheet dated for the above study.			
2	I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.			
3	I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.			
4	I understand that any information given by me may be used in future reports, articles or presentations by the research team.			
5	I understand that my name will not appear in any reports, articles or presentations.			
6	I agree to take part in the interview/questionnaire.			
7	**I agree to take part in the above mentioned study**			

_____	_____	_____
Name of Participant	**Date**	**Signature**
_____	_____	_____
Researcher	**Date**	**Signature**

APPENDIX F: PARTICIPANT RECRUITMENT MATERIAL

INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY

Cybercriminals in Nigeria commonly known as "419 scammers"; a word coined from the Nigerian criminal code that penalize people from obtaining under false pretense cost the Nigerian consumer $13.5 billion dollars in losses in 2012 (Sesan et al 2012). Despite efforts by the Nigerian Government to tackle it through the activities of law enforcement agencies, cybercriminals continue to operate to the detriment of the country.

This research aims at identifying the critical issues which require more attention for the purpose of tackling this criminal phenomenon. Such issues include adoption of a harmonized and digitized form of investigation, enforcement of the Cybercrime Act 2015 and enhanced international cooperation between relevant stakeholders in Nigeria as stipulated within the Council of Europe (CoE) convention on cybercrime.

By adopting international best practices and measures such as the Council of Europe (CoE) Convention of Cybercrime, the research will argue that such measures would positively affect the activities of investigators and prosecutors in curtailing the menace of cybercriminals in Nigeria.

This study will focus on activities of law enforcement agencies both in the UK and Nigeria in tackling Advance Fee Fraud, a variant of cybercrime.

Advance Fee Fraud has become a multi-national organized crime that requires a multinational response because over the decade, the arrest and prosecution of hundreds of cybercriminals has not been an effective deterrence due to the increase in 419 incidences.

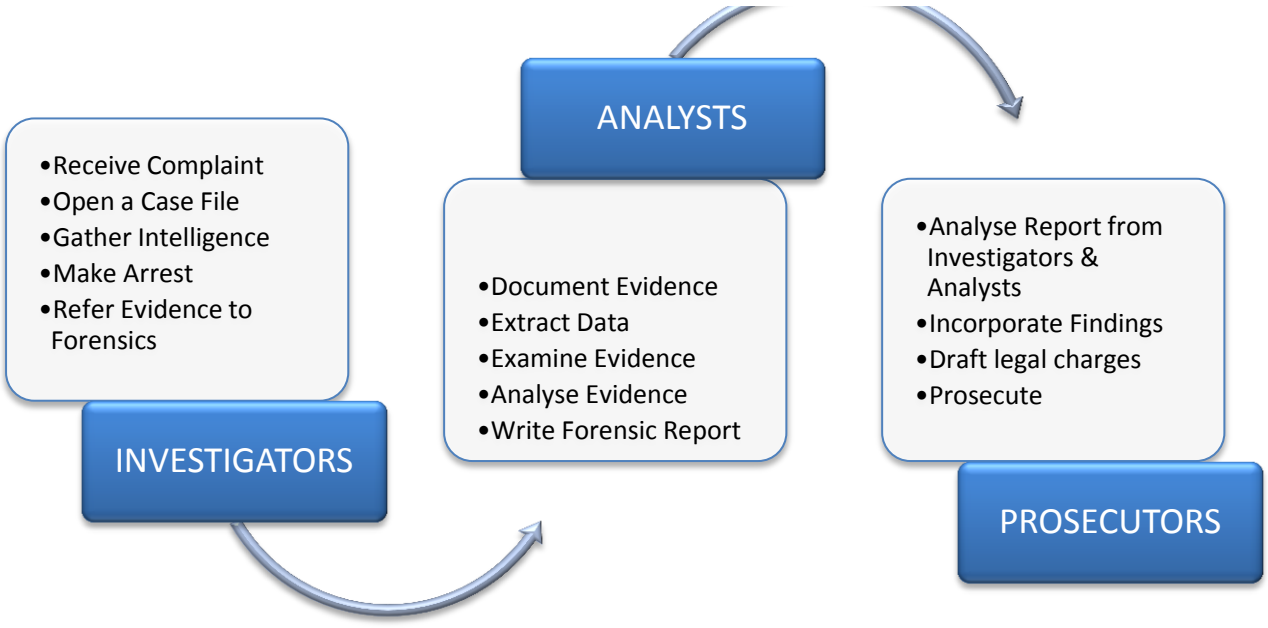


Figure 1: Current Approach in Investigating Cyber-crime in Nigeria

The above figure shows the current standard operating procedure of how cybercrime offences are investigated. This research will focus on the activities of Investigators and Analysts in understanding what improvements are needed in tackling Advance Fee Fraud.

APPENDIX G: **ETHICAL APPROVAL**

Research, Innovation and Academic Engagement Ethical Approval Panel

Research Centres
Support Team
G0.3 Joule House
University of Salford
M5 4WT
T +44(0)161 295 7012
www.salford.ac.uk/

7 June 2016

Muktar Bello

Dear Muktar

RE: ETHICS APPLICATION SBS16.08 - Investigating Cybercriminals in Nigeria: A Comparative Study

Based on the information that you provided, I am pleased to inform you that your application SBS16.08 has been approved.

If there are any changes to the project or its methodology, please inform the Panel as soon as possible by contacting SBS-ResearchEthics@salford.ac.uk.

Yours sincerely,

Professor David F. Percy

Chair of the Staff and Postgraduate Research Ethics Panel

Salford Business School

APPENDIX H: **INTERVIEW QUESTION & TRANSCRIPT-INVESTIGATOR**

Interviewee: XX
Date: 30/08/16
Time: 12:00PM
Location: Lagos
Designation: Cybercrime Unit (Lagos)
Office: EFCC

INTRODUCTION: Good Afternoon Mr. XX. [redacted]. I am Muktar Bello, a PhD Candidate of the University of Salford doing a comparative research on Cybercrime Investigations in collaboration with Law enforcement and other stakeholders in the UK and Nigeria. The research seeks to identify the critical issues that require urgent attention in the International effort to tackle cybercrime globally. Thanks for taking part in this research.

Q1: Sir, what role does the cybercrime unit play within the EFCCs mandate in tackling economic and financial crimes?

Well as you know the mandate of the EFCC is to investigate economic all economic and financial crimes. Ahhh in the country so by extension what it means what it means is that economic and financial crimes can come in so many forms and we see cybercrime one of those crimes that falls within EFCCs mandates. Because if you look at financial crimes in this day is there have now gone digital more or less and we have the duty again by law to enforce the Advance Fee Fraud Act. And we have seen a shift from the local traditional ways fraudsters do conduct their fraudulent activities. From the analogue now to the digital. That is the more reason why ahh we have a cybercrime unit. When the EFCC started there was no cybercrime unit but we have come to realise that without cybercrime unit we would be lagging behind no doubt but so as such the cybercrime unit plays a very important role within the EFCCs mandate. And that's it.

Q2: What role does the cybercrime unit play in investigating cybercrime in Nigeria?

Well cybercrime unit is an investigative section that actually investigates and prosecutes. Prosecution we have our own lawyers here. Basically what we do is that we investigate cybercrime cases. That's our primary assignment amongst other things that we do. But this is the major thing that we do investigation. Trying to find out the bad guys, trying to save the public from being defrauded using I mean the cyberspace, specifically that's what we do.

Q3: Why do you think the role of the Cybercrime Unit is important in investigating cybercrime?

Well because if you look at cybercrime you need a expertise. It is a different, you can be an investigator but for you to investigate cybercrime cases you must have that expertise. You must acquire the knowledge that necessary for you to investigate that kind of cases and more so that's why there was a need a separate unit so that training would be tailored to those kinds of investigators to deal with the current realities of issues. And if you look at ahhh I mean if you look at our life now virtually everything we do if one way or the other dependent on technology so the the crimes are changing now. You see more of digitally driven crime than the local or traditional crimes that we use to know. YES.

Q4: What crimes are considered as cybercrime?

Well since there is no broad definition of that but for me from this part where we do from the experience from what we do here at the EFCC we see cybercrime as crimes committed within the

cyberspace with a use of a computing device ah ah and we can say that there are two kinds of crimes that we see from these. We see crimes against computer systems and we see crimes by use of computer crimes as either as a tool and again as a target. So so again any crime I mean that's targeting the confidentiality, availability and integrity of computer systems we see it as a cybercrime.

Q5: Based on your experience what form of cybercrime offences do you think is prevalent in Nigeria?

Well in Nigeria there are different trends that we see but the ones that we see most, most of the cases we are receiving today are due to the drive of the cashless economy today in the country. Ahh everybody is driving towards ahh using ahh the e-channels todays and by so doing ahh we have seen kind of phishing, social engineering through phishing. We have seen malwares and viruses being distributed. We have also seen hackling of accounts you understand. Email accounts that are been hacked, taken over and other kinds of scams that are being perpetuated with the use of a computer like romance scam for instance, auction scams you know and website defacement is on the rise. We have seen hacktivist coming up defacing prominent websites in this country, government agencies websites including the Nigerian site website was unfazed and so these are the kind of crimes that we see but most of them are financially. They are motivated I mean for financial gain to a large extent I would say.

Q6: Based on your experience what factors do you think contribute to high cases of cybercrime in Nigeria?

Well there are so many factors; I would say that one of the drives for the cashless economy is there, one. Secondly online commerce sites we have so many retail companies online, e-commerce to say the least. Ahh and more so again I would talk about unemployment of the youths in this country today. And lack of credible database you understand so you would not be able to. If you make arrest, if the agencies make arrest it would be difficult for you to bring it together to see who is doing who, you understand. I know so. I think I should say inadequate, inadequate industry wide collaboration everybody is working on his own. That's another factor. And there is low level of awareness again and and some of the factors again, low security controls in so many agencies you understand. So that gives rise to occurrences because there is this perceived opportunity. These factors are there. You find out. I talked about low employment, if you look at the country today, 70% of our population is the youth so think of the youth without employment and they always devise a means of making money. And these are some of the factors that we see as being responsible for for the rise in cybercrime cases in the country.

Q7: What kind of relationship does that cybercrime section have with other departments within the Commission in investigating cybercrime?

Well you see in the commission so many departments and we do complement each other for us we are investigators. We investigate cases but we have a forensic department. Forensic department I mean assist in forensically examining all the recovered devices and they give us results and analysis of those things. We also have the legal department who now guide us into the work that we do. I mean because we operate within the ambit of the law ahh they look at our files at the end of our investigation to see if they can prefer charges against the accused or if they Act that is being committed contravenes any of the laws so I mean we have a very good working relationship with some of the departments.

Q8: Do you think the relationship of the Cybercrime section with other departments is relevant?

It is very very relevant. Very very relevant in the sense that if you make an arrest and you do investigation, if you recoveries you make you recover items in a scene of crime. I mean the forensic department are the people that would do the forensic analysis of those devices and that would further tell you the kind of criminal group that you are doing with yeah and the legal department too, if you dont prosecute, prosecution is a deterrent, so if you don't prosecute so at the ned the whole thing would become meaningless, it is very very important, it is very very important.

Q9: What kind of relationship does the section have with external stakeholders in investigating cybercrime in Nigeria?

Well cybercrime being that it is it is transnational in nature and also there are lots of facilities that are been used in which you would have to work with other external stakeholders. The cybercrime unit we have had a good working relationship. We have collaboration with so many stakeholders most especially the ISPs, the banks, very important because if you have to make use of their facilities the online services for you to perpetuate this kind of fraud and also the telecommunications companies, the GSM companies because now if you look at it most of the service providers that actually provide services including the mobile technology. So gone are the days where people go to cyber cafes to send emails, everybody does it through the comfort of his house. So working together with other external stakeholders is very important. And that does not mean we only collaborate with Nigerian external stakeholders, we also do collaborate with external international stakeholders. We have had several discussions with Microsoft; in fact we even signed an MOU with Microsoft. Last week we had a visitor from Facebook, Director of Trust and Safety was here. We reached out to them to see how we can work together and see how we can work together to address the growing threat of cybercrime. And again we are part of a lot of joint investigative bodies around the world. We are part of the International Mass Marketing Fraud working group comprising of about 9 countries comprising of regulators and law enforcement around the world. We also signed an MoU with FTC, Federal Trade Commission in the US and recently I was in Singapore where I visited the ICG, Innovation Centre, it's an Internal office specifically designed created to deal with cyber threats. I was there we had a meeting in which other countries from Asia were there. Collaboration is ongoing, we try to establish collaboration with other countries because you realise that one country cannot fight it alone and more so again if you look at the services that are been provided online, they are all scattered all over the world. You can use online services based in America, you can use IP address based in another country, you move money here and there. So we collaborate very well with external bodies, both external and internal. You understand, and we have had good working relationship with certain Law enforcement agencies for the same purpose.

Q10: Do you think the relationship with other external stakeholders is effective in prosecuting cybercrime?

It is. It is very very effective. In fact one of the cases I can give you example if is the one after our meeting in Singapore in which countries several countries were there mostly Asia, America was there as well. We discussed about cases that transcend borders. One of the cases we discussed were an arrest was being made and charges are being preferred. So this is an example of International Partnership. You understand and the victims are from different countries and the perpertrators are from different countries, the mastermind is in Nigeria but at the end we were able to arrest and we

are going to get evidence from the other people so that we can prosecute them. We have charged them to court now. So it's very very important. YES.

Q11: What current measures are you deploying to assist the Commission in addressing the issue of cybercrime in Nigeria?

Well there are so many so many initiatives that we came up with. We have got like a three way approach. We deal with intelligence, one, we deal with intelligence; secondly we deal, when I say intelligence because people don't go to cyber cafes anymore. We don't rely on people to come and say this cyber café is doing this is doing that. Because of the complaints we receive from outside we know that a lot of cybercriminals are having a field day. SO We have now devised a means where we encoded people to give confidential information. We have a website where we have an email addresses that people can write to us anonymously and we do a check and see if really something Last week we arrested like 16 boys, 16 boys living in a flat and all of them are engaged in cybercrime. And that was based on an informant who gave us an information and anonymously we don't even know him. Ahh and I would say that I mean if the public see that you are doing the work, everybody would come forward and give you the information. Secondly, in terms of enforcement. We have had a lot of enforcement activities. And one enforcement activity is presently we are working with the Nigerian Postal Inspection Services and Nigerian Postal Service here. We have a lot of Nigerians who steal credit cards; they do phishing and get details of people and order goods online with somebodies credit card through identity theft. So in that regard what we do is we work with them, any good that is coming that is suspicious that they should stop and should ask and should revert to us to come in and intervene. Now we have hundreds and hundreds of equipment's and items that are unclaimed because they are all proceeds of cybercrime. And they are all high end gadgets, watches, we have iPhone, we have computers, you have jewerlly, you have shoes, you have so many things, high end luxury items that are being ordered by stolen credit cards. This is one of the enforcement. Another enforcement measures that we are employing is the vigorous arrest and prosecution. Yes. Vigorous arrest and prosecution of these people. Whoever that we arrest, at the end of our investigation; if he is found wanting and indicted we make sure that he's prosecuted. So that has done a long way in this issue. We have over 300 convictions in that regard. We have over 300 convictions in that regard, you understand. And our laws are very so good for us in that sense in the sense that whoever or even when you are arrested and found with material that is capable of or is a tool that is being used to commit fraud. For instance if you found with malware in your system and it appears that this malware cannot reasonable tell why you keep the malware there and you have send it to other people, the laws permits us to take those kind of people to court and prosecute them. So in terms of disruption, in disruption measures we are working with banks for those that normally go to bank to collect money, it's a disruptive measures. We have arrested a lot of people at the bank who hack into people's account and move money to their accounts. They call it BEC, business email compromise where they move money from peoples account when they hack into people's account and move to other accounts. So in collaboration with the banks we are able to arrest people and whenever they see something that is suspicious they always inform us and we move in. so these are some of the disruptive measures and or we stop the account, we place caution on the account that nobody should put this money and we get a court order until the person comes forward to tell us why he needed the money. We work closely with our legal department, whenever we see any suspicious transaction you try as much as you can to conduct to place caution on that account while we start the process of getting an interim forfeiture unless somebody comes forward to explain the source of that fund. So

these are some of the disruptive measures we are doing. And also the media campaign, we have been trying to raise awareness, raise awareness as in schools, we have gone to NYSC camps, we have gone to schools, we have gone to conferences to raise awareness about the dangers that are inherent of the cyber risks inherent. So we tell people to be careful this is what you do, we give example of cases or how it is done so that people can safeguard their confidential information without losing it anyhow. So there is Media outreach as well. YES.

Q12: How successful are these measures in curtailing the activities of cybercrime?

It is the measures are successful in one of the thing that we did most especially when it comes to the western union stuff. Like I said most of the cybercrime are financially motivated so for those that do that and actually get money from the banks. The western union or the banks have introduced measures that make it very difficult for anybody to come and pick money. There must be a kind of documentation that makes it a bit hard for somebody to meet up. So there must be success story. It's not that we are satisfied with what we have now. Every day we look the whole strategies and try to change to see how we can achieve maximum maximum results.

Q13: Are the current laws adequate in investigating cybercriminals?

I think the current laws are adequate. We have the Cybercrime law now which was just in 2015. We have the Advance Fee Fraud Act even though it's not cyber as in but there are some sections which even proscribes some of these offences. So to me for now I think the laws are adequate. YES.

Q14: What challenges do you have in the discharge of your duties as it pertains to investigating cybercrime?

Well some of the challenges that we do have, being that it is transnational in nature sometimes you would tend to have cases that we might need to reach out to other countries and other countries might not be cooperative. This is one. Secondly again you may have, that's jurisdictional issues. This is one. Secondly sometimes again the expertise you understand, technology is growing at the speed in which it's going, it's going at a very high speed. We need to be up to date with the kind of things that are happening so the need to have dedicated and up to date skills and in tackling these kind of things is very, you understand. Thirdly, some of the challenges we are having, we don't have, we have a problem of identity management system in this country, anybody can be anything is this country. We don't have a single database today whereby they can check your records and say yes this is who you are because there is, everybody is picking information but they are not they aren't able to share that information so that has been a major challenge to us. If you have a phone number, you have an IP address if you go there it could be registered to somebody whose name could be fake, fictitious. So you don't any database, a central database or a national database to fall back to, cross check and assist you in your investigation. So these are some of the challenges we are seeing. The laws are ok to a large extent. We tried and see and there are lots of thing we can do with that. And again ahhh maybe Equipments, Equipments is very important, tracking devices; forensic devices because these things changes you have to be up to date with some of the devices. Otherwise you would be left alone with an absolute device that makes no that would not achieve any results for you.

Q15: What recommendations would you suggest to effectively tackle these challenges?

While it's just the opposite. You are talking about training and re-training, one, secondly, reaching out to some of these countries to have a better understanding of the whole problem and working

together. International cooperation is very very key. Thirdly those Equipments, tracking devices are very very important as well.

Q16: Finally Sir, what advice do you have for the Commission in its mandate to tackle the activities of cybercriminals?

My advice to the Commission, I would say that we would have to enhance our technical capacity. That is very very important and more so again the commission should give emphasis on the need to train their staffs train and retrain their staffs. These are the two advices. When I say train and re-train, I mean they should allotted resources kind of.

MB: Mr. XX, [redacted] Thank you for taking part in this research.