AN ASSESSMENT OF THE ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC) IN COMBACTING CYBERCRIMES IN KWARA STATE, NIGERIA

ALOKUN, Ayomide Emmanuel
20PGEC000126
B.Sc. ( )

A Dissertation in the Department of Political Science and International Relations

MASTER OF SCIENCE (M.Sc.)
of the

LANDMARK UNIVERSITY, OMU ARAN, KWARA STATE

Supervisor: Dr Ake Modupe

August, 2022

DECLARATION

I, ALOKUN Ayomide Emmanuel, an M.Sc. political science student in the (Department of Political Science, International Relations and Mass Communication), Landmark University, Omu-Aran, hereby declare that this Dissertation entitle "An Assessment of the Economic and Financial Crimes Commission (EFCC) in Combating Cybercrimes in Kwara State, Nigeria," which I have submitted, entirely focused on my original research. All information derived from other sources or completed by other people or institutions has been properly acknowledged.

_____

Student's Full Name

Matriculation Number

_____

Signature & Date

CERTIFICATION

This is to certify that this research work was carried out by ALOKUN Ayomide Emmanuel (20PGEC000126) in the Department of Political Science and International Relations, College of Business and Social Sciences, Landmark university under our supervision.

…… …….

Dr. Modupe Ake **Date**

Supervisor

…… ……

Dr. Joseph Iseolorunkanmi **Date**

Co-Supervisor

…… ……

Dr. Modupe Ake **Date**

Head of Department

Name

…… ……

External Examiner **Date**

DEDICATION

I dedicate this work to God Almighty.

ACKNOWLEDGMENTS

My profound gratitude goes to God Almighty for His direction and providence to have come this far. I am also grateful to Dr Modupe AKE and Dr Joseph Iseolorunkanmi, whose ideas and interactions guided my intellectual development. I acknowledge the contribution of my parents, colleagues, friends, informants and my Lecturers' immense support and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

EFCC	Economic and Financial Crimes Commission
NIFU	National Intelligence and Financial Unit
GDT	General Deterrence Theory
RAT	Routine Activity Theory
ICPC	Independent Corrupt Practices and other Related Offences Commission
FBI	Federal bureau of investigation
NITDA	National information technology development agency
CSI	Crimes scene investigation

ABSTRACT

The Nigerian economy has been plagued by fraudulent activities, economic mismanagement, corruption, a lack of accountability and transparency. Systemic inefficiencies, particularly in the public sector, were caused by fraud that went undetected. Nigeria is the most populous nation in Africa with a population of over 200 million and 91 million active internet users. With 47% of its population from West Africa, the nation is multicultural and multiethnic. The study adopts the general deterrence theory because it integrates choice theory and rational choice theory because the seriousness, promptness, and certainty of punishment can deter criminal behavior. This study is aware of how cybercrime affects the Nigerian system. This study aims to evaluate the contribution made by the EFCC to lowering cybercrime in Nigeria using data from all three senatorial districts in Kwara State as well as a few selected government parastatals. The purpose of this study was to better understand the nature of cybercrime, its effects on the Nigerian system as a whole, and the efficiency of the EFCC in reducing cybercrime among young people in Kwara State and throughout Nigeria. The study reveals that cybercrime has penetrated the Nigerian system profoundly and if left unchecked, would persist in the nearest future due to the EFCC's failure to permanently reduce youth cybercrime. Conclusions were generated based on the results of the test performed using all pertinent information gathered and examined for each of the analyses. The findings demonstrated the effectiveness of EFCC efforts in promoting financial accountability and transparency in cyberspace, as well as its capacity to identify and tackle cybercrime across the nation of Nigeria.

Keywords: Fraud, Corruption, Conviction, Cybercrime, Security

Word counts: 265

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

With 91 million active internet users and a population of over 200 million, Nigeria is the most populous country in Africa. The country is cosmopolitan and multiethnic, with 47% of its population hailing from West Africa (Internet World Stats, 2017; World Bank, 2017). Maintaining public security, however, is one of the nation's toughest problems (Owen, 2014; Nwachukwu, 2012). Due to the integration of digital technology and internet connectivity, cybercrime has increased in frequency in Nigeria as a result of a lack of oversight and enforcement of pertinent laws and policies. The arrival of the internet and cellphones, which have improved access to and made the internet more inexpensive for everyone-including criminals-has made this problem worse (Saulawa and Abubakar, 2014). (2017) Adesina; (2011) Nkanga.

In response to the damaging socioeconomic effects of cybercrime in Nigeria, the government established a new agency, passed cybercrime legislation, and worked with partners to substantially reduce hackers' activities (Adesina, 2017; Adomi and Igun 2008). To investigate financial crimes including cybercrime, the EFCC Act (2004) and Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, two acts of parliament, led to the creation of the Economic and Financial Crimes Commission (EFCC).

To safeguard Nigeria's online, the Cybercrime Prohibition, Prevention Act (2015) was passed; nevertheless, over time, the efficacy of the laws and policies addressing cybercrime has decreased (Chawki & Paul, 2015). Society is becoming more and more dependent on contemporary information technology and the internet to conduct business, coordinate industrial activities, and interact with friends and family. Modern technology increases productivity, production, and communication, but it also puts people who wish to seize new opportunities in danger.

Vati (2009), because of the internet's quick development and extensive use, more people are using it. The internet provides countless opportunities for business, social interaction, and education. It also serves as a thriving haven for illegal activity. Nowadays, internet fraud schemes carried out via e-mail, the phone, chat rooms, message boards, or websites are the most common. The chief of the FBI's (Federal bureau of investigation)

financial crime section claims that the agency's Computer Crime Investigations used the Internet to acquire unauthorized access to computers (Brey, 2001).

Fraud, subpar economic management, corruption, a lack of accountability, and transparency have all plagued the Nigerian economy. Systemic inefficiencies, notably in the public sector, were caused by unreported fraud. The National Assembly introduced an Act in 2002 that created the EFCC in response to this threat, and it later amended it in 2004. It was established in response to the Federal Government's initiatives to combat financial and economic crime and restore order to Nigeria's economy.

According to the Act, the EFCC is responsible for combating financial and economic crimes by conducting investigations and filing lawsuits against offenders among other things, the EFCC is responsible for investigating and prosecuting offences like as financial fraud, tax fraud, illegal bunkering, financing of terrorism, capital market fraud, cybercrime, and abuse of office (Olukoya 2012). With a mission to combat the corruption threat, which hinders Nigeria's progress; protect domestic and foreign assets in the country; instill in people a spirit of hard work while discouraging the desire for ill-gotten wealth; detect and confiscate such ill-gotten wealth; establish a moral workforce in both the public and private sectors of the economy, and participate in the global fight against corruption.

Since its formation, the EFCC has worked diligently to locate, track down, freeze, confiscate, or seize the proceeds of such illegal acts. There have been several documented convictions for crimes related to corruption, money laundering, oil pipeline sabotage, and other similar activities (Adebayo, 2018In Nigeria, website cloning, misleading advertising, online purchasing, and other types of e-commerce fraud are the most common types of cybercrime.

Financial fraud, electronic mail cloning, and identity theft are the three types of cybercrime that are most common in Nigeria (Olugbogi, 2010). Which frequently manifests itself or takes the shape of imposters appearing as representatives of financial institutions sending customers emails requesting vital information about their accounts to prevent their accounts from being banned, which would make transactions impossible. The stolen goods are taken out one slice at a time (Hassan & Kolade 2012).

Corrupt politicians and their associates were found to be in control of more than $11 billion in assets and funds (Adekoya, 2011). The Commission is tenacious, with over

1500 additional cases pending in court, over 600 convictions, and over 65 high-profile cases being prosecuted in various Nigerian courts at various stages (Augustine, 2010). The tremendous increase in internet fraud in Nigeria over the past few years is deeply concerning, and the detrimental effects on the nation's socioeconomic condition are both crippling and unsettling. Crimes in Nigeria and the rest of the globe, according to numerous perspectives (Buchanan & Grant, 2001).

Chawki & Wahab, (2006) highlight how cybercriminals use technology to mask their identities and physical locations, making it more difficult for law enforcement officials to hunt them down. Cyber fraud has flourished as the internet has developed across the world, particularly in the United States. Tive, (2006) looks into the methods and mindset of Nigerian fee scammers. He observes that con artists work with phony lexical elements. Stajano & Wilson, (2011) investigate several fraud techniques employed by Nigerian cyber con artists and describe how security-engineering activities may aid in resolving the issue.

Adeniran, (2008) examines the relationship between the Internet and the rise of Yahoo individuals and the Yahoo subculture in Nigeria. Olukoya (2019), claims that the Internet has not only contributed to the growth of cyber criminals in Nigeria but has also promoted the commission of crimes involving money among young Nigerians. Anonymous servers, hijacked emails, and phony websites, according to Chawki (2009), are common cyber tools used by Nigerian cyber thieves. A range of government and business actions has been implemented to curb and counteract this threat.

Due to a lack of transparency and accountability in both the private and commercial sectors, Nigeria is recognized for pervasive corruption (Olukoya, 2012). As a result, the Nigerian government has been unable to offer basic services to its citizens. The country has seen a decrease in direct foreign investment in recent years. According to recent reports, despite the various efforts taken to date, there has been no major drop in this EFCC heinous art.

Nigerian cyber thieves invent new techniques to commit this unlawful commerce daily, and the traditional methods of tracing them are no longer effective (Ajaro, 2010). It also emphasizes the role of the EFCC in these new tactics, as well as potential

infrastructures for their treatment and the consequences of implementing such procedures (Daniel, 2006).

The mission of the EFCC concerning curbing the menace of cybercrimes centres on protecting Nigeria's image, encouraging both domestic and foreign investment in the nation; fostering a work-ethic culture among the populace; and reducing the desire for unjust wealth. Thus, the EFCC identifies individuals and groups involved in internet-related frauds and confiscates their ill-gotten wealth as well as prosecutes them, thus contributing to the global war against cyber-crimes (Ifeyinwa & Anene, 2011).

1.2 Statement of the Problem

The rise of cybercrime in Nigeria is an increasing issue for law enforcement agencies since the information technology revolution began. In the same way, a nation that is rife with financial and economic crimes won't be able to have economic stability, prosperity, and advancement. Cybercrime, sometimes known as computer crime, is the use of a computer as a tool for illegal conduct, such as fraud, the trafficking of persons' pornography and stolen goods, identity theft, and privacy concerns. The importance of cybercrime, particularly online, has increased as computers have become more essential for business, entertainment, and government (Nkojo, 2009). Nigeria's failure to prevent or curtail cyber or internet crime can be attributed to inadequate policy ideation, formulation, and implementation of economic and financial crimes.

Youth are responsible for the majority of these digital crimes, which include identity theft, spoofing/phishing, credit card fraud, cyberstalking, and other offences, according to Akanbi (2007). Because the majority of young people today have the get-rich-quick syndrome, these youth activities have led them to neglect the African ideal of dignity in employment. Everyone aspires to become rich no matter what it takes, Nigerian youth involvement in internet crime has hurt the nation's brand internationally (Hassan, 2015).

Every day, there are more and more concerning instances of cyber criminality. These cybercrimes are currently exerting strain on the Nigerian economy and e-commerce. Additionally, (Meke, 2012) observed that due to Nigeria's incapacity to combat such crimes, the international community now views Nigeria as one of the most corrupt countries in the world. Internet crime has increased significantly in Nigeria over the past

twenty (20) years, according to Meke. In this study, youngsters and online crimes in Nigeria are mostly examined.

The main issues Nigeria is currently facing in the fight against fraud are political connections, internal controls, poor accounting record keeping, a lack of qualified staff, and problems with plea agreements and presidential pardons on fraudsters (Ameh, 2007). Additionally, the Federal Republic of Nigeria's Attorney General prefers to file Nolle Presque to free fraudsters despite having the constitutional ability to do so under sections 174 and 211 of the (2011) Constitution as amended.

Achua, (2009) assert that it is urgently necessary to safeguard the commonwealth from fraud and subpar performance as well as to shield people from the state's surrogate administrators' arbitrary, unlawful, and capricious activities. To prevent and manage frauds and forgeries in the Nigerian public sector, this research aims to determine the reasons behind the inefficiency of these anti-corruption institutions.

1.3 Research Questions

i. What are the factors that motivate youths' involvement in cybercrime in Kwara state Nigeria?
ii. How effective are the strategies of EFCC for detecting cybercrime among youths in Kwara state Nigeria?
iii. What are the challenges confronting EFCC in detecting cybercrime among youths in Kwara state Nigeria?

1.4 Objectives of The Study

The main objective of this research is to assess the achievement of the Economic and Financial Crimes Commission (EFCC) in its fight against internet fraud in Kwara state Nigeria. Therefore, the specific objective of this study includes the following:

i. To examine the factors that motivate youths' involvement in cybercrime in Kwara state Nigeria.
ii. To access the effectiveness of the EFCC in curbing cybercrime among youths in Kwara state Nigeria.
iii. To examine the challenges confronting EFCC in detecting cybercrime among youths in Kwara state Nigeria.

1.5 Significance of the Study

The study would be beneficial since it will give the public factual information on the EFCC's operations, particularly its efforts to combat internet fraud in Nigeria. It will also be crucial in identifying areas of risk and determining how to best address them to sustain effective fraud regulation. The study will provoke further studies and contribute to the development of fresh theories and methods that will enhance knowledge of how the EFCC enforces financial responsibility and transparency online. The research's conclusions will help government parastatals, organizations, ministries, companies, and other groups create pertinent internet fraud rules. This research will also benefit future scholars and add to the body of knowledge on the EFCC and internet fraud.

1.6 Scope of the Study

The geographical focus of this study is Kwara state, Nigeria. Kwara state is the focus because, in recent times, there has been an increasing upsurge in cybercrime activities in the state. The period of the study is from 2015-2021. This study's objective is to examine the EFCC's initiatives to combat internet fraud in Nigeria and how they can advance cyber security and transparency. It includes activities in the public and private sectors intending to improve financial efficiency.

1.7 Limitation of the Study

This scientific project has experienced numerous setbacks for a variety of reasons. One of these is the inability to acquire information from the EFCC office. At the moment, they are concerned about security and are reluctant to provide information and plans are not accessible to the commission. A few articles and publications that might have been useful for this study project could not be accessed. Similarly, the vast majority of the study's important informants declined to provide the study with the necessary level of detail. Though additional states should have been engaged, efforts were made to gain in-depth research in Kwara state, Nigeria, due to time, security, and other intrinsic constraints.

1.8 Operational Definition of Terms

Economic and Financial Crimes Commission (EFCC): This name designates the Economic and Financial Crimes Commission. It is a commission that was created in 2003

by a law passed by the National Assembly and changed in 2004. Its responsibilities include investigating and applying any laws that forbid economic and financial crimes.

Fraud: The act of misleading someone to illegally get money or things. It also refers to someone who deceives others by seeming to possess qualities, abilities, skills, etc. that they do not possess. It is an independent central national agency with EFCC as its home base and is tasked with collecting and analyzing financial data.

Cybercrime: According to Maitanmi *et al.* (2013), is any activity carried out online intending to commit a crime. These can be divided into crimes against people (or people), crimes against companies, and crimes against non-profit organizations. From all of these, it is sufficient to define cybercrimes as actions involving the use of Information Technology (IT) instruments, such as computers, smartphones, and the Internet, to defraud people, businesses, or the government.

Investigation: This refers to a certain type of investigation that involves an investigator looking into accounts or data for a predetermined reason based on the circumstances (Chike & Nwoha, 2013).

CHAPTER TWO
LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.0 Introduction

This chapter has to do with reviewing relative literature and the body of the work. The government and people of Nigeria have spent a lot of money defending against and preventing the online crime of all types. The government has invested up to 50 billion Naira in resources, infrastructure, and experts over the years to help combat this menace. The endemic and persuading feature of this crime, according to Myrem and Garcoa (1989), is that it poses special legal hurdles as well as challenging accounting and auditing problems, as explained by Anene (2011).

2.1 Cybercrime

According to the EFCC (2003), cybercrime, also known as internet fraud, is commonplace in the Nigerian system. They do not rely on the use or threat of physical force or violation; instead, they are characterized by deception, concealment, or a breach of trust. Such crimes are committed by people and organizations for their own and other people's financial gain. The handling and monitoring of important and intricate cybercrime activities include hacking, wire transfers, dating, identity theft, internet stalking, insurance fraud, and money laundering.

Due to the Economic and Financial Crimes Commission (EFCC), a body whose purpose is to monitor financial fraud and economic irregularities involving people, businesses, and national communities. Internet fraud or electronic crime refers to any crime that is performed while utilizing or knowing about the internet. (Spring) Electronic devices include, but are not limited to, computers, phones, and other portable devices. Online frauds are defined by Brenner and Susan (2001) as crimes committed using computers and networks as well as the use of technology to facilitate more conventional forms of crime. Internet fraud is believed to occur often, however, its exact reach is unknown. When crimes are identified, they are often not reported because businesses fear that they will lose more money as a result of the bad press than they do as a result of the actual crimes.

According to conservative estimates, computer hackers cost enterprises and government organizations billions of dollars every year. The average computer crime,

which is significantly more expensive than most other crimes, has a value of roughly 600,000 dollars, according to the FBI. The Volkswagen Company in Germany lost more than 260 million dollars in 1984 as a result of one instance of computer fraud. Daily, the software is sold on pirated CDs from Computer Village, a well-known market in Ikeja, Lagos, Nigeria. Microsoft has established itself in the sector and law enforcement has advanced significantly.

However, this unlawful activity is still being done covertly. Cybercrime in Nigeria: Definition, nature, and types Cybercrime has been defined by various academics from various angles. According to Maitanmi, *et al.* (2013), cybercrime includes any type of crime that is committed by offenders using a computer as a tool and the Internet as a connection to actualize or realize a variety of goals, such as illegally downloading music files and movies, pirating, spam mailing, among other things. This academic claims that a phenomenon results from improper or abusive usage of Internet services.

The characteristics of cybercrimes, according to Mconnell International (2000), are quite different from most terrestrial crimes in that they are very simple to learn, require few resources compared to the harm they cause, and can be committed within a geographic area without being physically present there, and are frequently not illegal. The Nigerian government has made the practice illegal by including section 419 of its criminal code as part of its effort to fight the problem. However, the phenomenon has continued to flourish there, giving the nation a negative reputation among League of Nations members worldwide.

According to Maitanmi, *et al.* (2013), the Yahoo assault encompasses the use of email address-harvesting tools to gather information about the potential victim's email address(es) from Internet access points to send such scam messages. It also involves phishing, which includes the offender cracking the passcodes of financial institutions or organizations for e-commerce, funds point cards, and e-marking, as well as phishing (cloning of products and (in which the fraudster follows up on the unsuspecting victim). Placing onerous financial demands on its victims is a common method employed by online con artists to defraud them. Usually, the victims of this crime are White women seeking Black men.

Along with the efforts of these scholars, it has been established that other types of cybercrime that might happen in Nigeria include blind dating and fake online dating. A notable example of this is the anti-language, anti-slang, and anti-cyber-scam subculture among urban youth in southwest Nigeria. Permit 514 internet con artist may ask gullible victims out with the prospect of marriage while posing as someone else. The current study is unique in that it adds a new dimension to the studies on cybercrime in Nigeria, but it's important to note that these studies serve as the springboard for the (current) study's engagement with the phenomenon.

Putting the current research into perspective: moving from the known to the unknown. It would therefore be fair to briefly summarize the research's contributions to our understanding of the dynamics of cybercrime in Nigeria while meticulously setting the current study in its context. Various facets of cybercrime in Nigeria and around the world have been studied in several academic papers. Buchanan and Grant (2001) give an overview of Nigerian fraud schemes and argue that the global, but particularly in Nigeria, rise of the Internet has allowed cybercrime to flourish.

Cybercriminals employ technology to conceal their identities and whereabouts, making it more challenging for law enforcement to locate them (Chawki and Wahab, 2006). Tive (2006) examines the tactics used and mentality of Nigerian fee scammers. He notices con artists using false lexical elements. Stajano and Wilson (2011) study examines the various fraud strategies used by Nigerian cyber-scammers and shows how security-engineering initiatives could help with the issue. The relationship between the Internet and Nigeria's emergence of the Yahoo boys and yahoo subculture is examined by Adeniran (2008).

The study finds that the Internet has helped to spread financial crime among young Nigerians and increase the number of internet frauds in Nigeria. According to Chawki (2009), Nigerian cyber scammers frequently employ anonymous servers, hijacked emails, and bogus websites to carry out their evil actions. He offers solutions to deal with this reprehensible behaviour within the confines of the country's criminal legislation. To combat cybercrime, he advised creating a high-level global network of coordination between national, regional, and international law enforcement agencies and police forces.

This network should work to increase global awareness, increase literacy rates, coordinate legislative initiatives, and take other measures. Costin *et al.* (2013) looked at the role that phone numbers play in online fraud schemes and used empirical data to determine their significance in 419 frauds. The Nigerian cyber scam, according to Isacenkova, *et al.* (2013), is a well-known sort of fraud in which the perpetrators trick the victim into paying a specific amount of money under the pretence that they will receive a bigger return in the future. The techniques that online con artists use to deceive and manipulate their gullible victims were the subject of this research. They concluded that online scammers craft their con emails carefully to persuade their victims that the conversations are real.

Contrary to popular belief, Ogunsanya (2015) examines the problem of cybercrime in Nigeria from an ethnographic perspective. She finds that it is a subset of all other corrupt cultural practices that are native to the country, such as money rituals and Advanced Free Fraud. He claims that the engagement of Nigerian youth in cybercrime has only helped to emphasize their consumerist way of life. Researchers looked at the strategies fraudsters employ to trick and control users online. The connection between human security, poverty, and cybercrime in Nigeria is examined by Adesina (2017). The grim reality is that the vast majority of cybercriminals execute their crimes to get money, she notes, despite the stereotype that computer crooks are lazy and greedy.

In other words, crime is a means of survival for these cybercriminals in the face of the challenging economic conditions that characterize Nigeria's socioeconomic sector. Researchers looked at the strategies fraudsters employ to trick and control users online. The importance of Nigerian hip-hop artists in the "institutionalization" of cybercrime in Nigerian society is examined by Ajayi and Bamgbose and Lazarus (2018). They have a strong conviction that a significant portion of the lyrics in hip-hop songs performed by Nigerian musicians openly support cybercrime and other social vices, especially among young Nigerians.

As was already mentioned, a critical analysis of the research reveals that none of them, particularly in terms of linguistics, have attempted to engage in cyber fraud in Nigeria. This research is important as a result. In the literature, financial scams have been discussed in a wide range of ways. There are numerous efficient descriptions. Financial

fraud is described as "crimes against property, especially the illegal conversion of another person's property to one's own" in the Wikipedia dictionary. Williams (2005) mentions corruption in his examination of financial crimes. Bribes, cronyism, nepotism, political donations, kickbacks, deceptive pricing, and frauds of all kinds are included in William4's (2005) list of frauds.

Even though some of the elements of financial crime have already been highlighted, the list is not all-inclusive. A variety of economic and financial violations committed both inside and outside the organization were addressed by the 2004 EFCC Act. Any type of fraud, drug trafficking, money laundering, embezzlement, bribery, looting, and other corrupt behaviours are among the main issues in the EFCC's (2004) definition. Tax evasion, currency manipulation, illegal oil extraction and bunkering, child labour, and child labour on the foreign exchange market are additional serious issues.

Both corporate financial crimes and the kinds of crimes committed by provision authors could be covered by this general term (William and Khan, 2005). There is evidence that financial crimes have helped bring down corporate businesses. Cotton (2003) attributes the failures of Enron, WorldCom, Tyco, and Adelphia to corporate misconduct. About $460 billion in losses were estimated. According to allegations, the management of Cadbury Nigeria Plc. illegally changed the company's documents, resulting in a loss of $15 million in Nigeria (15 Billion Naira).

Financial fraud and crimes against money were discovered to have been targeted at nine business institutions. It is alleged that several ways were used to misappropriate one trillion naira. The EFCC Act states that they are still investigating this (2004). Both individuals and organizations can do financial fraud in a variety of ways.

2.2 Forms of cybercrime

Scammers on the internet are continuously developing new techniques for carrying out their evil schemes. The forms listed below are just a sample of the various online scams; they are not meant to be comprehensive.

2.2.1 Hacking

Unauthorized entry, defacing, hijacking, bombing, denial-of-service assaults, diddling, super zapping, and eavesdropping are just a few examples of internet fraud. Some Internet users find hacking to be brilliant entertainment, while others see it as a serious

invasion of privacy and a danger to e-commerce. There are, according to the Information Security Advisory Group, about 100,000 hackers or crackers working today. Grey-hat hackers fall in the middle of the spectrum between white-hat and black-hat hackers, who discreetly infiltrate networks while conducting security tests for businesses. Numerous websites, including those of the US Department of Justice, US Air Force, Central Intelligence Agency, NASA, and other organizations, were compromised by hackers in 1990 (Sandeep, 2004).

In 1991, a significant American carmaker lost $500 million in potential future automobile designs as a result of a security compromise at its research lab. Due to other automakers stealing the design, this also decreased the company's market share. The Defense Department's networks were the target of 250 000 hacking attempts in 1995, according to a General Accounting Office survey. Even Microsoft was the target of hackers in 2000 (Handbook of Cyber Law, 2000).

2.2.2 Pirating

Digital technology makes flawlessly reproducing creative works like music and movies exceedingly straightforward, and the Internet provides a free and essentially anonymous way of transferring or sharing these pirated assets worldwide. According to studies by the Business Software Alliance (BSA), a world organization that represents leading software and e-commerce suppliers (www.bsa.org), global software piracy is an $11.8 billion problem (Privacy journal, 1996).

2.2.3 Stalking on the Internet

There is not a widely agreed-upon definition of "online stalking" yet. One typical description is the use of the Internet, e-mail, or another type of electronic interaction to stalk or harass someone. A pattern of threatening or irritating behaviour is called stalking. Cyberstalking is the practice of following people using modern technology like cell phones, fax machines, and other gadgets. There are many definitions of cyberstalking, and they vary depending on the country or region. A cyber-stalker can send repetitive, threatening, or harassing messages at scheduled or arbitrary intervals by just clicking a button. The anonymity of the Internet makes it possible to completely conceal the identity of a wrongdoer.

Additionally, violent crime in the actual world has increased as a result of cyberstalking. For instance, an anonymous person has harassed a South Carolina woman over years via email, threatening to kill her, assaulting her daughter sexually, and disclosing her home location to anybody with access to the Internet (Toronto Star, 1995). 20,000 people are allegedly stalked annually (Economic Times, 2004). Stalking laws have been passed in seven states (India, 2004).

2.2.4 Trading Illegally

This refers to the practice of engaging in illegal trade through the use of online resources such as chat rooms, message boards, newsgroups, and websites (e.g., fake drugs, human trafficking, etc.).

2.2.5 Squatting in the Digital World

Squatting is the practice of reserving a particular Internet domain name to later resell it for a higher price. A rush to register a company's name has resulted from the demand for well-known corporate addresses in cyberspace, even though a domain name's primary functional use is to identify a website online. Cybersquatting frequently takes the form of reserving websites with names of people or businesses. As a result, anytime a well-known person or business chooses to launch an official website and requires the domain name, cyber squatters will profit. Hertz and Panasonic are two prominent examples of cyber squatter victims.

2.2.6 Fraud

This category encompasses behaviours such as packet reading, accessing confidential information, bid fraud, investment fraud, escrow fraud, and other comparable behaviours. The Internet is regularly used by con artists to deceive users of particular websites (such as banks, building societies, and other financial organizations) into divulging their passwords or other personal information necessary to access their accounts. In response to emails asking them to do so, clients are frequently urged to check or confirm their credentials by visiting a website that appears trustworthy but is phony and inputting their passwords. Then, someone may use their personal information to get unauthorized access to the person's account.

2.2.7 Money Laundering

When money from public accounts is forcibly transferred online to private ones, this happens. Italian politicians think that the Sicilian Mafia is using online commerce and banking to launder vast quantities of money. In Nigeria, money laundering is a typical type of internet fraud.

2.2.8 Communication Services Theft

This involves employing software that is easily accessible online to access a company's phone switchboard or fraudulently obtaining an employee's access code. Fraudsters may seek to target victims in other countries when personal telephone verification checks are not feasible. For instance, it may be difficult to observe a transaction at first since money may be electronically removed from accounts late at night when a firm is closed. Early ATMs had a similar problem where accounts may fall into overdraft at night while the machine was "off-host" (Chapman & Smith).

2.2.9 Phishing

Phishing is the practice of posing as an official email from a respectable company to fool a person into providing personal information that will be used to steal their identity. The customer is sent to a website where they can reset their password, social security number, bank account, credit card, and more. In the US, 57 million Internet users have admitted to receiving emails that constitute phishing attempts, according to a Gartner survey (PC Quest, 1999).

2.3 Emerging cybercrimes methods and tricks

The following are examples of new Nigerian e-mail frauds:

2.3.1 Beneficiary of a Will Scam: The scammer emails the victim saying that she is a named beneficiary in an estranged relative's will and is therefore entitled to a substantial inheritance.

2.3.2 Online Charity: Hosting bogus charity websites that ask for money and supplies for nonexistent groups is another type of e-crime that is common in Nigeria. Unfortunately, this is how a lot of innocent people have been exploited.

2.3.3 Visa fraud: When the victim asks questions, the scammer launches a fake online bank and leads them to the page, which shows a deposit of millions of dollars. In Nigeria,

registering for university admission and even earning money online using a bogus website can result in visa fraud and university admission fraud. These techniques have been used to defraud thousands of individuals online.

2.3.4 An American soldier in Afghanistan or Iraq: The con artist meets an American soldier in Afghanistan or Iraq and requests personal and financial information to deposit money from a terrorist currency hoard he claims to have discovered.

2.3.5 Next of Kin Scam: To obtain funds from numerous banks and transfer fees, the victim is persuaded to assert an inheritance of millions of dollars held in a Nigerian bank by a long-lost relative.

2.3.6 Bogus cashier's check: After the victim posts an item for sale online, a bogus customer from Nigeria or another African country calls them. After that, a cheque or money order much larger than the item's asking price is issued to the victim. After that, the victim is told to send the con artist the cash difference. If the victim does not wait for the bank to authenticate the check, he runs the risk of losing thousands of dollars.

2.3.7 Lotteries: Some companies in Nigeria encourage customers to text or call in their responses to a situation that is being highlighted on television to draw in millions of viewers. Millions of Naira may be spent on such viewer calls or SMS, yet the payout may be as low as 10,000 Naira.

2.3.8 Donation Solicitations: The victim gets an email asking for "donations" to fight against a terrible African regime or tyrant. The victim is asked for bank account information so that the "gift" can be instantly withdrawn from the bank.

2.3.9 Reshipping: There are numerous clever strategies used by Nigerians to get Americans to take part in fraud. The "reshipping" scam is a common type of scam that begins on a single chat service. Friending a potential victim in a chat room is fraud. The victim is then urged to accept things that are later shipped by the assailant from Nigeria after placing online orders. Using the details of her stolen credit card, the criminal makes online purchases and has them mailed to America. To mail the items to a Nigerian address, the victim repackages the items (Mickinley, 2005).

2.3.10 Time Theft from Computer/Internet Services: Nigerian whiz kids have devised a method of linking Cyber Cafes to the networks of some ISPs in a way that is undetectable by the ISPs, allowing the Cafes to operate free.

2.3.11 Impersonating Foreign Relatives/Acquaintances: Victims get phone calls claiming to be from a relative in another country, like the United States of America, asking for help or asking for money to mail packages to them.

2.3.12 Phreaking: theft of telecommunication services, including, most recently, the cloning of mobile sim cards and the use of cereal box whistles to simulate phone call signals. A homemade cable that, when attached to a video player, may connect to multiple DSTV television stations is currently used to connect many Nigerian homes to DSTV products.

2.4 Intricacies of Emerging Tricks

Detecting and investigating various forms of e-crime can be extremely difficult due to several factors, even though strengthening law enforcement agencies' proficiency in this area is a crucial objective. In reality, while many crimes involving computers are simply old crimes that have been made more effective by the use of a computer, some are not (Thompson, 2009). Computer systems and information technology add several complicated issues to the field of criminal investigation with this kind of criminal behaviour. Here are a few examples:

a. The speed and strength of modern information technology make it harder and harder to detect and investigate computer crimes. A basic personal computer may easily connect to locations across many continents or hemispheres thanks to today's global communications networks. This presents important issues concerning jurisdiction, the accessibility of evidence, the coordination of the investigation, and the legal framework(s) that may be applied to criminal activity that occurs in this setting.
b. The formation of innovative notions that are unsupported by the law or other concepts is a result of new technologies. Some computer viruses, for instance, are very innocuous and have little impact on the computers they infect (although many benign viruses still cause unintentional damage). The resources of a system are used

by viruses, in contrast, without the owner's knowledge. As a result, any virus, no matter how benign, could be mistaken for system incursion, electronic vandalism, or a harmless practical joke. The fundamental criticism is that the legal system, and hence the definition of computer crime, are reactive and unable to account for new computational ideas or behaviours.

c. The ability to remain in the real world and the ability to be returned to the owner after duplication or theft are just a few of the information's unique and abstract features. Over the past 10 years, the legal system has struggled to address the effects of this in a computer-based environment. Because current definitions of theft and break-in, for instance, relate to conventional notions of physical damage (theft) or permanent deprivation or removal (break-in), it is clear that traditional ideas of copyright, patent rights, and theft have been strained when applied to software and computer-based information (break-ins). These two concepts are essentially unrelated to computer hacking or data theft from systems. The legal system is still working to relate these groundbreaking ideas to the current criminal justice system as a result.

d. Similar characteristics include the simplicity and scope of digital information adaptation. In other words, there are numerous different data formats in which a piece of data (i.e., a program) can be expressed. Additionally, it can be changed in many various ways, including theoretically, through encryption, or by turning it into a holographic image or a piece of music. It can be expressed as executable code (binaries), program text (source code), or any combination of these. The transformation method(s) must be known to translate the music, image, or encrypted data. As a result, it might eventually lose its legitimacy as informational law. As an alternative, some evaluation of its worth or utility as knowledge may be employed to judge its legality and financial status. It’s worth or commercial feasibility may also be estimated using this approach.

When information is compromised, it may be temporarily rendered inaccessible or encrypted rather than permanently erased, which has implications for system invasions (as in corrupted or wiped). These actions in no way constitute theft or deliberate destruction. On items like hard or floppy disks, magnetic tape, paper tape, computer printouts, and other

items, information can also be found in a physical form. These also raise classification issues for the legal system due to the possibility that various physical representations may be governed by various legal systems even when the information is comparable.

Additionally, Thompson (2009) identified several traits that make identifying, looking into, and prosecuting e-crime even more challenging:

i. Internet scams are typically low-profile, making them harder to identify
ii. Internet fraud can be carried out over long distances, spanning interstate and international jurisdictional borders
iii. 'Inside jobs' account for a substantial percentage of computer-related crimes;
iv. In a technologically complicated computer crime, locating and understanding the offender's method might be challenging once the crime has been identified.
v. Internet scams are typically low-profile, making them harder to identify;
vi. Internet fraud can be carried out over long distances
vii. Physical evidence is more elusive than in other commercial crimes; computerized information with evidentiary value can be changed or erased quickly with little to no evidence of tampering
viii. In a computerized world, issues surrounding the admission of evidence in court become much more problematic
ix. Moreover, it can be challenging to succinctly explain the technical aspects of a computer-related offence to a court.
x. Tracking down Offenders Comes with Risk
xi. According to the FBI, computer crimes cost billions of dollars each year.

Only 17 per cent of impacted firms, according to some estimates, notify law enforcement of these breaches due to worries about shareholder value and consumer confidence. They contend that disclosing internet scams exposes them to leaks and that constantly enhancing their electronic security measures is the only solution (Webster and Borchgrave, 2000). We examined a few of the problems and dangers associated with tracking.

The Difficulties of Conducting Investigations: Investigating cybercrimes on a national level is difficult enough. It is challenging to ensure that the evidence is acceptable as well as easily available, secure, and unaltered. When cross-border difficulties are taken

into account, the legal, evidentiary, and jurisdictional challenges significantly worsen a law enforcement body would need to know who to call first to collaborate with a matching agency in another nation and protect the environment. After establishing contact with the appropriate authority in a foreign state, the investigative agency must deal with the varying levels of competence in other nations.

Legal limitations may make coordination difficult as well. Some nations' disregard for internet frauds: A recent study found that several nations aren't even close to being ready to handle internet scams. The legal systems of only nine of the fifty-two nations can successfully pursue online fraud. Even when there is international cooperation in finding and apprehending a suspect, the country where the "victim" computers are located may have a great deal of difficulty locating the criminal for trial.

Obtaining Witness Cooperation: One of the most difficult challenges for investigators is getting the cooperation of complainants and witnesses. It cannot be denied that many who have been the victims of cybercrime are reluctant to report their offences to the police. Only 25% of the scams described in the survey were reported to the authorities, and only 28% of the respondents were satisfied with the investigation that followed, according to Ernst & Young's most recent 8th Global Study on Business Fraud. seeking out suspects It can be challenging for e-crime investigators to find the proper suspects.

When the wrong individual is held, this could have disastrous results. Being able to conceal one's identity in a variety of ways thanks to digital technology makes it challenging to pinpoint exactly who used a computer to initiate illicit contact. This issue is quite common in workplaces where numerous people may have access to a computer and where passwords are known and shared. Cryptography-related issues When dealing with data that has been encrypted by suspects who won't divulge the password or decryption key, e-crime detectives have a difficult situation. The Gathering and Preservation of Useful Information: Finding and safeguarding electronic evidence can be challenging since crucial evidence and related time and date records can be altered simply by turning on a computer. To find the required information, it can also be necessary to sift through a mountain of data.

2.5 An examination of Nigeria-originated cybercrime

Cybercrime unquestionably has a bad impact on Nigeria's reputation. Internet fraud is a source of worry and humiliation for the nation, as demonstrated by Olusegun Obasanjo,

a former president of Nigeria, who founded the Nigeria Cyber Crime Working Group (NCWG). Commercial, social, and internet platforms enable the availability of a wide range of educational options. The Internet does, however, pose its own particular set of hazards, as evidenced by the case of cybercrime.

2.5.1 Cybercrime Incidents

Fake lotteries and the most complex cyber frauds are only a few of the instances mentioned here. Elekwe, a chubby 28-year-old guy who holds a diploma in computer technology but has been jobless for two years, made a lot of money from the prank. He now owns two homes and three nice vehicles as a result of his adventures. In July 2001, security agents in Ghana detained four Nigerians they believed were operating a "419" internet fraud scheme to deceive unwary foreign investors. Prospective investors allege that their business activities cost them millions of dollars.

Recently, two young men were detained for making two fictitious laptop purchases from a woman's website. Soon after giving birth, government agents captured them. In exchange for developing a website that promoted alluring but fraudulent procurement contracts, Mike Amadi was given a 16-year term. Even though he appeared to be the EFCC Chairman, an undercover agent posing as an Italian businessman was able to capture him.

The greatest con artist in history, Amaka Anajemba, got imprisoned. She also had to pay back $25.5 million of the $242 million in stolen funds from a Brazilian bank that she and others were involved. On July 16, 2006, a story on a current online scam between Yekini Labaika, 24, of Osun State, Nigeria, and Thumbelina Hinshaw, 42, an American nurse, was published in the Sunday PUNCH newspaper. The two victims were Thumbelina Hinshaw and Yekini Labaika. He devised shady schemes to steal the victim of $16,200 and several valuable items. The con man was given a cumulative term of 19 years in prison after being found guilty on eight of the accusations brought against him.

These kinds of things are happening more frequently these days. Nevertheless, several young men who loot businesses and innocent victims are successful in carrying out these criminal operations. Raymond Abbas, also known as "hushpuppy," is currently wanted on financial charges in the United States of America for conspiring to launder money obtained through business email compromise frauds and other scams, including schemes that fooled a U.S. law company. He had a net worth of about $40 million before

his arrest by the Dubai police in June 2020 and his extradition to the US; he had illegally transferred $14.7 million from a foreign financial institution, and he had planned to steal $124 million from an English football team.

He has uploaded images and videos of his showy purchases on Instagram, where he has more than 2.5 million followers and other valuables which include luxury vehicles, timepieces, diamonds, and himself boarding a private jet with Nigerian athletes, actors, and politicians like Senator Dino Melaye and Senator Bukola Saraki, the former president of the country's senate. He has also shared pictures and videos of himself with other celebrities, including Sen. even though he asserted to be a real estate developer (Wikipedia, 2020).

2.5.2 Telephone Crime Instances

The rate of e-crime in Nigeria that is related to telecommunications is rising alarmingly quickly. The Global System for Mobile Telecommunication (GSM) has brought with it frauds, which Nigeria is now subject to. The "send me credit" scam has received numerous people around the nation. When it happened, The Pacific Journal of Science and Technology was involved. A mother in Ibadan was tricked into giving 5,000 naira by a conman so that his belongings could be removed from South Korea.

The conman purported to be the woman's son over the phone. The money was to be sent as a phone recharge card, per the scammer's request. She didn't recognize this till she understood she had been tricked. The head of the computer science department at the Nigeria's Federal University of Technology encountered a like circumstance. When the department head requested the account number in Osogbo, Osun State, Nigeria, the con artist's luck ran out. Authorities were informed of the event.

Another example is a professor at Lagos State University who found out he had won N1 million in a recent MTN promotion. A fake MTN employee's phone number was provided in the mail. When they called the specified number, the personnel informed the professor that he had won. The winner was then told to text the number 33354 with his or her contact details, including the address where the N1 million check would be sent. In response, a computerized system asked for N6,000 in recharge cards to pay the courier's fee for delivering the cheque. He took the cash as the check was never delivered. Many further cases had not been reported.

2.6 Cybercrime Statistics in Nigeria

The amount of money lost as a result of an internet scam cannot be calculated. An MTN campaign was still going on when word reached a lecturer at Lagos State University that he had won N1 million. A letter with a fake MTN employee's phone number was then sent to him. After dialling the proper number, the staff informed the professor that he was one of the fortunate recipients. As soon as the winner's contact information was texted to 33354, an automated system demanded N6,000 in recharge cards from him to pay for the courier who would deliver the check. The cheque was never cashed, but he received the cash.

In a separate incident, a young guy was recently detained in the Ikorodu neighbourhood of Lagos state for defrauding hundreds of people by obtaining their bank verification numbers (BVNs), after which he took thousands of dollars from his victims. Numerous such incidents went unreported. The United Kingdom is in second place with $520 million in losses, followed by Spain and Japan, each with roughly $320 million. According to the article, con artists posing as Nigerians defrauded the respected founding director of the University of California's Psychiatry Department in Irvine, USA, Luiz Gottschalk, of $3 million in March of last year.

According to a recent study, software piracy costs Nigeria about $80 million annually. The Institute of Digital Communication, a market research and forecasting firm in South Africa, conducted a study on behalf of the Business Software Alliance of South Africa. According to the American National Fraud Information Centre, Nigerian money claims surged at a rate of up to 900 per cent in 2001, making them the fastest-growing web fraud. According to the Center, Nigeria has a very significant per-capita impact on internet fraud.

2.7 Impact of cybercrime on Nigeria

According to Tunji Ogunleye, an ICT security consultant and member of the Nigeria Cyber Crime Working Group, the incidence of e-crime in Nigeria has overtaken the rate of Internet usage in the country (NCWG). Nigeria, in his estimation, ranks 56th out of 60 nations for Internet adoption while ranking third for fraud attempts. Residents of Nigeria have previously been harmed by cybercrime. One of the nations with the highest

levels of corruption, according to international organizations like Transparency International, is Nigeria.

Nigerian internet fraud may impede technology advancement, which is essential for higher output and, eventually, socioeconomic growth. This is because foreign financial institutions are becoming increasingly wary of Nigerian paper-based financial instruments. Checks and drafts from Nigerian banks are not commonly used as payment methods. International methods have previously been used by ISPs and email providers to blacklist Nigeria. Numerous businesses have restricted access to substantial portions of the Internet network as well as Nigerian traffic. To make it simpler to recognize and isolate Nigerian email traffic, more modern and sophisticated technologies are being developed.

It's almost certain that unauthorized access to vital national infrastructure and information security resources would result in damage. How Internet crime would impact Nigeria's economy is unknown. It is becoming increasingly clear that there will be significant economic and financial repercussions. Due to the requirement for sufficient verification, international banks routinely postpone financial transactions involving Nigeria, and foreign investors frequently view Nigeria as an unfavourable market.

2.8 The Reasons behind cybercrime Situation

We can wonder why there has been such an increase in e-crime in Nigeria, and what reasons have rendered Nigerians so vulnerable to internet scams. The explanations are not far-fetched, given the country's current economy is a slump and political instability, and they include the following:

1. **Unemployment:** Nigeria's alarmingly high unemployment rate is increasing daily. Businesses are closing and financial institutions are failing. Punch (2020). The federal government has recommended mass layoffs for 33,000 public servants. Employers are also firing workers in large numbers. Financial companies have implemented mass layoffs based on unjustified conclusions and set arbitrary age limits for job applicants (Makinwa, 2015).
2. **Poverty Rate**: Nigeria is regarded as a third-world country on a global scale. The amount of poor people keeps rising. The richest people continue to get wealthy, while the poorest people continue to get poorer. Small businesses have had to close because of a lack of basic services and an unstable power supply (Gboyega, 2014)

3. **Corruption**: Nigeria was ranked third on the list of the world's most corrupt countries. Corruption was accepted as a way of life in Nigeria until 1999.
4. **Gullibility/Greed of the victims**: Most internet scam victims display some degree of greed or gullibility. They typically don't conduct a thorough investigation before engaging in negotiations. Because of their greed, the victims keep the supposedly life-changing transaction they've just learned about a secret until they become victims themselves (Emeka, 2012).
5. **Lack of Standards and National Central Control:** According to Charles Emeruwa, a consultant with the Nigeria Cyber Crime Working Group, the absence of laws, regulations, and a computer security and protection act hinders real business (NCCWG). Outsourcing and foreign direct investment (FDI) increase computer abuse and misuse (Nwoke, 2018).
6. **Inadequate Infrastructure:** Modern, sophisticated information and communication technology equipment is required for efficient monitoring and arrest.
7. **Lack of National Functional Databases**: A national database may be utilized to track down the perpetrators of these terrible acts by looking up historical personal records about them and keeping track of their whereabouts.
8. **The proliferation of Cybercrimes:** In order to make ends meet, several entrepreneurs opened cybercafés that serve as safe havens for syndicates to conduct their activities by providing night surfing services to potential consumers without being observed or monitored. The porousness of the Internet There is no central authority on the Internet. Consequently, the chaos that is being felt right now (Obi, 2021).
9. **Get-Rich Syndrome**: In today's Nigeria, practically everyone, especially the youth, aspires to get rich quickly and easily. The current online fraud tendencies have been fostered by this get-rich-quick mentality (Gani, 2016).
10. **Nursing personal greed**: research revealed that one of the major reasons why the internet scam situation in the country presently is at its peak presently is because a great number of Nigerians are nursing their greed.

2.8.1 Origin of Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC) was established in 2002 by an Act of the National Assembly, and it underwent an update in 2004. At the time, Olusegun Obasanjo, a former president, was in control. The federal government's commitment to upholding all economic and financial criminal laws to revive Nigeria's economy led to the creation of the commission (EFCC information). The economy and reputation of Nigeria were seriously threatened by Economic and Financial Crime before the establishment of the EFCC. The nation has previously provided sanctuary to those who had engaged in financial and economic crimes. Fraud, subpar economic management, corruption, and a lack of accountability have aggravated the economy.

The EFCC Act constituted a significant divergence from earlier enabling laws for preventing economic and financial crimes in terms of authority, authority, and obligations. The commission has received backing from the Nigerian president, the legislature, and other important security and law enforcement organizations. The EFCC is made up of a variety of units that assist them in performing their job in an efficient manner (Olukoya, 2017). They include:

a. Executive chairman's office
b. The commission secretary's office
c. Organizational support for the director
d. Zonal workplaces
e. Units that are in use
f. Account and Financial Unit
g. Unit for human resources
h. Units that collaborate externally
i. Publicity and the media
j. The unit for information, communication, and telecommunication
k. Unit for Financial Intelligence in Nigeria (NFIU)
l. Servicemen unit/Inspectorate Directorate.
m. Institutions for training and research

2.9 Mandates of the Commission

Conducting investigations and defending the law against economic and financial crimes in all of their forms are among the responsibilities of the EFCC. The EFCC Information Handbook 2 lists the following as the primary duties and requirements outlined in the enabling Act:

a) The proper implementation and enforcement of the Act's provisions.
b) Taking steps to hunt down, freeze, confiscate, or seize assets that are essentially similar to money earned through financial or economic crimes, or terrorist activities, or to find, track, and seize the money that was.
c) The appraisal by the government, individual people, or organizations of monetary loss and other losses of a comparable sort.
d) The implementation of measures to lessen and prevent financial and economic crimes to locate the people, businesses, or groups in charge.
e) Assisting other governmental entities both inside and outside of Nigeria in carrying out all or a portion of the commission's responsibilities.

2.9.1 Matters EFCC Investigates

The EFCC focuses its investigations on financial crimes and aids criminals who disobey the law in forfeiting their assets by assisting them.

i. **Banking Fraud:** This sector's objective is to find and bring criminal groups and individuals who engage in fraud schemes against our nation's financial institutions to justice. Typically, it looks at things like bank fraud that have an impact on banks and other financial institutions. Here are a few examples: stealing money from other nations, utilizing phony checks, cashing phony checks, and scamming other financial institutions.

ii. **Government Fraud:** In this area, the EFCC discusses issues with transparency, accountability, and good governance. In addition, it examines crimes including official corruption, abuse of public office, and bribery of public officials, as well as theft of public funds through the granting of fake contracts, corruption in the distribution of land, tax fraud, stock market fraud, money laundering, and oil bunkering.

iii. **Advance Fee Fraud:** This type of fraud, which frequently surfaces during investigations into advance fee fraud, entails obtaining money through several shady schemes, including credit card fraud, inheritance fraud, contract fraud, job fraud, lottery fraud, wash fraud (money laundering fraud), marriage fraud, immigration fraud defence, and religious fraud. Additionally, the commission looks into cases of cybercrime countrywide that are committed by patrons or proprietors of cybercafés.

2.10 Constraints Faced by EFCC in Curbing Cybercrime in Nigeria

When it comes to identifying and combating financial crime in both the public and private sectors, the commission has over the years run across a range of complicated, challenging, and recurrent difficulties. These restrictions were not due to her incompetence or refusal to carry out her monitoring responsibilities, but rather to administrative quirks in criminal prosecution and a focus on economic crime prosecution. The commission specifically addresses the following types of internet fraud in Nigeria. Accounting limitations and Legal limitations.

2.10.1 Accounting Constraints

While auditing is the process of reviewing these records, constructing a summary statement in light of the analysis, and assessing if the summary statement is a reliable representation of the financial operations, the practice of recording and comprehending financial transactions is known as accounting. Following Adeniyi (2004), auditing is

> "the independent examination of and expression of opinion on, the financial statements of an enterprise by an appointed auditor in obedience of the appointment and compliance with any relevant statutory obligation, the executive chairman's office being one of them".

Even if there were no claims of legal infractions in every one of these records, accountants and auditors are used to, create records that will be used in a range of administrative and civil legal procedures. One of them is the executive chairman's office. Auditors and accountants generally do not investigate economic crimes and frauds as their primary aim due to their lack of expertise in the procedure for gathering and keeping evidence in a way that secures its inclusion in subsequent criminal proceedings.

These specialists are now more regularly involved in investigations and criminal prosecutions than they were in the past as economic fraud prosecution has gotten more attention. Even public sector auditors lack the skills necessary to spot the point at which a detained witness becomes a suspect criminal and offer aid. Even if the evidence is important or even compelling and vivid, they might not be aware of the higher standard of proof required in criminal trials to establish some elements of a civil case. Contrarily, criminal investigators are often less prepared and skilled than accountants or auditors when it comes to finding and documenting the paper trails leading up to and from each financial transaction.

Furthermore, they (criminal investigators) lack the information and materials necessary to establish civil and administrative rule violations, which could result in sanctions that are more effective at holding an activity's cause accountable than any criminal penalties on the books. Even since 1970 almost every major federal department has had an office of the inspector general, and even though previously separate accounting/auditing units and criminal investigative units had frequently been united in that office to monitor and stop every sort of fraud in the public sector, all of them had undergone irreconcilable conflict without any prospect of being separated, frequently we have heard auditors/accountants remark that their needed level of scrutiny is not sufficient.

2.10.2 Legal Constraints

Whether they are accountants, auditors, or other specialized professionals, investigators who focus on financial and economic crimes must navigate a very complex and tough area of the law, both criminal and civil. Legal professionals have long struggled to discern between ideas like fraud, embezzlement, theft by deception, and the acquisition of valuable objects through deception. Numerous nations have combined these accusations into a single "stealing" felony even though there are frequently alternatives to criminal prosecution, civil remedies, and administrative or regulatory remedies to modernize and simplify the law.

The prohibition of exceptionally offensive behaviour is one of them. Since "Economic Crime" is not specifically defined by law, it is the court that will be evaluating the case that has the burden of proof. As a result, the EFCC was established to address this problem and formulate charges that are appropriate for the numerous offences.

According to Mohammed (2004), the EFCC Act of 2003 created the Economic and Financial Crime Commission as a body corporate to carry out and oversee the Act's provisions. It has the authority to coordinate the several groups attempting to prevent money laundering and ensure that all financial and economic crimes are against the law in Nigeria. It is a recognized subset of financial intelligence in Nigeria. According to the EFCC Act of 2003, the commission's various legislative duties include dealing with economic and financial violations as well as preventing terrorism and terrorist tendencies. There are still issues even if we have been effective in locating, catching, and sentencing perpetrators.

2.11 Different Ways Cybercrime has been addressed by the EFCC

Microsoft Corporation and the Nigerian government signed a Memorandum of Understanding on October 14, 2005, in London, setting the stage for future cooperation between Microsoft and the Economic Community of West African States. To fight cybercrime, the Nigerian Financial Crimes Commission (EFCC) was created. This agreement, the first of its kind between Microsoft and an African nation, will benefit Nigerian policymakers by encouraging foreign investment, long-term economic growth, and a safe environment for technological advancement. An excellent example of public-private cooperation is the effort to combat spam, financial fraud, phishing, spyware, viruses, worms, hazardous code releases, and counterfeiting.

Through the Nigerian Cyber Crime Working Group, the Nigerian government has developed and is putting into effect legislation to ensure the security of computer systems and networks as well as the preservation of Nigeria's crucial ICT infrastructure (NCWG). The group's members include representatives from the National Intelligence Agency, the Department of State Services, the Nigerian Police, the EFCC, the Nigerian Communication Commission, and the main commercial ICT businesses (such as Internet Service Providers. The working group is laying the groundwork for the creation of an internet fraud agency that will eventually be in charge of combating internet fraud by working to educate the public, build institutional consensus among existing agencies, provide technical assistance to the National Assembly on internet fraud, and draft the Cyber Crime Act.

Nigerian authorities are taking the lead in combating online fraud and collaborating with foreign law enforcement agencies. One of them is the executive chairman's office.

After the 2005 Computer Crime and Security Survey, which was conducted by the FBI, the African Information Security Association (AISA) was founded to boost awareness of computer security and online scams throughout the continent. According to a statement, AISA was founded to advance global norms for data, computer, and internet security, combat online fraud, conduct annual information security audits, enhance legal and regulatory frameworks, and build networks and linkages across Africa.

2.12 Power of EFCC in Controlling Crime

The commission has the power to:

a) Order the beginning of an investigation to discover whether someone has broken the law
b) It can also check to see if anyone is breaking the law right now. A person should have their properties scrutinized if the commission decides that their lifestyle and the size of their properties are out of proportion to their income.

The commission is also responsible for upholding the laws listed below that came before them.

a. The Advance Fee Fraud and Other Related Offences Act revisions from 1995.
b. The Institutions Act of 1994, as modified, contains provisions addressing financial misconduct and debt collection from failing institutions.
c. Act Concerning Different Offenses (3) (cap. 401: LFN).
d. The criminal code, penal code, and any other laws or regulations governing economic and financial offences.

2.12 Achievements of EFCC on Cybercrime

The EFCC was founded as a result of the EFCC Establishment Act of 2004. By taking this action, we have made it much simpler to acquire a Nigerian attitude and dispelled any uncertainty over our goals as a people and a country. An objective of the EFCC in carrying out her duty has been to restore responsibility, integrity, transparency, and knowledge in the management of public resources. The position of executive chairman is one illustration of one of them. In Ajibade, (2017) presentation was made to the Senate on September 27, 2016.

Former EFCC executive chairman Mallam Nuhu Ribadu said:

> 'We at the Economic and Financial Crime Commission (EFCC) never forget that we were given a mandate by this chamber and that we are ambassadors for the vision you created, I stand gladly before you tonight to tell you about just a few of our modest successes thus far in carrying out the commission's mandate for prosecution and prevention. 88 people in total were convicted, $5 billion in assets and cash were seized, 4324 petitions were submitted, 2103 cases were being looked into, 306 cases were in court, 2000 arrests were made, a large number of houses, lots, expensive cars, planes, and oil tankers were located, and 2000 arrests were made' (Alaba, Bolaji, and Awolabi, 2016).

The Commission (EFCC) was able to successfully encourage investment in the financial and industrial sectors of the economy by developing a system of legality. It is crucial to acknowledge the EFCC's accomplishments in light of the difficulties it has encountered and the toxic atmosphere it operates. The Anti-Corruption Revolution campaign (ANCOR), a public/civil society partnership program, increased public awareness of the issues that corruption has brought in addition to equipping citizens to lead the anti-corruption movement (Fashola, Jegede, Olukoya & Adeboye, 2018).

2.13 Theoretical Framework

A theory, according to McQuade (2006), is a group of interconnected, testable hypotheses that make an effort to explain a phenomenon. Theory can be used to create the most effective plans for controlling and preventing crime, safeguarding vital infrastructure, and securing information systems. The classical school of criminology, which was centred on the notions of rational choice and deterrence, focused exclusively on eighteenth-century legal systems. It criticized or decried the harsh punishments meted out to lawbreakers arbitrarily and without regard for justice, fairness, or human rights (Williams & McShane 1993).

This literature, according to McQuade (2006), did not address the significance of crimes committed using technology or examine "the social, physical, or psychological ramifications of technologies utilized to punish offenders." The integration of computing and communications has started to alter how we live and how we commit a crime, but it's critical to stress that "virtual criminality" still falls under the same classification as traditional crime, according to Grabosky (2001).

The "time-honored motive of greed, passion, power, revenge, adventure and the desire to taste forbidden fruit" was still present in those who committed crimes involving computers, he writes. To understand the causes of victimization, the effect of technology on criminal behaviour, and the applicability of conventional theories of crime to virtual offences, a criminological study has widened its scope over the past two decades (Bossler and Holt, 2014).

According to Clarke, the internet has produced a novel setting where traditional 84 crimes like fraud, identity theft, and child pornography can thrive (2004:55). Criminologists agree that new opportunities for crime and victims have been generated by technology improvements. Reyns (2013) went on to remark that the development of the Internet in particular shows how even little technology advancements may have a substantial impact on society's day-to-day operations. The effectiveness of the legislation is determined by the criminological theory that supports the behaviour that criminal law seeks to regulate or prevent, claims Kigerl (2012).

2.13.1 General Deterrence Theory and Its Criticism

Cesare Beccaria and Jeremy Bentham, two utilitarian philosophers from the eighteenth century, developed the general deterrence theory. Both of them thought that crime was an attack on society as much as on the individual (Wikipedia, 2022). Because strong, quick, and specific consequences can deter criminal activity, general deterrence theory incorporates choice theory and rational choice theory. Increased fines and punishments, according to this theory, could either encourage small offences or serve as a deterrence to criminal behaviour. The public announcement of potential punishment and actual punishment is a crucial element of deterrence (McQuade, 2006).

The central tenet of the global deterrence theory is that offenders ought to face consequences and the public ought to be made aware of them. Cybercriminals and other IT abusers may be subject to unofficial sanctions. Even if this theory is acceptable for this study, it is still important to collect empirical quantitative and qualitative data through surveys and interviews to determine whether deterrence is a workable strategy for preventing crime. This hypothesis was disproved by the study's interpretivism worldview and qualitative data collection approach.

The deterrence theory has received some criticism because it makes three assumptions, which are;

1. Know what the penalties for a crime are
2. Have good control over their actions
3. Think things through and make choices about their behaviour based on logic, not passion

In the case of many crimes, these three assumptions just are not true. Even so, deterrence theory does seem to have some merit, especially in the case of drunk driving.

2.14 Application of Theory to the Study

Choice theory and rational choice theory are incorporated into general deterrence theory because the severity, promptness, and certainty of punishment can deter criminal behaviour. This concept suggests that stiffer fines and punishments may either encourage small violations or entirely deter criminal activity. Making public knowledge of potential and current penalties is a crucial element of deterrence (McQuade, 2006). The key assumption of the global deterrence theory is that offenders should face consequences and have their deeds publicly known.

Cybercriminals and others who abuse it may be subject to unofficial sanctions. Even if this theory applies to our research, it would still be important to evaluate if deterrence is a practical crime prevention technique in Nigeria using empirical quantitative and qualitative data from surveys and interviews. due to the qualitative data gathering strategy and interpretivism foundation of the study. The theoretical framework chapter's final section examines both traditional and contemporary criminological theories and how they can be used to comprehend cybercrime in the context of the study. The chosen research theory was argued for throughout the entire chapter.

CHAPTER THREE
METHODOLOGY

3.0 Introduction

This covers the method of systematization (study design and layout), the tools used to collect and analyze data, and the theoretical underpinnings. In other words, the topics covered in this chapter are (a) research design, (b) study area, (c) data collection method, (d) selected sample, (e) methods for gathering qualitative data, and (f) data analysis using NVIVO. The study's ethical issues are also covered in this chapter, as well as its limitations.

3.1 Research Design

The majority of this project's research will be descriptive, and its approach will comprise key informant interviews, the utilization of primary and secondary data sources, and statistical methods for data analysis and interpretation.

3.2 The Study Area

This study aims to evaluate the contribution made by the EFCC to lowering cybercrime in Nigeria using data from all three senatorial districts in Kwara State as well as a few selected government parastatals. The researcher chose Kwara state as the focus of her study due to the state's recent rise in cybercrime activity and the large number of youths there who have been found guilty by the EFCC of cyber-related charges (Hassan and Makinde 2021).

3.3 Study Population

The target population for this study is young people between the ages of 18 and 30. This age range was chosen since the majority of cybercrime criminals are young persons in this age range (Tade and Aliyu, 2011). Instead of the planned 20 essential informants, 15 crucial informants were spoken with because the informant was unwilling to provide in-depth information and because the informant gathering process was inadequate. In the study, deliberate sampling was employed. This sampling strategy is used when specific individuals have prior knowledge and are in the best position to offer the essential information.

Organisation	**No. of Informants**	**Status**
EFCC Officials	5	Operational Unit/ NFIU Unit
Selected Youths	10	Unemployed Youths/Universities Dropout
Total	15	

Five EFCC employees, two from the operational unit and three from the NFIU section, were interviewed by the researcher at the EFCC zonal office in Kwara State, Nigeria. The researcher also conducted interviews with ten young people, including two youth leaders from each of the three senatorial districts in Kwara State (Kwara central, Kwara north, and Kwara south) and four young people chosen at random from the senatorial district.

3.4 Data Analysis

The study will include primary and secondary sources of information. Journal entries, bank records, books, newspapers, articles, documents, oral histories, social media, Google searches, etc. are used to acquire secondary data, whereas interviews are used to collect primary data. As a technique for data analysis, the researcher used content analysis with NVIVO.

CHAPTER FOUR
DATA ANALYSIS, PRESENTATION OF RESULTS AND INTERPRETATION

4.1 Introduction

This chapter presents the results of data obtained from the in-depth interviews conducted for this study

4.2 Data Presentation

The data obtained for the study are presented using table and graphic illustrations to show information on the in-depth interviews conducted and retrieved from the key informants. 15 interviews were conducted across the relevant agencies, which include the EFCC zonal office in Kwara State, Nigeria, and all the three senatorial districts in Kwara State, Nigeria.

4.3 Demographic Characteristics of Key Informants

The table below depicts the demographic characteristics of the key informants, showing questions and their responses.

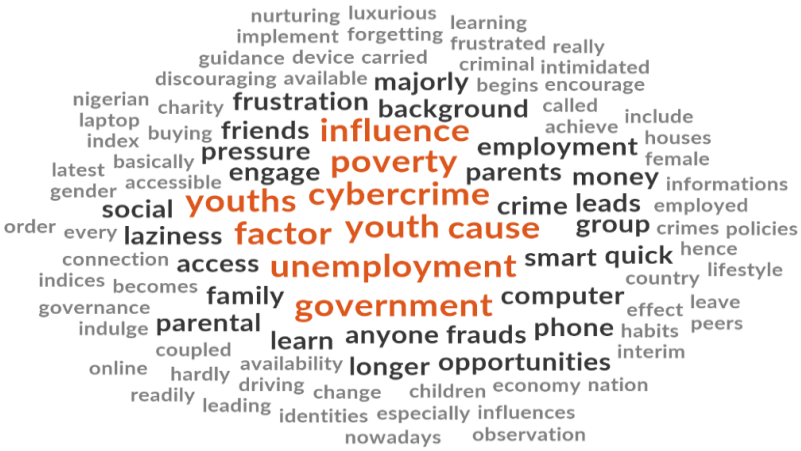
Informants	**Age/Rank**	**Male**	**Female**
EFCC Officials	Level 15 And Above	3	2
Selected Youths	18 Years And Above	7	3

4.3.1 Results on the Indices that Encouraged Youths' Participation in Cybercrime

	Question 1: what are the indices/factors that encouraged youths' participation in cybercrime
R1	One major factor is the government, the government hardly implements policies made, there are no jobs, and the government has not done well for her youth. There is also access to the internet as one major problem and peer influence.
R2	Such indices include Unemployment, Poverty, Peer group influence and access to technology especially through the use of computers or laptops, to get all sought information.
R3	I would say laziness and frustration there is this saying that the youth nowadays want short cut an easy way to success, it's pure laziness, youth not ready to work. Unemployment is also another issue and lack of strong criminal laws.
R4	Poor parental guidance and majorly poverty and unemployment are the major index that encourages cybercrime. Also, the availability of the internet on any smart device, even if you aren't doing crime, the Internet that can be easily accessible to anyone with a smartphone or computer can teach you several ways to scam people. One can learn how to change and hide their identity online as well as how to go unnoticed on the internet.
R5	The flow of money is very low, in the sense that there is no employment and even those that are employed are underemployed. The nation is not ready to support the youth and this is why they are involved in this quick money syndrome.

R6	Majorly it's the Nigerian government, there are no jobs, unemployment is the order of the day, the youth are not working and they need to engage themselves in one thing or the other and that is why so many of them are going into cybercrime. Family background is also a factor interim of upbringing. Also, poverty, when people don't have jobs the ripple effect is that it tends people to poverty and with that people turn to cybercrime for quick cash.
R7	Lack of job opportunities for the youths, they are discouraging youth from going to school with this constant strike and it can lead youth to engage in these frauds. So yes, unemployment is a huge factor.
R8	The situation of things in the country is bad, so I would say because of bad governance youth indulge in this crime, and they try to fight every day to get jobs. Parents also have a lot to do in other to achieve their aim, internet fraud is carried out by both males and females it is not gendered specific.
R9	The family background is a cause or a reason that leads these youths to get involved in cybercrime, parents no longer have time to train their children and these youths pick up habits from their peers, who in turn influence them, so I would say peer group influence is also a major cause.
R10	Parents are no longer nurturing their wards in the way that they should go, they leave the bulk of the work for the teachers, forgetting that charity begins at home. Poor parental training is also a cause.
R11	Peer influence is a factor that makes youth get involved in this type of crime. So many youths are easily intimidated, they want to make fast and get rich no matter the cost because their friends are driving the latest cars and buying houses. This peer pressure of influence becomes too much.
R12	So many youths are frustrated with the way the government and the economy are going, there is no employment, and they cannot make ends meet on their own. No job opportunities. Even when you find you need the connection to get in. this has led so many youths into frustration.
R13	Having a smartphone is also a cause or something that leads one to cybercrime, the internet is easily and readily available hence anyone can learn the trade, by observation from friends who engage in these crimes, or even by learning it over the internet.
R14	I believe that social media is also a factor that can lead these youths to engage in cybercrime, these so-called cybercrime offenders show off their luxurious lifestyle on social media for the world to see, these, in turn, put pressure on these youth watching from afar to be like that coupled with unemployment problem and even poverty.
R15	From what I have observed, poverty, unemployment and peer pressure are leading causes of cybercrime.

As argued by the respondents, there are cascading factors that had encouraged youths' participation in cybercrime, which include corruption, unemployment, peer group, etc. According to the word cloud representation below, the most emphasized factors that encouraged youths' participation in cybercrime are; poverty, frustration, laziness, unemployment, parental upbringing, etc.



4.3.2 Results on the Reasons Why Youth are Heavily Participating in Cybercrimes

	Question 2: What are the reasons why youth are heavily participating in cybercrime?
R1	The government in Kwara state is not trying, they are not giving the youth good job opportunity and I think that is the cause.
R2	These youths see it as a competition, profession and a means of living that are best known to themselves. They do it no matter the cost, some even find themselves ending their lives, or doing rituals to get money.
R3	First, I would say the situation in the state is not palatable, there is so much unemployment that these graduating youths have to be faced with, and many of them some that I know in the neighbourhood are still looking for jobs, going for interviews but then no positive replies, so because of this many of them result to the shortest way to earn a living but then it still boils back to laziness because I believe something can be done out of nothing. The get-rich-quick syndrome is just too much among these youths.
R4	Because of the government's inability to provide jobs or organizations where people can work and earn a living. It becomes difficult for these youths to able have a good standard of living as a result of unemployment.
R5	From what I have observed, youth in Kwara state is not ready for any work that would stress them, they don't want to do any work, so many of them just feel my friend has done it and has made it, let me just copy suit and do same, this is why the majority of the youth are involved in cybercrime. So, laziness is one serious reason.
R6	Kwara State doesn't have companies, even the schools are questionable, the youths are looking for ways to survive, and for them to survive they engage in either cybercrime or betting. Lack of means of survival leads these youths to poverty.

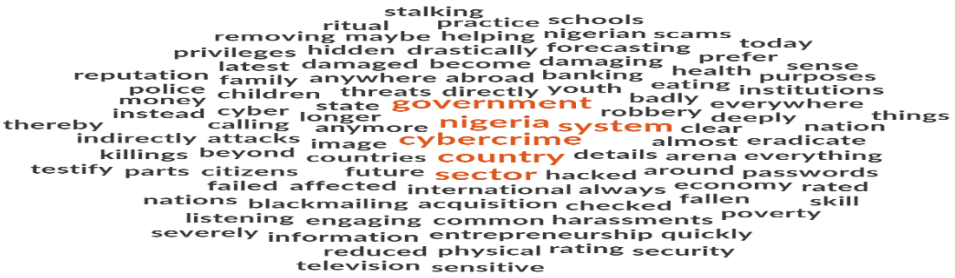
R7	Unemployment, laziness, many graduates are out there looking for jobs, most of them cannot do hard work, they are lazy and don't want to work. They think if you sit at home and press your laptop you can raise millions of naira instead of them to go out there and looking for a job, that pay so little and sometimes delay in paying these salaries with so many issues, so they think that its ok to participate in cybercrime.
R8	I think it is because of poverty, it is one of the major reasons, then imitation my friend has this I want it too, peer pressure also.
R9	Corruption is the main thing in this country, it has eaten deep into us. No one wants to earn an honest living anymore.
R10	I would say corruption, a lot of crimes go unpunished and these give more people reasons to commit it since they know they can bribe their way out of it.
R11	The kind of lavish lifestyle portrayed on social media puts unnecessary pressure on these youth, who gets easily swayed by worldly possessions and as a result, it leads them to commit cybercrime.
R12	Sometimes when these cybercriminals are apprehended, you receive a call your boss would call you or somebody higher may call you, just like a threat. Most of the time our hands are tied in some.
R13	Technological advancement, since the incorporation of the internet and telecommunication devices into our culture, the rise in cybercrime has been alarming. Youth flock to it, in other, to get rich quickly.
R14	A variety of low-cost hackers' tools are available for users online over the internet, what is stopping these culprits from getting a hold of them and using them to trap their victims, nothing.
R15	Lack of patience and acting impulsively to get whatever they want fast.

The majority of the respondents believed that the major reasons youths in Kwara State are heavily participating in cybercrime as represented in the cloud below can be subjected to the followings; unemployment, laziness, high level of poverty, and lack of employment opportunities in the state, etc.

4.3.3 Results on the Extent Cybercrime has Eaten into the Nigerian System

	Question 3 How deep has cybercrime eaten into the Nigerian system?
R1	90% deep, it's very high, because if you go anywhere now, in Nigeria it is full of cybercrime, just because of this same government they have not done well at all and I would keep on calling the government because they have failed woefully.
R2	It has eaten the system a lot, and many people have fallen victim not only in Nigeria but abroad too. It has eaten many citizens, just like a worker eating up tomatoes or food and making it sour, that is how cybercrime is in Nigeria, it is getting out of hand and uncontrollable in which we fear what may be the forecasting of our future of our unborn children
R3	Badly I would say. I was listening to the news though not directly on some latest things on rating nations on how bad they are, the rate of cybercrime in the countries and Nigeria was rated as the first of all and I think this is a bad thing on the image of the nation
R4	Very deep. Today there is a lot of youth that would prefer to go into cybercrime, instead of going for skill acquisition or entrepreneurship that could help them in the future.
R5	It has drastically eaten into the system such that the youth are involved directly or indirectly, such that some of them even go into bet way just so to get money, as a result, it has eaten deep if it is not quickly checked I begin to wonder how the tomorrow of Nigeria would become.
R6	Very deep, about 65% a lot of people around are into cybercrime and they are doing well. It is always helping in one way or the other, it has reduced the number of physical robbery attacks, and people are not engaging in this robbery anymore.
R7	It is going beyond the level of what people can just say, so many youths are into it, and even the underage are now a part. They use it as a way to eradicate poverty in their family
R8	From the television news and the police, they can testify to it. There are killings and removal of body parts for ritual purposes, it is no longer something hidden, it is clear even in schools. Cybercrime has eaten very deep.
R9	It has eaten so deep that security threats are now a common practice in the country. It has eaten so deep that countries no longer trust us. We have lost so many privileges as a result of this.
R10	.About 90% deep that we now have a bad image in the international arena.
R11	It has affected our economy and our international reputation has been damaged severely.
R12	Cybercrime has eaten deep into the state in the sense that no one is safe in the country anymore, passwords, card details, and bank details can be hacked at any time, and even the government and their sensitive information can be hacked and used for whatever.
R13	It has eaten deeply into almost all the sectors of the state, from the banking sector to the health sector thereby damaging the institutions in question.
R14	It has eaten deep to about 90% of everything in the country, so much cyber stalking everywhere, harassment, threats, blackmailing scams and the rest.
R15	Nil

As pointed out by the respondents, cybercrime has eaten very deep into the Nigerian system in such a way that has negatively affected the system as represented further by the cloud below.

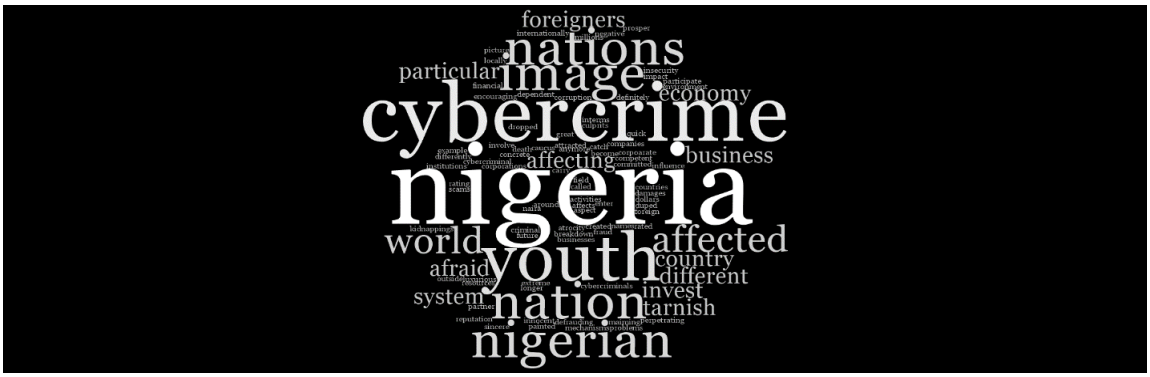


4.3.4 Results on the Various Ways Cybercrimes has Affected the Nigerian System

	Question 4 In what way has cybercrime affected the Nigerian system?
R1	It has affected the system because a competent person in a particular area of his field anymore. Let me do a breakdown of a particular issue, somebody who has been sincere for many years and because where he is working sincerity has given him a more upper hand to do a lot of things and because of the caucus around him, they would influence him to do something that he would not want to do.
R2	It has affected it by encouraging the youth to involve in criminal aspect perpetrating it, that also may tarnish the image of our great nation called Nigeria for example Hush Pupi is a Nigerian, now he is in jail and still committed an atrocity of 400 000 dollars in which up till now the white men are surprised that how did he do it. Whenever they see Nigerian youth they tarnish us as cybercriminals, they call us all sorts of names that are unbearable as Nigerians.
R3	The image of the nations. Many foreigners are afraid to invest in this nation because they are afraid of being duped, this is the picture that cybercrime has painted Nigeria to the world.
R4	This affects our image and reputation because it hurts the economy, if youth take cybercrime as a major business no country in the world would want to partner with Nigeria, as soon as they know that majority of the youth participate in cybercrime
R5	As it is now the future of Nigeria is unpredictable, our status rating among other nations has dropped, and the country has been rated to have a level of corruption and scams.
R6	Nil
R7	It is affecting in terms of our image of the outside world; once they hear you are from Nigeria their thinking is different and they don't trust us. In the past foreigners were attracted to Nigeria and we could enter other nations without much trouble, but the case is different now we have been treated differently.
R8	It has made the youth lazy and dependent of get rich quick mechanisms. youths don't want to work but they want to live a luxurious life
R9	Nil
R10	It has made the business environment very difficult for startup companies to succeed and for small businesses to prosper, foreign countries no longer want to invest in the nation, and this is a very serious issue.
R11	Loss of financial resources of the state, millions of naira each year are being lost to these cybercriminal activities. The damages are usually very extreme.
R12	Cybercrime has and is still affecting the economy of the nation of Nigeria both locally and internationally.
R13	Corporate internet fraud has been on the increase, defrauding nations, institutions and corporations.
R14	As a result of cybercrime, has led to the death of so many innocent people, kidnappings and even maiming. Nigeria has become very unsafe and insecurity is now on the rise.
R15	Because lack of concrete laws, has created many problems for the EFCC officials making it difficult to carry out their assignment and apprehend these culprits.

Cybercrime has affected the Nigerian system in such a way that it has given the country a bad light in the international arena. Father more, the cloud representation shows

the relationship between how cybercrime has affected the Nigerian system and Nigeria herself.

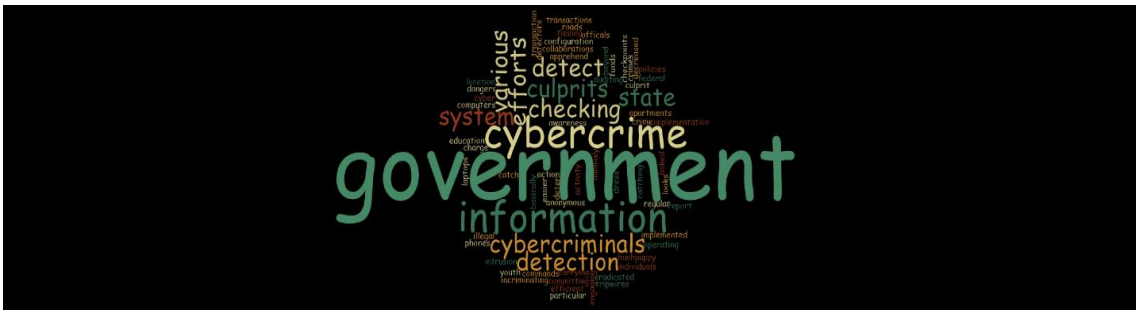


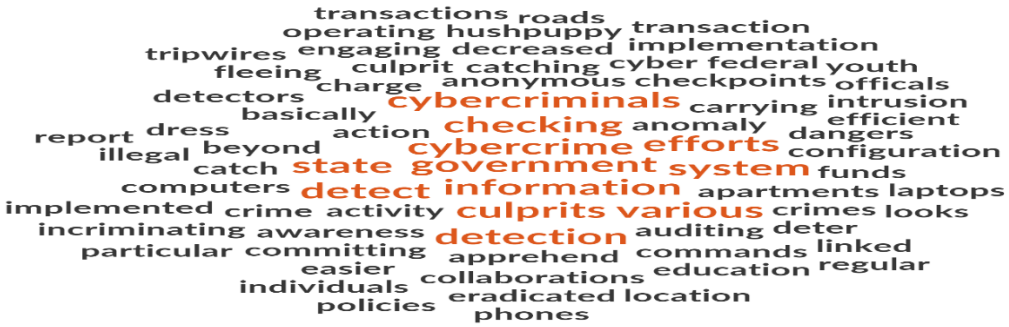
4.3.5 Results on Whether the EFCC has been able to Detect Cybercrime Among Youths in Kwara State

	Question 5 How has EFCC been able to detect cybercrime among youth in Kwara state?
R1	I don't think they are efficient in that area; the only way I see is that they are able to do that by means of internet by finding out those ones who using the internet to do cybercrime. So, it is through internet just like the case of Hushpuppy
R2	Basically, it's by their looks, the way they dress and the way they act or behave.
R3	Cybercrime cannot be totally eradicated, although it may be decreased. Individual efforts, together with government action, are, very, necessary.
R4	Through checkpoints on major roads, in other to deter these cybercriminals and also catch them at the point of fleeing to other states.
R5	Collaborations between the people and the officials in charge of catching these cybercriminals.
R6	Checking and going through phones, laptops and computers to find incriminating materials or clue that can point to the person in question as a culprit.
R7	Government policies and its implementation. Like When the federal government implemented the NIM to be linked to our bank to monitor our transactions this made it easier for the officials to detect any illegal activity once they see a particular transaction is getting beyond your regular funds.
R8	By carrying out a search of the apartments or rooms of these culprits based on the information got from various sources in other to apprehend them. Also, people also give out these information's to the officials on where the culprits are per time.
R9	Individual efforts or information in line with the government officials, working hand in hand.
R10	Government laws in other to tackle the issue in the state.
R11	Through anonymous tips by various individuals.

R12	Through the use of detection tools include intrusion detection systems, tripwires, configuration checking tools, honey pots (lures), anomaly detectors, and simple operating system commands.
R13	Through education and cyber-crime awareness with this people know the dangers of committing these crimes and also report those engaging in it, to the government.
R14	Through auditing of any suspicious event, flag by the system no matter the location
R15	Nil

In regards to the majority of the respondents, they argued that the EFCC has been able to detect cybercrime among youths in Kwara State through some intelligence means which includes; intelligence information, checking, detection, operational efforts, culprits' confession etc. it has been further emphasized through the word cloud representation below.





4.3.6 Results on the various Strategies Put in Place by EFCC to Detect Cybercrime among Youths

	Question 6 What are the strategies put in place by EFCC to detect cyber cybercrime among youth in Kwara state?
R1	By educating the public on cybersecurity and dishing out cybersecurity tips in other to stay better protected.
R2	There is a crop of trained personnel sponsored by the government to get the adequate knowledge required in catching these culprits.
R3	I'm not sure of such strategies, I am not personnel of the commission.
R4	Engaging the youth and getting them to talk and expose them and snitch on those who partake in these criminal activities.
R5	Leveraging trusted resources, and implementing a response plan for when red flags are detected.
R6	Punishment such as long jail terms, convictions and the likes.
R7	Arrest and strict punishments and also long jail terms after being convicted.

R8	Through effective public and private partnership that incorporates businesses and institutions of all sizes.
R9	There is the national, state, local, tribal, and territorial agencies created to produce successful outcomes in identifying and addressing threats, vulnerabilities, and overall risk in cyberspace.
R10	There are also regulations are regulatory instruments, guidelines, and frameworks that prepare the state for these criminals so as not to be taken unawares.
R11	Government collaborations with the people
R12	Through policies and regulations of government has it pertains to cybercrime.
R13	Punishments being stated clearly in the constitutions and state legislations.
R14	Strict cybersecurity awareness and education on the effect, punishments, and preventive measures.
R15	By making Prompt arrests and convictions to make publicly known on the EFCC websites.

Strategies put in play by the EFCC as emphasized by the respondents includes the following; regulations, cyber security, convictions, threat measures, arrest, etc.

4.3.7 Results on the Initial Strategies put in Place by the EFCC

	Question 7 What are the initial strategies put in place by the EFCC to curb cybercrime among youth in Kwara state?
R1	By using the gurus in the cybercrime business to find the others.
R2	Trained personnel's, some are in house in training and some are abroad. Because the federal government sent them abroad to be trained so they can compete.
R3	Different light sentences imposed as punishment but this has failed time and time again.
R4	There were also the plea bargain strategies, which wasn't also very effective. It was too liberal.
R5	Enacting and implementing stricter laws against cybercrime.
R6	SARS was one of the strategies but it didn't turn out well, now they doing themselves.
R7	Confiscation of properties belonging to arrested cyber criminals.
R8	Strict laws in terms of punishments meted out to the cybercriminals.
R9	Mobilization of men to the various agencies in different states.
R10	Searching through their phones, accessing these passwords is a bid problem.

R11	Establishment of formidable Internet Security Agency to Detect Cybercrimes
R12	Training of personnel in the act of detecting and catching the cybercriminals
R13	Keeping up with technological and security advancement as it unfolds.
R14	Seizing of properties owned by the cybercriminals, after an arrest.
R15	Formulation and implementation of policies, passing of bills against cybercrime.

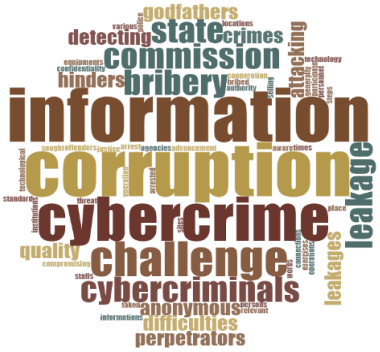
The initial strategies put in place by the EFCC as emphasized by the respondents includes; training, cyber security, punishment and sentences, sizing of properties etc.

4.3.8 Results on whether the EFCC Faces Difficulty in Detecting Cybercrime Offenders

	Question 8 Does EFCC face any difficulties in detecting cybercrime offenders?
R1	Yes, they face difficulties, nowadays people getting themselves into cybercrime are very smart, and so you need a smart person from the EFCC that can handle them that knows all the corners of this cybercrime people.
R2	Definitely, corruption is one major issue, corruption within the commission and corruption outside the commission; this has caused a lot of harm. Advanced knowhow of technological advancement of these cybercriminals is also alarming and a threat that possess a challenge.
R3	Officials of the law compromising on their standard as a result of bribery and corruption. Letting the culprits go if they are able to seek them with large sums of cash. This hinders justice in no small way.
R4	Lack of good and quality internet service in Kwara State is one challenge, network connections are poor, and this hinders progress.
R5	Lack of adequate personnel and staffs to carry out various functions and exercises. The officials find it difficult to be there in the particular spot where cybercrime is being carried out.
R6	Lack of confidentiality, information leakages on operation sites, time and locations.
R7	Inability to get good equipment is in other to carry out their jobs effectively, selling of information's in addition, on when certain operations would hold and take place, in other to warn their persons who participate in cybercrime. These leakages most of the times comes from the agencies or the commission.

R8	Information leakage on where and when EFCC officials would be attacking. Anonymous calls to be usually made to help catch these perpetrators.
R9	Information leakage on where and when EFCC officials would be attacking. Anonymous calls to are usually made to help catch these perpetrators
R10	Generally, bribery and corruption are the major challenge, ones they are bribed that is the end.
R11	Cybercriminals having people in authority who help to bail them out, when arrested. Is a major challenge.
R12	These guys have godfathers, once arrest is made, they call their godfathers and even hearing from them you may want to withdraw whatever you intend to do for them. Many of them have army or police stickers on their cars, once the officials stop, they point to their stickers, which is a lie.
R13	Yes, they do, lack of Cooperation from person/institutions who should furnish relevant information that can help in arresting or detecting these crimes. Also, information or words get out and theses cybercriminals are aware of the steps being taken by the officials.
R14	Lack of quality internet service in the state, and also the state doesn't have an up-to-date technology to detect these crimes.
R15	Bribery and corruption and information leakage.

It was agreed by the respondents that the EFCC face difficulties in detecting cybercrime offenders. They equally pointed out some of the difficulties face by the EFCC which include; leakage of information, bribery, corruption practices within the agency, godfatherism, etc. which was further emphasized by the cloud representation below.



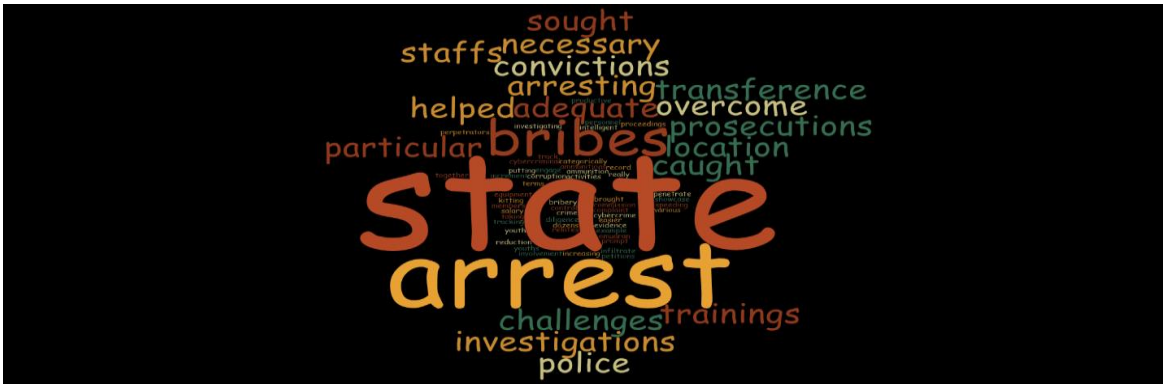
4.3.9 Results on the various Challenges Faced by EFCC in Detecting Cybercrime among Youths in Kwara State

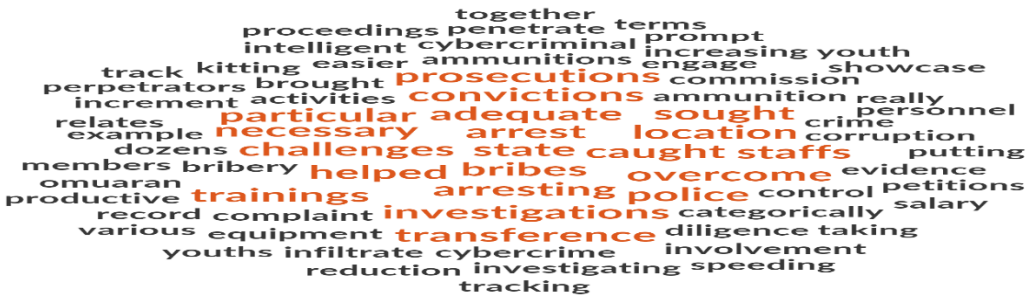
	Question 9 What are the challenges faced by the EFCC in detecting cybercrime among youth in Kwara State?
R1	The government is not giving this people good equipment to challenge the cybercrime in Kwara State, of course they won't be effective, you can't tell a person to do a particular thing and you don't give him the equipment to do it, you didn't show him the way to do it. That effectiveness in the act would not show, because you are not giving the person the equipment to fight the cybercrime.
R2	These guys some of them have people in higher authorities who do them favors in turn for cash. They get released even before they are being convicted.
R3	Corruption, lately the complaint has been that most of the personnel in this commission they are not helping the matter, in that you are supposed to investigate and curb when you have a suspect, or someone caught found guilty of these crimes, ones they are paid, they let go or drop the charges, I believe that one of the major challenges is corruption.
R4	Network or internet issues, limited workers.
R5	The use of spiritual powers by this yahoo boys to carry out their activities.
R6	Bribery and corruption. The police collect bribes and they choose who to report and give information on, these cybercriminals bribe the police to notify them when these officials are around.
R7	Lack of adequate technology to detect these crimes, the equipment's are not up to date.
R8	The workers being deployed are not sufficient to go round within the state and this poses a great challenge.
R9	The problem of implementation, implement policies formulated is a big challenge.
R10	No access to good enough network access, and mainly bribery and corruption.
R11	The use of spiritual powers, bribery and corruption and the Godfather syndrome.
R12	Corruption in forms of bribery, embezzlement, misappropriation and money laundering within the EFCC, is a major challenge.
R13	Lack of accountability, corruption and embezzlement of funds
R14	No trained staff, or not enough trained staff.
R15	Nil

	Question 10 How has EFCC been able to overcome the challenges, if at all they have?
R1	by investigating the petitions brought up by the members of the state.
R2	Speeding up of investigations and prosecutions, together with intelligent and diligence evidence tracking.
R3	None, because the complaint on the news has been that, these personnel's have been taking bribes which is not a record of success at all
R4	They have to infiltrate the youth, get more staffs for the EFCC to work among Kwara State, so that they can easily penetrate this youths and find out those that engage in this crime
R5	They have not been able to overcome these challenges, because the more they try to control the more the number is increasing for example in Omu-Aran Kwara State the EFCC makes arrest but the more they do the more you hear of dozens of cybercriminal activities
R6	I cannot categorically say.
R7	Transference of these officials from one state to another state, it makes them work very hard. If they stay too long on a particular location, they can begin to take bribes and do all sought. Also, the increment of salary's too also helped, and give them full ammunition and more ICT Trainings to help track down these perpetrators, to make work easier for them.
R8	We do what is necessary by arresting them when they are caught. The EFCC Is to arrest and then hand them to the police.
R9	Transference of EFCC officials from one state to another state, it makes them work very hard. If they stay too long on a particular location, they can begin to take bribes and do all sought.
R10	Reduction in the media showcase of investigations and convictions has really helped to be more productive and have more successful prosecutions.

R11	We do what is necessary by arresting them when they are caught. The EFCC Is to arrest and then hand them to the police.
R12	Less involvement of the media as it relates to cybercrime proceedings, arrest and convictions.
R13	Putting up a fight against bribery and corruption within the commission.
R14	By making prompt and adequate arrest.
R15	Adequate kitting of the staffs in terms of ammunitions, equipment and various trainings.

The challenges faced by the EFCC in detecting cybercrime youths in Kwara state as pointed out by the respondents include; Challenges of state participation, challenges in making an arrest, challenges in making investigations, location challenges, bribes and corruption, staff involvements, etc.





	Question 11 Has there being any success recorded so far by the EFCC in curbing cybercrime among youth in Kwara State?
R1	Yes, I heard the news in some areas of the state concerning these cybercriminals the number of people caught with proof, having their laptops on them, they need to get an internet that is very good too.
R2	Some offenders are serving jail term as we speak in Kwara State in correctional service, from January to April as we speak, we have recorded both male and female apprehended with exhibits in their custody. There has been successes and we are making progress.
R3	Yes, there has been success, even though it has not really deterred others from committing the same crime.
R4	Yes, there are lot of success recorded. We have seen a lot of these cybercriminals been apprehended and convicted and there are EFCC officials around us working, also many youths are now going back to entrepreneurship in other to earn a livening.
R5	There has been, studies have showed this with the EFCC reports in respect to this.
R6	They are succeeding gradually, but it is not significant, so many of these cybercriminals are travelling, relocating ones they notice EFCC is around they have to travel from that area to another area

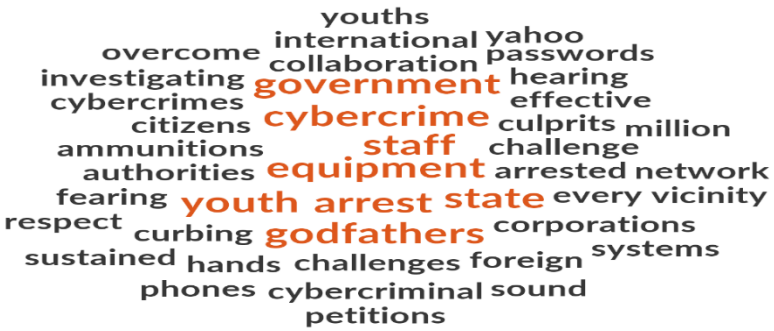
R7	has been a lot of success, they are trying their best, their success is more than the ones before
R8	Yes, there is. The Kwara State command is not relenting in their effort to do the normal things. There are many of them that have been apprehended
R9	There has not been much success because of the fact that the number of cybercriminals out there keeps rising.
R10	Has there been any success recorded by the EFCC in curbing cybercrime in Kwara state? There has been, studies have showed this with the EFCC reports in respect to this.
R11	There has been a considerable level of success, just recent the EFCC uncovered over 1000 ghost workers in Kwara State, adding this to others in the news, I think they see doing their best.
R12	Yes, there has been successes, the total number of convictions in the state has significantly increased.
R13	It has been successful, that the Attorney General in Kwara State had to congratulate the EFCC team.
R14	A number of successes has been recorded so far.
R15	Nil

As argued by the majority of the respondents, there have been successes recorded so far by the EFCC. According to one of the respondents who pleaded anonymously stated categorically that there has been a great success recorded by the EFCC that even made the Attorney general in Kwara state congratulate the EFCC team.

4.3.12 Results on the various Challenges faced by the EFCC in investigating Cybercrime among Youths in Kwara State

	Question 12 What are the challenges faced by the EFCC in investigating cybercrime among youths in Kwara state?
R1	It still goes to when there is no good equipment to fight cybercrime, like I said you can't ask a person to go to the far without a cutlass they are going to fail woefully, that day would be wasted for the person, even though he is going with an equipment, is that equipment effective for that day and some other day.
R2	Higher authorities asking for the release of an arrested cybercriminal against protocols. Most of the time our hands are tied in some areas, we cannot double cross it, but we time we can overcome it and we are trying our best to bring those boys to book.
R3	No good or sound network systems.
R4	limited staff, in Kwara State there are more than 2 million youth. EFCC has to get more staff to work among the youth
R5	Citizens not cooperating with the government, to help with the arrest of such culprits. except every individual is totally involved in respect to curbing these cybercrimes the EFCC would continue to find it difficult
R6	Searching through their phones, accessing these passwords is a bit of a problem
R7	Not having God fearing people among them, if they do, they would be more successful in their work.
R8	These guys have godfathers, once arrest is made, they call their godfathers and even hearing from them you may want to withdraw whatever you intend to do for them.
R9	I Lack of partnerships with corporations and foreign bodies.
R10	Neighbors within that vicinity do not work hand in hand with these officials to arrest these yahoo boys, this shows that there is a collaboration between the people and the government.
R11	The constant increase in the number of petitions on the website of EFCC.
R12	NIL
R13	International partners are from little to no existence. This also poses a challenge.
R14	Limited staff, equipment, and ammunitions.
R15	Lack of sustained partnership.

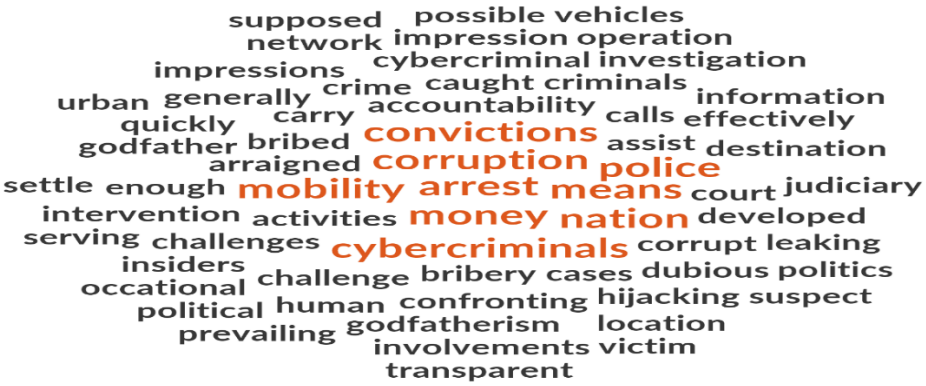
The challenges faced by the EFCC in making an investigation of cybercrime in Kwara State are subjected to a lack of good and modern facilities and equipment. However, it is important to note that some of the respondents pointed out that another major challenge is the lack of collaboration between the neighbourhood and the EFCC.



4.3.13 Results on the Challenges Confronting the EFCC in Making Convictions

	Question 13 What are the challenges confronting the EFCC in making convictions/ arrest?
R1	Involvements of these officials in cybercriminal activities also, and also them serving as insiders for these criminals.
R2	Human right intervention at the point of arrest.
R3	I would say it boils down to corruption, because once they are paid, they drop the case, they forget about it.
R4	Not effectively working with judiciary as it pertains to convictions, investigation and arrest.
R5	It is politics, the political godfatherism, when I am being caught and I have godfather I quickly make calls across of which I would be set free on bail. Another issue is money, these cybercriminals have the money to settle whatever case that may come up and the corrupt nation that we have has made this to be very possible. The EFCC is trying but compared to the developed nation it is not at par
R6	Generally, bribery and corruption are the major challenge, ones they are bribed that is the end
R7	Mobility to the location they want to get to. No fuel or the vehicles may not get to where they are going, it would affect them when they want to carry out their operation.
R8	The police should assist the EFCC too, there has been cases where the police free some of this suspect that are supposed to be arraigned to court saying that they are not cybercriminals
R9	Mobility is a big issue, not being able to get to their destination on time, as a result of bad road network.
R10	Hijacking money through dubious means won't make the victim happy and I would say they should find a means of having the fear of God.
R11	Corruption and lack of accountability, I believe that they are not transparent enough.
R12	It is the prevailing impression that crime pays. They move to urban cities based on these impressions and then start commit and early
R13	Occasional incompetent
R14	Information leaking, this makes other effort one that has ended before it started.
R15	Nil

The challenges facing the EFCC in making convictions and arrests as argued by the majority of the respondents include lack of mobility, hijacking of suspects, leakages of intelligence information and reports, bribery, and police involvement.

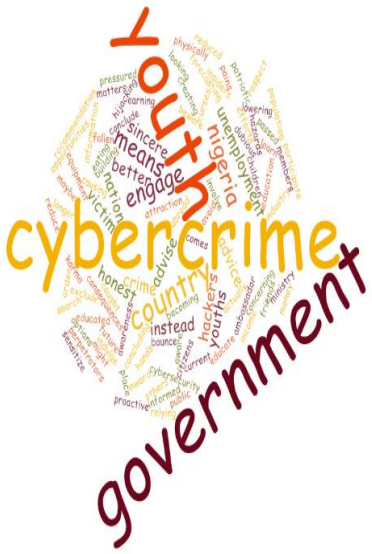


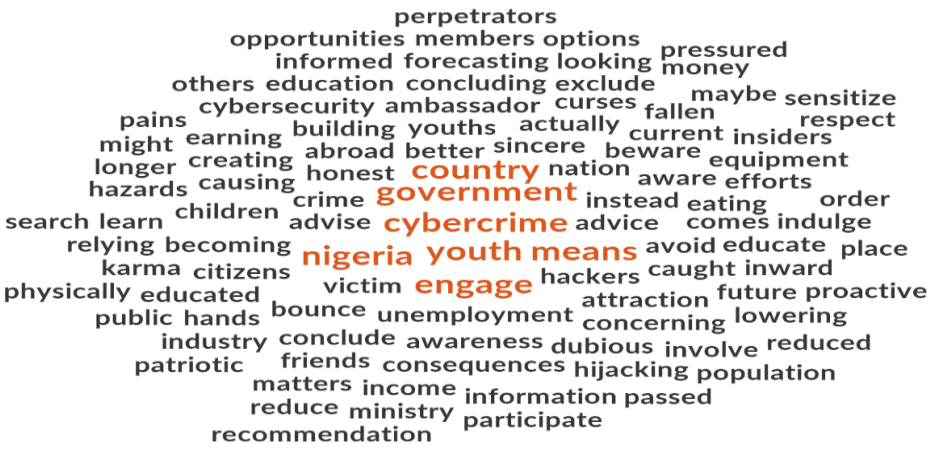
4.3.14 Results of Respondents Conclusion on EFCC and Cybercrimes in Kwara State, Nigeria

	Question 14 What is your concluding sentence concerning EFCC and cybercrime?
R1	I would conclude by saying the government should give the EFCC good equipment to fight this cybercrime, actually one cannot know those ones who are sincere because sincerity is one that matters a lot, insiders are the ones not making this cybercrime to die once and for all, the government should fish them out and those ones who are sincere the government should fish them out and put smart people. Do you have any advice for the perpetrators? Hijacking money through dubious means won't make the victim happy and I would say they should find a means of having the fear of God.
R2	I would like to put it like a shout out to our youth, if they would heed to it, some may say that the country is bad so we have to engage our self in a good living. I would like to say they shouldn't indulge in crime, there is no small crime once you are caught that is it. I would advise them to exclude themselves from such, and try to be a good youth and ambassador of the country.
R3	I would say we should all be patriotic. It's our nation, it's our home. We have education, tools etc. that we are giving up and not building our nation.
R4	Youths should look inward seek what they can do instead of relying on cybercrime, because whatever you do with your hands would surely last longer than what you only sit somehow and by means of unscrupulous act get, those ones would not last.
R5	My recommendation is that the government look at how it might engage the youth in the search for work and income options. I believe that unemployment has led to this, therefore if the government can look into it, it will go a long way toward lowering the country's rate of cybercrime.
R6	Youth should engage in more honest living instead of causing pains to others, they should find a better job to do. And the government
R7	The youth should stop this and think about the consequences, the karma, and the curses. Spiritually and physically, I advise them not to do it, because when the result comes, it would affect them. All these things can bounce back. The government should all put in more efforts in creating jobs to make Nigeria a better place for the youth.

R8	Youth should be serious, they should make an honest living, have work at hand, learn a skill even if you are a student
R9	It has eaten the system a lot, many people have fallen a victim not only in Nigeria but in abroad too. It has eaten many citizens, just like a work eating up tomatoes or food making it sour, that is how cybercrime is in Nigeria, it is getting out of hand and uncontrollable in which we fear what maybe the forecasting of our future of our unborn children
R10	Nil
R11	My advice is that the government should see how to involve the youth, in respect to looking for opportunities where they would be working and earning their living. I feel that it is unemployment that has led youth to this so if the government can look into this, it would go a long way to reduce the rate cybercrime in the country
R12	Government should work with the state's Ministry of Youth and Sports to educate these kids about the hazards of cybercrime, as well as to help sensitize other youths who may be pressured by their friends to participate in cybercrime.
R13	There should be cybersecurity threat awareness and information passed across to people to beware and be safe.
R14	The bulk of the population should be aware of this and take proactive steps, hackers will be less successful, and the attraction of the cybercrime industry will be reduced.
R15	Members of the public should be educated and informed about current cybercrime trends in order to avoid becoming victims of hackers.

Conclusively, the majority of the respondents believed that the government should work with the state's Ministry of Youth and Sports to educate these kids about the hazards of cybercrime, as well as to help sensitize other youths who may be pressured by their friends to participate in cybercrime, while another respondent believed that the government should see how to involve the youth, in respect to looking for opportunities where they would be working and earning their living. I feel that it is unemployment that has led youth to this so if the government can look into this, it would go a long way to reduce the rate of cybercrime in the country.





4.4 Discussion of Findings

The impact of cybercrime on the Nigerian system is known in this study. The goal of this study was to learn more about the nature of cybercrime, how it affects the Nigerian system as a whole, and how effective the EFCC is at preventing it among young people in Kwara State and across Nigeria. According to the study, youth cybercrime has deeply permeated the Nigerian system and, if left unchecked, would continue shortly due to the EFCC's failure to do so.

The following objectives were established:

a) To investigate the causes of youths' involvement in cybercrime in Kwara state, Nigeria
b) To determine the effectiveness of the EFCC's efforts to reduce cybercrime among young people in Kwara State, Nigeria.
c) To investigate the difficulties faced by EFCC in identifying cybercrime among youths in Kwara State, Nigeria.

The bulk of the informants had strong ideas regarding the causes that they thought led young people to engage in cybercrime. They said that peer pressure, unemployment, poverty, and greed are the main factors motivating young people to engage in cybercrime.

Regarding the first objective, which examined the causes of youth involvement in cybercrime in the Nigerian state of Kwara, all respondents agreed that peer pressure, unemployment, and idleness are the main causes of youth involvement in cybercrime. If all of these issues are resolved, the involvement of young people in cybercrime will significantly decline in Nigeria as a whole.

Regarding the second objective, almost all of the respondents concluded that the EFCC is now much more effective in preventing youth involvement in cybercrime in the Nigerian state of Kwara. However, all respondents argued that the EFCC needed additional skilled workers, equipment, mobility, training and retraining, as well as appropriate funds, to successfully eradicate cybercrime in the country.

Regarding the third and final objective, which was to look at the difficulties the EFCC faces in identifying cybercrime among young people in Kwara state, the majority of respondents argued that there are many obstacles the EFCC must overcome to effectively combat cybercrime in Nigeria. These obstacles include corruption, a lack of equipment, a shortage of trained personnel, leaks in the intelligence unit, bribery and corruption, godfathers, etc.

One of the first research questions, is, what are the factors that motivate youths' involvement in cybercrime in Kwara state, Nigeria? It was relatively clear that the majority of the youths suffer from the get-rich syndrome, however, one of the respondents was quoted as saying, "poverty is the major factor that is encouraging youths' participation in cybercrimes in Nigeria.

The second research question, which is, how effective are the strategies of the EFCC for detecting cybercrimes among youths in Kwara state, Nigeria? The researcher uncovered that the EFCC has been effective in curbing cybercrime in Kwara state, however, it was equally argued by the respondents that the EFCC is adjudged ok in detecting cybercrime among youths, through some intelligence and strategic means.

The final research question is, what are the challenges confronting EFCC in detecting cybercrime among youths in Kwara state, Nigeria? Unanimously, the respondents pointed out some of the major challenges facing the EFCC in curbing cybercrimes in Kwara state, Nigeria. The respondents agreed that corruption, mobility, godfatherism, bribery etc. are the major challenges confronting the EFCC in totally eradicating cybercrimes in Kwara state and Nigeria at large

Numerous research goals and the results of the qualitative research served as the direction for this study. The qualitative study investigated the many functions that the EFCC performs in combating cybercrime in all of Nigeria. It emphasized the various definitions of cybercrime as well as the type that is most common in Nigeria. It also

determined the root causes. It also looked at the steps taken by the EFCC to combat cybercrime. Finally, it described the difficulties the EFCC faced and looked at the necessary changes to combat cybercrime. With a focus on various facets of the phenomenon under inquiry, this conversation is divided based on the research questions.

Conclusions were generated based on the results of all the interviews performed using all pertinent information gathered and examined for each of the analyses. The analysis demonstrated the effectiveness of the EFCC's efforts in promoting financial accountability and transparency in Nigeria's cyberspace, as well as its capacity to identify and tackle cybercrime across the nation of Nigeria. In light of this, it is important to note that the EFCC has made a significant contribution to the improvement of accountability and transparency in cyberspace, not only in the state of Kwara but throughout Nigeria.

To support this claim, the world transparency international reports that Nigeria has improved from its previous ranking as the world's second-most corrupt nation, moving up to number 31, this is due to the economic and financial crimes commission's tenacious campaign and fight against corruption at large.

CHAPTER FIVE
SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

Understanding the EFCC's influence in lowering cybercrime in Nigeria's Kwara state was the primary objective of this study. Nigeria has recently been identified as a centre for cybercrime operations because the country's money laundering and fraud investigations are well-known. This study looked into how the EFCC helped Kwara state, Nigeria, combat youth cybercrime. The study's summary, conclusions, and recommendations for resolving the difficulties they present are repeatedly emphasized.

5.2 Summary

As stated in the introduction and literature analysis, there is a shortage of information on law enforcement and the roles played by EFCC employees in battling cybercrime. The majority of past studies concentrated on the socio-economic effects of cybercrime, its origins and repercussions in Nigeria (Hassan, 2012; Adesina, 2017); and the legal penalties for computer abuse (Saulawas and Abubakar, 2014). (Sesan, 2012). Similar to the studies conducted by Maghairah (2009) and Alkaabi, the current study integrates all these various components to comprehend cybercrime from the perspective of Nigerian law enforcement (2010).

The research also uses a conventional criminological framework known as Routine Activity Theory to assess the theory's applicability to cyberspace, which Yar (2005) claimed can be taken into account in understanding cybercrime. The theory's justification was thoroughly discussed in the chapter before. An interpretivism paradigm and a relativist philosophical viewpoint were used to frame the research, which adjusts the methodology to the current study's exploratory and explanatory nature.

Interviews were used to acquire information using a qualitative method because the study question is social. Interviews with 15 residents of Kwara State took place. According to evidence from the report, the EFCC has tried to resolve challenges in investigating cybercrime through collaboration, training, and application of appropriate laws and regulations. The discovery also broadens the criminological knowledge of online aberrant behaviour and enriches the ongoing discussion on the function of law enforcement in policing cybercrime in Nigeria.

The study's findings, taken together, provide light on the EFCC's role in lowering youth involvement in the Nigerian state of Kwara, the factors that contributed to youth involvement, and the strategies the EFCC has used to lessen youth cybercrime. The preceding chapter also served as the basis for this study because it called for testing all relevant findings and information gathered using the NVIVO software program to make a precise inference based on the responses from the respondents.

5.3 Conclusion

Based on the test results and all relevant data collected and carefully evaluated for each analysis, conclusions were drawn. The results showed the many indicators that promoted young involvement in cybercrime in Nigeria's Kwara state. The results also showed that the EFCC has numerous obstacles in its efforts to completely eradicate cybercrimes in Nigeria's Kwara state. The findings also showed that the EFCC is capable of identifying and combating cybercrime throughout the country of Nigeria and that its efforts to promote financial responsibility and transparency in cyberspace have been successful. As a result, it is crucial to recognize that the EFCC has significantly improved accountability and transparency in cyberspace, not just in the state of Kwara but across all of Nigeria.

5.4 Recommendations

The researcher felt the following recommendations, which will help to encourage the government to take notice of improving the EFCC's operations and also assist the commission itself in enhancing financial accountability and transparency in Nigeria, were necessary to attach in light of the challenges the commission was facing and the research's findings.

1) **Introduction of modern technology:** The government must implement modern information procurement to streamline and simplify Commission operations. This will strengthen and improve the commission, especially by acquiring more computers, servers, and mainframe workstations.
2) **Adequate funding:** According to this report, one of the main obstacles the EFCC faces in completely eradicating cybercrimes in Nigeria is a lack of funding. As a result, the government should provide the commission with the required funding for mobilization and mobility.

3) **Building an integrated data network**: Within the context of its information strategy, architecture connects the department's zonal offices, training centre, and all of its other offices.
4) **Staff training and retraining**: Since it is essential to train and retrain the commission's workers, agents, and partners to raise management exports, improve staff competency, and help the commission meet its objectives, the commission should upgrade its staff training facilities.
5) **Capacity Building:** Given that it contributes to the generation of first-hand information on economic and financial challenges, the commission should maintain a solid database for capacity building. being able to collect, analyze, store, and retrieve data from a variety of sources, including market players in the relevant financial and capital markets. To conceal illegal conduct from law enforcement and regulatory agencies, more investigation into corporate crimes such as accounting fraud, executive self-dealing, and justice obstruction needs to be done, especially in the banking sector.
6) **Eradication of corruption practices:** If the commission is to successfully carry out its objective of completely reducing cybercrime among youths in Kwara state and throughout Nigeria, it must completely abolish corruption and unethical behaviours inside the agency.

REFERENCES

Abebusiyi, I.A, (2010) The Internet and Emergence of Yahoo Boys' Sub-Culture In Nigeria. *International Journal of Cyber Criminology (IJCC).* Vol.2 (2): 368-381.

Adegboyega. D, (2011) *Economic and Financial Crimes Commission EFCC,* Information Handbook 1, Jexcel Commercial and Securities Printers, EFCC, PP 1-5.

Ademola. A, (2011) Endangering Good Governance for Sustainable Democracy. The Continuity Struggle Against Corruption in Nigeria, *Journal of Research in Peace, Gender and Development, Volume* 1 (11), Pp307-314.

Adeniran, A, (2010) A Non-Dependent Framework for Development. This Day, Www.Thisdayonline.Com

Ajaro, C, (2014): In The Eyes of EFCC, News Watch Computer; Communication Center.

Akanbi, M.M, (2011). *Corruption and The Challenge of Good Governance in Nigeria*. In Olurode, L. & Anifowose, R. (Eds) Rich but Poor: Corruption and Governance in Nigeria. Faculty of Social Sciences: The University of Lagos, P. 122.

Axelrod. R, (1997). The Dissemination of Culture: A Model with Local Convergence and Global Polarization. *The Journal of Conflict Resolution* 41(2) 302-226.

Babawale T. & Onuah B, (2013). *The State, Corruption and The Challenge of Good Governance in Nigeria.* In Olurode, L. & Anifowose. R. (Eds) Rich but Poor: Corruption and Good Governance in Nigeria, Faculty of Social Sciences: The University of Lagos, Pp. 70-79.

Brenner, J.K. & Susan, W.Y, (2011) Is There Such a Thing as, Virtual Crime. *Cal. Criminal Law Rev.* 1(4).

Brey, P. (2011). *Disclosive Computer Ethics. In: R. A. Spinello and H. T. Tavani (Eds.). Readings in Cyber Ethics*, Jones and Bartlett: Sudbury, MA.

Chapman, A. & Smith, R.G. (2001) *Controlling Financial Services Fraud. Trends and Criminal Justice.* No. 189. Australian Institute of Criminology: Canberra, Australia.

Clarke, R.V & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 52, 170-183

Colins.O, (2011) The Effectiveness of Economics and Financial Crime Commission (EFCC) On Fraud Prevention and Control in The Public Sector in Nigeria (Unpublished Thesis Ebonyi State University)

Commonwealth (2000) Common Principles On Promoting Good Governance and Combating Corruption. Commonwealth, Heads of Government Meeting Durban South Africa.

Cybercrime Watch-Security Information (2011). Com/Cybercrime/Cyber-Crime-Statistics.Html.

Daniel, J.S. (2006). A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria.

Dariye, Nyame, Kalu & Turaki, In Prison, (2011) Vanguard, Vol. 23 No 60374, Page 15.

EFCC Establishment Act, (2004). EFCC Money Laundering and Prohibition Act, 2004.

Egbebor. A, (2005): Corruption Has Destabilized Our Society, Ventral Press and Printing Ibrahim. Federal Bureau Of Investigation FBI, (2006): Financial And Economic Crimes, FBI, Www.Google.Com.

Ernst & Young. (2014) 8th Global Survey of Business Fraud.

Felson, M, (1998). *Crime and Everyday Life*, 2nd Edn. Thousand Oaks, CA: Pine Forge Press.

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 Propensity-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 Kon

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

Howard, O, (2005) *Techniques and Strategies for Detection of Fraud*: John Wely & Sons, Inc. Hoboken, New Jersey.

Kigerl. A, (2012). Routine Activity Theory and The Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486.

Mcquade, S.C. (2006). *Understanding and Managing Cybercrime*. New York: Allyn and Bacon

Nigeria Financial Intelligent Unit Information Handbook (2007): "Public Service Corruption, The New Offensive," *Journal of EFCC (Zero Tolerance)* Jan.3, Vol.1 No. 3

Nigeria Financial Intelligent Unit Information Handbook: (2007): Public Service Corruption, The New Offensive, *Journal of EFCC (Zero Tolerance)* Jan. 3, Vol. 1 No. 3.

Nwali, N.B (2010), Making and Effective Use of Account in The Fight Against Corruption by EFCC. A Seminar Paper Presented at The Accountancy Department. Ebonyi State University, Abakiliki

Olukoya. D.O, (2007) EFCC Made Me Cry, *Journal of EFCC (Zero Tolerance)*, 4th April, Vol.1 No. 4.

Onyesanya.F. (2004): A Performance Review of EFCC and NCNF, www.nigeriavillaeaguar. Com *Oxford Dictionary, Advanced Learning Dictionary*, 6th Edition.

PC Quest. T, (1999). A Cracker Breaks in Pokhran. *Privacy Journal*. "SSN" Online". 4.

Ready to Return Loot, (2007): Vanguard, Vol. 23: No 6, July 23Frontpage P. 15.

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

Sandeep, D, (2004) *Bid to Block Anti-India Website Affects Users*. The Hindu. New Delhi, India.

Tedeschi, B, (2003.) Cybercrime, They Just Don't Mention It". The Age. Http://Www.Theage.Com.Au/Articles/2003/01/30/10438044474 47. Html

The Nigeria Capital Market; Developments, Investment Options, Players, Prospects, Challenges, Produced by Research and Market Dev. Dept (SEC)

Thompson. D, (1989) Police Powers - Where's The Evidence? Proceedings of The Australian Computer Abuse Inaugural Conference.

Times of India, (2004) Online Lotteries Bring Bumper Worries.

Tive, C, (2006). *419 Scam: Exploits of The Nigerian Con Man*. New York: Universe Inc

Toronto Star. (1995.) *Scam Artists Await Unwary Travelers*. F-19.

Vanguard, Vol. 23: No 6, July, (2007): 23 Front Page & P. 15. I'm Ready to Return Loot

Vatis, (1998) Congressional Statement of the Director National Infrastructure Protection Center. Senate Judiciary Subcommittee Papers. Washington, D.C. Www.Fbi.Gov/Pressrm/Congress98/Vatis0610.Html

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 TX Ford Handbook On The Law And Regulation Of Technology, Oxford: Oxford University Press.

Webster, W. & Borchgrave. A, (1999) *Cybercrime, Cyber Terrorism, Cyber Warfare: Averting an Electronic Waterloo*. CSIS Publications: New York, NY.

Yar, (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4)407-427

APPENDIX 1

QUESTIONS FOR AN UNSTRUCTURED INTERVIEW

Introduction

My name is **Ayomide ALOKUN**, I am a postgraduate student of the department of political science and international relations, landmark university Omu-Aran, and I am carrying out a study on "Economic and Financial Crimes Commission (EFCC) and Cybercrime in Kwara State, Nigeria"

Key Informant Questions

This study is strictly for academic and research purpose. All information supplied will be used strictly for the purpose of this study and only will be treated with utmost confidentiality. Hence, your name is not required. I solicit for your sincere cooperation by providing your time to answer the questions herein as honest as possible. You have been purposively selected for this study. Thanks for your anticipated cooperation.

SECTION A: What are the Factors That Motivate Youths' Involvement in Cybercrime in Kwara State Nigeria?

1. What are the indices that encouraged youths' participation in cybercrime?
2. What are the reasons youths in Kwara State are heavily participating in cybercrime?
3. How deep has cybercrime eaten into the Nigerian system?
4. In what ways has cybercrime affected the Nigerian system?

SECTION B: How Effective are the Strategies of EFCC for Detecting Cybercrime among Youths in Kwara State Nigeria?

1. How has the EFCC been able to detect cybercrime among youths in Kwara State?
2. What are the strategies put in place by the EFCC to curb cybercrime among youths in Kwara State?
3. What were the initial strategies put in place by the EFCC to curb cybercrime among youth in Kwara State?
4. Does the EFCC face difficulty in detecting cybercrime offenders

SECTION C: What are the Challenges Confronting EFCC in Detecting Cybercrime among Youths in Kwara State?

1. What are the challenges facing the EFCC in detecting cybercrime among youths in Kwara State?
2. How has the EFCC been able to overcome the challenges?
3. Have there been any success recorded so far by the EFCC in curbing cybercrime among youths in Kwara State?
4. What are the challenges faced by the EFCC in investigating cybercrime among youths in Kwara State?
5. What are the challenges confronting the EFCC in making conviction on cybercrime?

APPENDIX 2