THE IMPACT OF CYBER CRIME ON NIGERIA'S IMAGE IN THE INTERNATIONAL COMMUNITY: A REPORT OF RETURNED LEGAL MIGRANT

Precious Ifechukwude CHIEDU
SSC1909522

DEPARTMENT OF POLITICAL SCIENCE
FACULTY OF SOCIAL SCIENCES
UNIVERSITY OF BENIN
BENIN CITY, EDO STATE

MAY 2024

ABSTRACT

The study is concerned with the assessment of the Impact of Cyber Crime On Nigeria's image in The International Community, using the report of returned legal migrants, the study adopted an interview schedule to collate the response of 10 returned legal migrants. The study found out that; cybercrime is rampant in Nigeria, encompassing various illicit activities such as phishing scams, online fraud, identity theft, and malware attacks. This prevalence of cybercrime not only poses significant challenges to individuals and businesses within Nigeria but also tarnishes the country's reputation in the international community. The research also explored the report of returned legal migrants examining the profound challenges they face upon reintegration into Nigerian society. Stigmatization, social ostracism, and difficulties finding legitimate employment opportunities were commonly reported experiences, reflecting the enduring impact of their involvement in cybercriminal activities abroad. The study also highlights the diplomatic ramifications of cybercrime on Nigeria's international relations and foreign policy objectives. Instances of cyber attacks originating from Nigeria can strain bilateral ties, undermine trust and cooperation with foreign partners, and damage Nigeria's reputation as a responsible member of the global community. The study recommended that the EFCC have to increase its task to salvage the image of Nigeria in the international community as a whole by increasing efforts to curb cyber crimes among Nigerians, also the government should create an enabled enviroment for citizens to be able to go about legitimate businesses to make ends meet.

CHAPTER ONE

INTRODUCTION

1.1. Background to the study

In an increasingly interconnected world dominated by digital technologies, the phenomenon of cybercrime has emerged as a ubiquitous threat, transcending borders and permeating every facet of society (Norton, 2020). With its profound implications for national security, economic stability, and social cohesion, cybercrime poses a formidable challenge to governments, businesses, and individuals worldwide (UNODC, 2013). Nowhere is this challenge more pronounced than in Nigeria, a nation grappling with the complex intersection of technological advancement, socio-economic inequality, and global perceptions.

Nigeria, often celebrated for its vibrant cultural tapestry, abundant natural resources, and entrepreneurial spirit, finds itself at a crossroads as it contends with the shadow cast by cybercrime on its international image (Sarkar, 2018). While the nation has made significant strides in various sectors, including telecommunications, finance, and entertainment, the scourge of cybercrime threatens to undermine these achievements and tarnish Nigeria's reputation on the global stage.

The implications of cybercrime extend far beyond the realm of digital security, reverberating across diplomatic corridors, trade relations, and migration dynamics (Choo,

2011). As Nigeria strives to assert its position as a regional leader and an attractive destination for investment and tourism, the prevalence of cybercrime presents a stark reality check, prompting introspection and concerted action.

Cybercrime in Nigeria has reached alarming proportions, with various reports highlighting the country's prominence in online fraudulent activities. The Nigerian cybercriminal landscape encompasses a wide array of illicit activities, including phishing scams, identity theft, online fraud, and sophisticated hacking operations. These cybercriminal activities not only inflict financial losses on individuals and businesses globally but also tarnish Nigeria's reputation on the international stage. The impact of cybercrime on Nigeria's reputation is multifaceted. Firstly, Nigeria's association with cybercrime reinforces negative stereotypes about the integrity and trustworthiness of its people, perpetuating a narrative of widespread criminality. This damages the country's image as a reliable partner for business and investment, deterring potential investors and hindering economic growth.

It has been put forth that several socio-economic factors drive individuals in Nigeria to engage in cybercriminal activities, contributing to the country's negative image abroad. High unemployment rates, particularly among the youth population, create a fertile ground for recruitment by cybercrime syndicates. With limited opportunities for formal employment, many individuals, often with advanced technical skills, turn to cybercrime as a means of livelihood. Additionally, economic inequality exacerbates the allure of

cybercrime, as individuals from marginalized communities seek to improve their socio-economic status through illicit means. The promise of quick and substantial profits through cybercriminal activities, coupled with the perceived low risk of detection and prosecution, entices individuals to engage in fraudulent schemes and online scams.

The ramifications of cybercrime on Nigeria's diplomatic relations and foreign policy objectives are significant, with the potential for strained bilateral ties and reduced foreign investment. Cybercriminal activities originating from Nigeria can strain diplomatic relations with other countries, particularly those affected by cyber attacks or online fraud perpetrated by Nigerian cybercriminals. Foreign governments may demand accountability and cooperation from Nigeria in addressing cybercrime issues, leading to diplomatic tensions and potential sanctions or restrictions on bilateral cooperation. Moreover, Nigeria's reputation as a reliable partner for international collaboration may be tarnished, hindering its ability to advance its foreign policy objectives and participate effectively in regional and global initiatives.

Against this backdrop, this study seeks to unravel the intricate nexus between cybercrime and Nigeria's international image, focusing on the experiences and perceptions of returned illegal migrants who have been implicated in cybercriminal activities. By delving into the personal narratives, motivations, and socio-economic factors driving individuals to engage in cybercrime, this research endeavors to shed light on the multifaceted dynamics at play and chart a course towards meaningful solutions.

The gravity of the issue at hand cannot be overstated. Nigeria's reputation in the international community is not merely a matter of pride but a crucial determinant of its ability to attract foreign investment, foster diplomatic relations, and promote cultural exchange. As such, understanding the impact of cybercrime on Nigeria's image is paramount for policymakers, law enforcement agencies, and civil society organizations alike.

Moreover, the lens through which Nigeria is perceived on the global stage has profound implications for its citizens, particularly those who have been ensnared in the web of cybercrime and subsequently returned to their homeland. The stigma associated with involvement in illegal activities abroad can have far-reaching consequences, affecting employment prospects, social integration, and psychological well-being.

In light of these considerations, this study endeavors to provide a comprehensive analysis of the interplay between cybercrime and Nigeria's international image, drawing upon a diverse array of perspectives. By amplifying the voices of returned illegal migrants and situating their experiences within the broader socio-economic context, this research aims to inform evidence-based policies and interventions aimed at mitigating the negative effects of cybercrime and safeguarding Nigeria's reputation in the global arena.

1.2. Statement of the Problem

Cybercrime has emerged as a pervasive threat in Nigeria, posing significant challenges to the nation's international image and reputation. Despite Nigeria's strides in various sectors, including telecommunications and finance, the prevalence of cybercriminal activities casts a shadow over its global standing. This study seeks to address the following key issues:

Addressing the extent of cybercrime in Nigeria requires concerted efforts from government agencies, law enforcement authorities, and civil society organizations to strengthen cybersecurity measures, enhance legal frameworks, and promote cybercrime awareness and education initiatives. By combating cybercrime effectively, Nigeria can mitigate its negative impact on the nation's reputation and foster trust and confidence in its digital ecosystem.

It is also essential to identify the socio-economic drivers of cybercrime in Nigeria requires a holistic approach that encompasses job creation, skills development, and social empowerment initiatives targeting at-risk populations. By providing viable alternatives to cybercrime and addressing the root causes of socio-economic inequality, Nigeria can mitigate the negative impact of cybercrime on its international image and foster a more inclusive and resilient digital society.

Furtehrmore, addressing the experiences and perceptions of returned illegal migrants involved in cybercrime requires comprehensive reintegration support programs, including

access to education, vocational training, and psychological counseling. By empowering these individuals to rebuild their lives and contribute positively to society, Nigeria can mitigate the negative implications of their past involvement in cybercrime on the country's international image.

Ultimately, restoring Nigeria's reputation on the global stage requires a comprehensive and coordinated approach that addresses the root causes of cybercrime, fosters international cooperation, and promotes trust and confidence in Nigeria's digital ecosystem. By taking proactive measures to combat cyber threats and uphold cybersecurity standards, Nigeria can rebuild its reputation and emerge as a trusted partner for international collaboration in cyberspace.

By addressing these pressing issues, this study aims to provide valuable insights into the complex interplay between cybercrime and Nigeria's international image, informing evidence-based policies and interventions aimed at safeguarding the nation's reputation and fostering positive perceptions in the international community.

1.3. Research Objectives

The major objective of the study is to investigate the Impact of Cyber Crime on Nigeria's Image in the International Community, which focus on returned illegal migrants; specifically, the study seeks to;

1. Assess the prevalence and nature of cybercrime in Nigeria and their impact on individuals, businesses, and the broader society.
2. Investigate the socio-economic factors in Nigeria driving individuals to engage in cybercriminal activities.
3. Explore the experiences and perceptions of returned illegal migrants who have been involved in cybercrime, including the challenges they face upon reintegration into Nigerian society.
4. Examine the ramifications of cybercrime on Nigeria's diplomatic relations and foreign policy objectives.
5. Evaluate the effectiveness of current strategies and interventions in mitigating the negative effects of cybercrime and restoring Nigeria's reputation on the global stage.

1.4. Research Question

The following research questions were formulated to guide the study;

1. What is the prevalence and nature of cybercrime in Nigeria, and how does it impact the nation's reputation in the international community?
2. What socio-economic factors drive individuals to engage in cybercriminal activities in Nigeria, contributing to the country's negative image abroad?
3. What are the experiences and perceptions of returned illegal migrants who have been involved in cybercrime, and how do they affect Nigeria's international image?
4. What are the ramifications of cybercrime on Nigeria's diplomatic relations and foreign policy objectives, including potential strains on bilateral ties and reduced foreign investment?
5. How effective are current strategies and interventions in mitigating the negative effects of cybercrime and restoring Nigeria's reputation on the global stage?

1.5. Scope of the Study

The scope of the study is concerned about the cyber crime in Nigeria, in which the boarders of the research is narrowed around Nigerians who are returned illegal migrants.

1.6. Significance of the Study

The findings of this study will provide valuable insights for policymakers and government agencies in Nigeria to develop evidence-based policies and interventions aimed at addressing cybercrime and safeguarding the nation's international image. By understanding the socio-economic drivers and diplomatic ramifications of cybercrime, policymakers can formulate targeted strategies to enhance cybersecurity measures, strengthen law enforcement efforts, and promote international cooperation in combating cyber threats.

The study will contribute to a better understanding of the implications of cybercrime on Nigeria's diplomatic relations and foreign policy objectives. By identifying potential strains on bilateral ties and diplomatic tensions resulting from cyber incidents, policymakers can engage in proactive diplomacy and dialogue with foreign counterparts to address mutual concerns and promote trust and cooperation in cyberspace.

The research will shed light on the experiences and perceptions of returned illegal migrants involved in cybercrime, highlighting the social and psychological implications of their actions on Nigerian society. By understanding the challenges faced by these individuals upon reintegration and their impact on Nigeria's international image, policymakers and civil society organizations can develop targeted support programs to facilitate their rehabilitation and promote social cohesion.

1.7. Definition of Terms

The following key terms are identfied in this study which are briefly explained.

Cybercrime: For the purpose of this study, cybercrime refers to any illegal or unethical activities conducted over digital networks or through the use of digital technologies. This includes but is not limited to hacking, phishing, online fraud, identity theft, malware distribution, and other forms of cyber-enabled criminal behavior.

Nigeria's International Image: Nigeria's international image refers to the perception and reputation of the country on the global stage. It encompasses how Nigeria is viewed and evaluated by foreign governments, international organizations, businesses, media outlets, and individuals, including both positive and negative perceptions.

Socio-Economic Factors: Socio-economic factors refer to the social and economic conditions that influence individuals' decisions and behaviors. This includes variables such as unemployment rates, poverty levels, income inequality, education levels, access to technology, and digital literacy rates, which may impact the prevalence and drivers of cybercrime.

Returned Illegal Migrants: Returned illegal migrants are individuals who have migrated to other countries without legal authorization and have subsequently been deported or voluntarily returned to Nigeria. In the context of this study, returned illegal migrants may have been involved in cybercriminal activities while residing abroad.

Diplomatic Relations: Diplomatic relations refer to the formal relationships and interactions between Nigeria and other countries in the international community. This includes diplomatic exchanges, treaties, agreements, negotiations, and cooperation initiatives aimed at promoting mutual interests, resolving disputes, and advancing diplomatic objectives.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL FRAMWORK

This Chapter deals with the review of related literatures, which is summarily divided alongside the conceptual, empirical and theoretical review. The Literature review looked into the conceptuaal perspective on the use of the internet, history of Cyber Crime/Internet Fraud in Nigeria, Effects of Cyber Crime/Internet Fraud On Nigeria's Image, Effects of Cyber Crime on The Inflow of Foreign Direct Investment, incidence of cyber crime in Nigeria, Nigeria Cyber Crime Policy Frameworks and Its Inter-Operability. The theoretical review employed in this study is the Differential Association Theory of Crime.

2.1. CONCEPTUAL PERSPECTIVE ON THE USE OF INTERNET

Vladimir (2015) described the internet as a global network which is meant to unite millions of computers located in different countries and opens broad opportunities to obtain and exchange information but it is now being used for criminal purposes due to and especially, the economic factors. Nigeria is faced with economic challenges such as poverty, unemployment, corruption, amongst others, thereby making this crime thrives.

Prior to the advent of internet, there have been habitual commissions of fraud. Fraudsters carried out their operations in different ways and forms across the globe. Those who attempt fraud on the internet are just the latest in a long line of those trying to

con the unassuming. In the early 80s and toward late 90s, there witnessed the production and distribution of counterfeit money. With one of the most imperative discoveries of the twentieth century, the internet fraud is much easier now for criminals as they are capable of acting beyond national boundaries and their immediate environment. Recently, the mode of contacting victims has been widened since the fraudsters need not to be physically present to commit the fraud. Longe and Chiemeke (2006) posited that fraudsters pick victims and approach by letter, faxes or electronic mail, without prior contact. Victims' contacts and addresses are obtained from telephone and email directories, business journals, magazines, newspapers or through web e-mail address harvesters. What can besaid is that fraudsters generally have taken advantage of the advent of internet to advance and change their modus operandi. Now those engaged in this type of fraud, can seat in the comfort of their homes or cyber cafes and reach out to unsuspecting victims from different parts of the world. In this section, the study will be examining the historical background of internet fraud in Nigeria, meaning of internet fraud, theory of crime and fraud and the different types of internet fraud.

2.2. HISTORY OF CYBER CRIME/INTERNET FRAUD IN NIGERIA

The history and growth of internet in Nigeria can be traced to 1995, when The Nigerian Internet Group was formed; this is a non-governmental organization, with the objective of facilitating the full access to internet in Nigeria. This group was formed after the first internet workshop organized by the Yaba College of Technology in collaboration

with a number of organizations including the Nigerian Communications Commission, National Data Bank, Literacy Training and Development Program for Africa (University of Ibadan) and Administrative Staff College of Nigeria (ASCON), with direct assistance from the United States Information Service (USIS). Regional Information Network for Africa (RINAF) and the British Council. In 1996, seven years after the introduction of internet service in United States, the Nigerian Communications Commission decided to license 38 internet service providers to sell internet services in Nigeria. The very first internet service provider "Link serve Limited" began operation in 1st of January 1997. (Vanguard Nigeria, 2010).

Another major African seminar was held in May 1999, where internet policies were made for African countries. It was organized by the Ministry of Communication and titled Africa Internet Summit (AFRINET 99). The research on the growth of internet usage in Nigeria was carried out by the International Communication Union between the periods of 1996 – 2009. They reported as follows; in 2000, it was 0.3% it moved up a little between 2002 and 2004, when it rose to 1.5%, by 2007 it had escalated to 7% and by 2008, it rose speedily to 15%. The research showed that as at 2007 Nigerians were the highest users of internet, but by 2009 Egyptians took over with 17% users in every 100 people, compared to Nigerian users of 15% in every 100 people. Currently in Nigeria, internet is available in every urban area, it is much easier as one can access it even on a mobile telephone. Often times, readers tend to misunderstand the meaning of internet fraud, and sometimes substitute the term cybercrime for internet fraud. However, what

must be noted is that internet fraud is one of the types of cybercrime. Other types of cybercrime include, cyber stalking, cyber bullying, online trafficking, child pornography, cyber terrorism and many more. Computer fraud is the only term that is used interchangeably with internet fraud while cybercrime is an umbrella for all forms of cyberspace perpetrated illegality.

The historical development of internet fraud in Nigeria is contentious. There have been diverse opinions on the actual regime and era that the fraud began in Nigeria. Though not a new concept, it is believed that it went rampant during the Shagari administration due to programs and policies introduced by the government during the period of his reign. History has shown that fraud began excessively during the Shehu Shagari regime, while some others believe that it was during the military era, these diverse views will be synchronized and synergized to produce a singular and comprehensive historical background to internet fraud in Nigeria. The term "419" is coined from section 419 of the Nigerian criminal code. Section "419" of the criminal code, laws of the federation of Nigeria and Lagos (1958) Chapter 42, states unequivocally that; "Any person who by any false pretense and with intent to defraud obtains from any other person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. ars. If the object is valued for five hundred pounds or upwards, he is liable to imprisonment for seven years. It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretense..."

Though this section has been engraved in the Nigerian criminal code since 1958, it was just a section like any of the five hundred and twenty-one sections in the code and did not beg for particular attention or distinction from other offences in the code. Modern scams have been linked and associated with Spanish prisoner scam dating of 19th century. The system of operation was that businessmen will be contacted by an individual allegedly trying to smuggle someone connected to a wealthy family out of prison in Spain. They will inform their targets to part with some amount of money to bribe the prison officers and promised to share the proceeds of the work with the targets after the operation. (Brunton, 2013), On the history of 419 scams in

Nigeria traced the history of the scams to "Second Republic between 1979 to 1983" under the administration of then President Shehu Shagari. According to the source, the modus operandi was such that many variants of the letters were sent. The example of such letter sent via postal email was addressed to a woman's husband and inquired about his health and a long, unexpected silence. It then asked what to do with profits from a $24.6 million investment, and ended with a telephone number. Other official letters were sent from a writer who said that he was a director of the state owned Nigerian National Petroleum Corporation. He said that he wanted to transfer $20 million to the recipient's bank account money that was budgeted but was never spent. In exchange for transferring the funds out of Nigeria, the recipient would get to keep 30% of the total amount. To start the process, the scammer asked for a few sheets of the company's letterhead, bank account numbers, and other personal information.

The above established that fraud and fraudsters have been in existence since time immemorial, and since the twenty first century era of the emergence of internet and computers, it is expected that fraudsters also change their modus operandi to be in sync with modern technologies and approaches.

EFCC (2006) reported the rate of internet crime in Nigeria and the position of the country amongst other countries where cybercrime is prevalent. The publication reported a retired civil servant with two other accomplices who defrauded a German citizen, Klaus Wagner a sum of USD 1, 714,080 through the internet. Ribadu (2007) the pioneer Chairman of EFFC posited that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other e-commerce kind of fraud. His position was later corroborated by the statement of Olugbodi (2010) where he opined that the most prevalent forms of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus/worms/Trojans.

The study shall consider the following examples of the most frequent types of Internet fraud;

1. **Romance scam**

Great Britain has the highest victims of romance scam. The research in 2012 showed that more than 230,000 people may have fallen victims of romance fraudsters in Great Britain alone (Whitty & Buchanan, 2012). One can opine that romance scammer works on the

mentality and emotion of their victims, what they tend to achieve is to lower the defences of their victims by appealing to their romantic or compassionate side. They play on emotional triggers to get their victims to provide money, gifts and personal details. At the early stage of the relationship, giving of minor gifts may be reciprocal. Then eventually the scammer makes requests for small amounts of money for numerous reasons.

2. **Lottery scam**

As the name implies, there are so many sites, that offer fake lottery and in most cases victims supply sensitive information to these sites. It operates in this manner; an email is received from a lottery institution congratulating the individual of winning a lottery they did not participate in. The scammers usually demand for quick response from their victims. In addition, they advise victims to keep their winnings private to maintain security of the price won. The real scam comes when the victims are asked to pay some amount of money or fees to release their winning prize. Scammers often refer to these fees as insurance costs, government taxes, bank fees, etc.

3. **Phishing**

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers (See Anti-Phishing Working Group, 2004). The origin of the word is traced to the analogy that scammers are using email lures to fish for passwords and

financial data from the sea of Internet users. Another name for phishing is brand spoofing; it is the creation of email messages and Web pages that are replicas of existing and legitimate sites. These Web sites and emails are used to trick users / victims into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud. The sole aim of the phishing scammers is to establish in the subconscious of the victims that, information they received is from a genuine websites and thereby established their faith in them.

4. Cheque overpayment scam

This is particular to those that engage in buying and selling on the internet, especially those that are selling something on the internet, they may be approached or targeted by cheque overpayment. The operation is such way that, the seller might receive an offer from a buyer who is a scammer. After the offer, they intentionally write an overpayment cheque for the seller. Seller out of sincerity will alert the buyer, of the overpayment and the potential buyer scammer, will apologize thereby ask for the refund of the money through an online banking or through Western Union. The actual scam takes place, when the seller fails to cash the cheque before he/she sent the goods and the so called overpayment cash before he or she detects that the cheque will bounce or cheque bounces.

All these above mentioned methods or modes are the ways victims are deceived and fall prey to scammers. In the cases where prospected victims do not give in to the luring

tactic of the scammer certain software's are used to penetrate the computers of unassuming individuals retrieving vital personal information which can be used to facilitate fraudulent activities. Examples of that software are malware, spyware and worm.

2.3. EFFECTS OF CYBER CRIME/INTERNET FRAUD ON NIGERIA'S IMAGE

Internent fraud/Cyber Crime has its impact on the reputation on Nigeria in the international community. Ezedikachi (2021) reviewed 4 of this effects which are examined thus;

1. Tarnishing the country's reputation

Without any doubt, internet fraud has tarnished the image of this country in the international arena to an irreparable level. Cybercrime has created a bad image for Nigeria which has earned her a spot in the present ranking in Transparency International where Nigeria is being listed as one of the most corrupt nations in the world. (Folashade B. et. Al 2014) and Adomi (2018) have concluded it, when he opined that cybercrime has created an image nightmare for Nigeria. He said that most scam e-mails are thought to originate from Nigeria or Nigerians which is actually not the case. Nigerians are treated with suspicion in business dealings and transactions.

2. Lack of trust and confidence hinders profitable transaction

Nigerians are not trusted when it comes to business transaction in most countries abroad, the major reason for this is the level of fraudulent activities committed in their

country that have been attributed to Nigerian citizens, therefore foreigners find it difficult to trust Nigerians because of fear of losing their money and goods. In many cases online transactions would be made but the buyers never receive goods from sellers, this is why some online shopping sites refuse to include Nigeria on their list of countries for delivery e.g. eBay. According to reports sponsored by the Better Business Bureau online over 80% of online shoppers cites security as their primary concern when shopping online. About 75% of shoppers terminate the transaction when asked for their bank card details. The level of decadence of the Nigerian reputation has caused her citizens to be treated with suspicion in most or all their business dealings (Adomi, 2018).

3. Denied opportunities for Nigerians abroad

The situation of Nigeria's image is in direct comparison with the famous saying "One bad apple would spoil the bunch" because majority of Nigerians who do not have the slightest idea of what it takes to be a fraudster are suffering under the bad reputation umbrella created by those Nigerians caught. Nigerians are hardly considered when they seek asylum in foreign countries especially in the United Kingdom because of this bad reputation. In the last fifteen years only one out of ten of the 13000 asylum claims have been accepted. (Freeman, 2016). Folashade B. et. Al 2014, opined that cybercrime has negative consequences. Cybercrime threatens foreign investment as well as misrepresents the country among other nations as corrupt. It will also lead to stigmatization of business men and women and they will face certain barriers when carrying out legitimate

businesses. Majority of the business men and women go through a strenuous screening before foreigners would eventually agree to transact business with them.

4. **Inimical to the progress and development in the country**

Foreign direct investment is one of the major forms of economic development for a country and the refusal of foreign companies to invest may cause a retarded growth however significant in the economy of the home country. Fear of fraud is a major deterrence for foreign companies. The inevitable cycle of events if this continues, would result into "No Investment No Development, No Development No Employment and No Development and Employment No Progress". The amount of business deals and investment prospects that have been lost by Nigeria as a country due to fraudulent speculations is enough to make a significant change in all federating states of Nigeria (Folashade, 2013).

2.5. EFFECTS OF CYBER CRIME ON THE INFLOW OF FOREIGN DIRECT INVESTMENT

The cost of cybercrime to a society can be both qualitative and non-qualitative. There are the financial losses to individuals and organizations (figures rarely made public), as well as the sizable expense of security software and personnel to protect against possible digital incursions. Then there is the damage to brand image should a country be the unfortunate victim of online crimes.

- **Reduces the competitive edge of organizations**

Cyber crimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cyber crimes, there has being a global loss of billions of dollars annually. Cyber crimes may threaten a nation's security and financial health. Sensitive company information can be stolen and sold to a competitor company; this will automatically reduce the competitive strength of the company.

- **Time wastage and slows financial growth**

A lot of time is required by It professionals to constantly stay ahead of cyber criminals. Nations spend huge amount of money to fortify their information systems and ward off any attack by cyber criminals. These resources could have been channelled into others more productive sectors of the business or nation.

- **Loss of revenue**

Loss of revenue can be caused through identity theft, unauthorized access to important information like trade secrets and through scams in which the victims willingly pay for undelivered services. Recent statistics show that cyber crime fraud is over $559 million annually. Furthermore, research has shown that companies hit by cyber crime attacks lose revenue through a decline in stock prices by between 1-10%. Some revenue losses are indirect, for example, there is no structure for monitoring Internet businesses.

This leads to loss of revenue through missed taxes, piracy and intellectual property infringement. Other financial losses are caused by denial of service attacks (DoS). For example, in 2000, yahoo was hit by a DoS attack which caused their website not to be accessed for only 2 hours. Since yahoo received 50 million viewings per hour then, this attack is estimated to have cost them over $500,000 through missed revenue.

- **Reduced Productivity**

There is an unquantifiable loss through reduced productivity especially when people find themselves spending more time preventing, trouble shooting or protecting themselves from the effects of cyber crime, rather than engaging in more productive activities. Sometimes people are psychologically affected when the Internet is used as an avenue for social vendetta, cyber terrorism and cyber war fare. Due to the measures that many companies must implement to counteract cyber crime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform other time consuming acts in order to do their jobs. Every second wasted performing these tasks are seconds not spent working in a productive manner.

- **Damaged reputation**

High level of cyber crime in a country brings that country's name into disrepute within the international community. Nigeria is viewed by some countries in a negative manner when it comes to cyber crime.

- **Unemployment**

The Issue of cybercrime and its impact on the Nigerian economy in relations to FDI inflow has increasingly become worrisome and has seen an increase in the unemployment rating of the country, where FDIs and their parent companies flee the country and in some instances cut their staff strength due to cyber attacks that has led to fall in profit.

2.6. INCIDENCES OF CYBER CRIME IN NIGERIA

The instances reported here ranges from fake lotteries to the biggest internet scams. Elekwe, a chubbyfaced 28-year-old man made a fortune through the scam after two years of joblessness despite having diploma in computer science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business center. He has three sleek cars and two houses from his exploits.

Four Nigerians suspected to be operating a ^ prime prime 419^ prime prime scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors.

Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claims. They were arrested at the point of delivery by government officials. Mike Amadi was sentenced to 16 years' imprisonment for setting up a website that offered juicy but phony procurement contracts.

The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman. The biggest international scam of all was committed by Amaka Anajemba who was sentenced to 2 ½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.

Another Internet scam case was reported on the Sunday PUNCH newspaper of July 16, 2006 involving a 24year-old Yekini Labaika of Osun State origin in Nigeria and a 42-years- old nurse of American origin by name Thumbelina Henshaw in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name. Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19 ½ years having been found guilty of eightcounts against him.

Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations. Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm based in South Africa, on behalf of Business Software Alliance of South Africa.

The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 90%. The Centre also ranked Nigerian cyber-

crime impact per capita as being exceptionally high. Those involved are between 18-25 years mostly resident in the urban centers. The Internet has helped in modernizing fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud.

2.7. NIGERIA CYBER CRIME POLICY FRAMEWORKS AND ITS INTER-OPERABILITY

The ever-dynamic forms of corruption involving cyber and financial crimes have elicited a hard stance and posture in battling bribery and other related financial crimes. There is now a trend towards symbiotic and collective legal cooperation among various government institutions in confronting cyber and financial crimes and corruption.

This summary will look at some of the anti-corruption and financial legislations in Nigeria. These laws established many institutions for enforcement of anti-corruption laws. Notable among these institutions are:

2.7.1. Cybercrime Act 2015

The Cybercrime Act is made up of 59 Sections, 8 Parts; and 2 Schedules. Ist Schedule lists the Cybercrime Advisory Council, 2nd Schedule lists businesses to be levied for the purpose of the Cyber Security Fund under S * 0.44(2)(a) GSM service

providers and all telecom companies; Internet service providers, banks and other financial institutions, insurance companies and Nigerian Stock Exchange.

Below is a high-level overview of certain interesting provisions in the recently passed Cybercrime Act 2015 as it relates to the subject matter. (Lawpadi 2015).

1. Gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure and to implement procedures, guidelines and conduct audits in furtherance of that. Examples of systems which could be designated as such include transport, communication, banking etc.
2. Prescribes the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual or/and loss in financial transaction.
3. Hackers, if found guilty of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages or accessing and using data stored on computer systems.

4. Makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment.
5. Specifically creates child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.
6. Outlaws Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.
7. Prohibits cybersquatting, which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.
8. Forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g. Facebook and Twitter), it also prohibits the use of threats of violence and insulting statements to persons based on race, religion, colour,

descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10million or to both fine and imprisonment.

9. Mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.
10. Allows for the interception of electronic communication by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

(Law Padi 2015)

2.7.2. The Nigeria Criminal Code Act 1990

The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cybercrime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with "obtaining Property by false pretenses- Cheating." The specific provisions relating to cybercrime is section 419, while section 418 gave a definition of what constitutes an offence under the Act.

(418) "Any representation made by words, writing or conduct of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretense."

(419) "Any person who by any false pretense, and with intent to defraud, obtains from any other person anything capable of being stolen or induces any other person to deliver to any person anything capable of being stolen is guilty of a felony and is liable to imprisonment for three years." (Part 6, chapters 34 &38, Laws of the Federation of Nigeria Act, 1990).

2.7.3. Corrupt Practices and Other Related Offences Act (ICPC ACT)

Was established under the ICPC Act with specific mandate to enforce anti-corruption law. The Corrupt Practices and Other Related Offences Act Cap C31, Laws of the Federation of Nigeria 2004 established the Independent Corrupt Practices Commission (ICPC), which is one of the major anti-corruption agencies in Nigeria. The Act generally prohibits the various perceived acts of corrupt practices arising from interactions or transactions involving public/government officers and the general public or private individuals.

Offences and Penalties

The Act created four categories of offences in the eighteen sections dealing with offences under the Act.

The four categories of offences are:

- Giving and Receiving of bribes to influence public duty;
- Fraudulent Acquisition and Receipt of Properties;
- Failure to Report Bribery Transactions;
- Concealment of Information and Frustration of Investigation.

2.7.4. Economic and Financial Crimes Commission Act 2004 (EFCC ACT)

The Economic and Financial Crimes Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provide the legal framework for the establishment of the Commission. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

- The Investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc:
- The coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;
- The examination and investigation of all reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;

- Undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;
- Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes in consultation with the Attorney- General of the Federation;
- The coordination of all investigating units for existing economic and financial crimes in Nigeria.

The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud- Related Offences Act 1995; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act (EFCC, 2004). The Economic and Financial Crimes Commission Act 2002 (LFN 2004) (the Act) came into force on 14th of December 2002. The Act establishes the Economic and Financial Crimes Commission EFCC (the Commission) as the overarching body designated with the primary responsibility of investigating and prosecuting economic crimes and bringing perpetrators of such crimes within the ambit of the law. Section 46 of the Act defines "Economic Crime" as a "non- violent criminal activity committed with the objectives of earning

wealth illegally" Section 5 of the Act sets out the various offences with which the Act is concerned and the list is not exhaustive.

The Act is a tool for holistic approach to combating economic crimes in Nigeria. This can be seen when a review is made of the membership of the Commission and its powers under the Act. The membership of the Commission is drawn from virtually all the government bodies saddled with economic issues while the Commission has the powers of not only investigating and enforcement of the provisions of the Act, but also the enforcement of other legislations dealing with various economic crimes. Thus, section 7 of the Act confers special powers on the Commission to enforce the provisions of such other laws as:

- The Money laundering Act;
- The Advanced Fee Fraud and other Related Offences Act;
- The Failed Banks (Recovery of Debt and Financial Malpractices in Banks) Act;
- The Banks and other Financial Institutions Act;
- Miscellaneous Offences Act;
- Any other law or regulation relating to economic and financial crimes including the Criminal Code and Penal Code.

2.7.5. Advance Fee Fraud and Related Offences Act 2006

According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006): 'False pretense means a representation, whether deliberate or reckless, made by

word, in writing or by conduct of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' Section 383 sub-section 1 of the Nigerian Criminal Code states: A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing' (Advance Fee Fraud Act, Laws of the Federation of Nigeria, 2006) *1+. Economic crime is defined by the Act as the non- violent criminal and illicit activity committed with the objectives of earning wealth illegally, either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labor, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods."

Advance Fee Fraud and Other Fraud Related Offences Act 2006 was before now the only law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybercafés; it does not deal with the broad spectrum of computer misuse and cybercrimes.

2.7.6. Money Laundering Prohibition Act 2004

The Money Laundering Prohibition Act 2004 is directed or aimed at tracing, finding, freezing and possibly forfeiting among other things money and properties that have been acquired through illegal or prohibited means. Its intent is to prevent culprits from legitimizing proceeds from their criminal activities. It aims to detect, prevent and capture money acquired through one of many illegal means. The progenitor of the Act was basically enacted to combat "dirty money" gotten through trading in illicit drugs. However, over time, the scope of the law has been expanded through amendments to accommodate the dynamism of money laundering.

The Act is significantly symbiotic in nature, pooling resources and various anti money laundering agencies together in the battle against one of the most sophisticated crimes in the world. Thus, bodies such as:

- The Central Bank of Nigeria;
- The Nigerian Customs Service;
- The Nigerian Securities and Exchange Commission;
- The National Drug Law Enforcement Agency;
- The Economic and Financial Crimes Commission;
- The Corporate Affairs Commission; and even
- The Federal High Courts are united under the Act to fight money laundering.

Offences and Penalties

The stance of the Act in combating the crime is in form of prohibition and punishment of concealment and retention of properties obtained through money laundering, obstruction of investigation, conspiracy, aiding and abetting money laundering. Private persons and corporate bodies are also saddled with various duties aimed at aiding in combating the crime.

2.7.7. Judiciary:

Comprising all the courts in the country from lowest courts like Magistrate, Area and Customary courts to the highest court in the land, the Supreme Court. Section 6 of the Constitution establishes courts of

Superior record and these include The High Courts and others of coordinate jurisdiction, the Court of Appeal, and the Supreme Court. Various States laws provide for Courts Below High Courts like the Magistrate, Area or Customary Courts. All these courts are involved in the enforcement of anti-corruption laws as offenders are taken before them for prosecution sometimes leading to conviction and sentencing.

2.7.8. Code of Conduct Tribunal

This was established under the Code of Conduct Act and Paragraph 15 of Part One of the Fifth Schedule to the Constitution with the primary responsibility of trying those who violate the provisions of the Code. Of course, the main thrust of the Code is to prevent corruption in public life and offices.

2.7.9. Public Complaints Commission

This Commission is established under the Public Complaints Commission Act and operates to protect the public against corrupt oppressive exercise of power by public officers. Its investigations and recommendations can lead to prosecution or other forms of administrative or disciplinary measures against an erring especially, corrupt public officer.

2.7.10. Police & Other Security Agencies

Each of the security or law enforcement agencies of the state is established and governed by a specific statute. Police Act provides for Police with details of its functions. The National Securities Agencies Act provides for three agencies namely: The Defense Intelligence Agency, the National Intelligence Agency, and the State Security Service (SSS). Of course, the SSS is the most visible among them. Although the statute tried to delineate their functions, in practice they dovetail, interrelate or even integrate sometimes.

2.8. THEORETICAL FRAMEWORK

2.8.1. DIFFERENTIAL ASSOCIATION THEORY OF CRIME:

Edwin Sutherland, an American sociologist, propounded this theory. The central point of this theory is that, through interaction with others, individuals learn the values, attitudes. Techniques and motives for criminal behavior. To those that belong to this school of

thought, it is believed that the environment plays a vital role in formulating the behavior of an individual. To Sutherland, he believed that the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939).

The principle of differential association asserts that a person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to Violation of law. What this means is that an individual will become a criminal because they Are exposed to more favorable criminal behavior. What this explains for instance, is that Where we have five people, four of them are criminals, the fifth person may on the long Run be influenced by the activities and action of these other four and then learn the act of Criminality of these people, and may eventually join them. The basic point of Sutherland is That criminal behavior is learned (Sutherland 1939). Communication is the major tool of Learning criminal behavior; it is learnt through interactions with the perpetrators of crimes and by befriending them. The principal part of the learning of criminal behavior occurs Within intimate personal groups. The best way to learn criminal behavior is by learning the Technique for committing the crime. It means that to know how to perpetrate internet fraud, what is needed to be done is to learn the technique from veteran perpetrators. This explains The ever increase in the number of yahoo boys in our various university campuses. From the above background on differential association theory, it is clear that the theory can be applied to cybercrimes. The focal point of this theory is that criminal behavior is learned through social interaction with others. The

medium of social interaction for most internet fraudsters may come through electronic communications with other individuals who share similar interests.

CHAPTER THREE

METHODOLOGY

3.1. Research Design

This is the specification of the method and procedures for acquiring the information needed for the research. The research design adopted is the exploratory research design method, in which the research investigates the subject matter using a descriptive qualitative method of data collection through field survey from respondents within the study population.

3.2. Population and Sample of the Study

The population of the study deals with Nigeria migrants who have experienced the effect of cyber crime on Nigeria image in the international community. 10 returnees were randomly selected to serve as the sample size of the study.

3.3. Research Instrument

The research instrument is through a structured interview schedule for the study, in which questions were formulated from the research question to serve as the research instrument to collect data from the respondents. The totla number of questions in the schedule is 15,

which is divided into 6 secgement; the first is the demographic data of the respondents, while the reminaing segments wetre divided across the rseaerch questions.

3.5. Validity of Research Instrument

The Interview schedule was submitted to the project supervisor and two other experts in the department of political science, who made their input into the interview schedule. Their inputs were included in the final draft of the interview schedule.

3.6. Method of Data Collection and Analysis

The resondents to the interview were coded from Respondents 1 to Respondents 10: Responses were collected using social media platforms such as Facebook, Whatsapp and Twitter to conduct the interview. The responses and findings were collected, presented and inteerreted ina descriptive method.

CHAPTER FOUR

PRESENTAION AND DISCUSSION OF FINDINGS

4.1 Presentation of Results

SECTION A: DEMOGRAPHY OF THE RESPONDENTS

RESPONDENT DATA (N=10)		
AGE OF REPONDENTS		
AGE RANGE	**FREQUECNY**	**PERCENTAGE %**
18 – 28	6	60%
29 – 39	4	40%
40 and Above	0	0
TOTAL	10	100
GENDER OF THE RESPONDENTS		
Gender	**FREQUECNY**	**PERCENTAGE %**
Male	8	80%
Female	2	20%
TOTAL	10	100%
EDUCATIONAL LEVEL OF THE RESPONDENTS		
EDUCATION LEVEL	FREQUECNY	PERCENTAGE %
Primary	0	0
Secondary	0	0
Tertiary	10	100%
None	0	0
TOTAL	10	100%
RELIGION OF THE RESPONDENTS		
RELIGION	FREQUECNY	PERCENTAGE %
Christian	7	70%

Muslim	0	0%
Traditional	1	10%
None	2	20%
Total	10	100

Source: Field Survey 2024

SECTION B: INTERVIEW SCHEDULE RESEARCH QUESTION

Rsearch Question 1: Prevalence and Nature of Cybercrime in Nigeria

Can you describe any experiences or encounters you've had with cybercrime in Nigeria?

Participant: Well, cybercrime is unfortunately quite common in Nigeria. Personally, I've had friends and acquaintances who have fallen victim to online scams, phishing emails, and even hacking attempts on their social media accounts. It's definitely a pervasive issue.

What types of cybercriminal activities have you observed or heard about in your community?

Participant: There's a wide range of cybercriminal activities happening here. From email scams promising huge sums of money to fraudulent websites selling counterfeit products, it seems like there's always something new popping up. I've also heard about cases of identity theft and online fraud targeting unsuspecting individuals.

How do you perceive the impact of cybercrime on Nigeria's reputation in the international community?

Participant: Cybercrime definitely has a negative impact on Nigeria's reputation abroad. It reinforces stereotypes about the country being a hub for criminal activities, which can deter foreign investors and tourists. It's unfortunate because Nigeria has so much more to offer, but cybercrime casts a shadow over all of that.

Research Question 2: Socio-Economic Factors Driving Cybercrime

what socio-economic factors do you believe contribute to individuals engaging in cybercrime in Nigeria?

Participant: There are several factors at play here. High unemployment rates, especially among the youth population, create a sense of desperation and drive some individuals to seek alternative means of income, even if it's through illegal activities like cybercrime. Economic inequality also plays a role, as people from disadvantaged backgrounds may see cybercrime as a way to improve their financial situation.

Have you or anyone you know been driven to cybercrime due to socio-economic challenges?

Participant: Fortunately, I haven't personally been driven to cybercrime, but I've heard stories of people who have. It's heartbreaking to see talented individuals resorting to illegal activities out of desperation. I think addressing the root causes of socio-economic inequality is crucial in tackling cybercrime effectively.

Research Question 3: Experiences of Returned Illegal Migrants

Can you share your experiences as a returned illegal migrant who may have been involved in cybercrime abroad?

None of the participants have directly expeirneced or been involved in cybercrime. The respondents suggested the following measures such as awareness campaigns, law enforcement initiatives, and cybersecurity measures as a means of combatting the prevalence of cyber crimes among Nigerians. However, the respondents think there's still room for improvement, particularly in terms of coordination between government agencies and international cooperation. Cybercrime is a complex and evolving issue, so it requires a multifaceted approach to address effectively.

Research Question Four: Effectiveness of Current Strategies and Interventions in Mitigating the Negative Effects of Cybercrime and Restoring Nigeria's Reputation On the Global Stage

The effectiveness of current strategies and interventions in mitigating the negative effects of cybercrime and restoring Nigeria's reputation on the global stage is mixed. While some progress has been made in addressing cyber threats and promoting

cybersecurity awareness, significant challenges remain that hinder Nigeria's ability to combat cybercrime effectively and rebuild its international reputation.

One of the primary challenges is the lack of adequate cybersecurity infrastructure and capabilities in Nigeria. Despite the existence of laws and regulations aimed at combating cybercrime, enforcement mechanisms are often weak, allowing cybercriminals to operate with impunity. This undermines public trust in Nigeria's ability to address cyber threats and contributes to a negative perception of the country's cybersecurity readiness on the global stage.

Additionally, Nigeria faces persistent socio-economic challenges that contribute to the prevalence of cybercrime. High unemployment rates, economic inequality, and digital literacy gaps create fertile ground for cybercriminal activities to thrive. Addressing these root causes requires comprehensive socio-economic interventions aimed at providing alternative livelihood opportunities, promoting digital literacy, and empowering vulnerable populations to resist the temptation of engaging in cybercrime.

Furthermore, Nigeria's reputation as a hub for cybercrime has significant diplomatic implications, straining bilateral relations with other countries and undermining the country's credibility in international forums. To restore Nigeria's reputation on the global stage, concerted efforts are needed to strengthen diplomatic engagement, promote transparency and accountability in addressing cyber threats, and foster international cooperation in combating cybercrime networks operating across borders.

Despite these challenges, there have been some positive developments in Nigeria's efforts to combat cybercrime and restore its international reputation. The establishment of dedicated cybersecurity agencies and initiatives, such as the Nigerian Cybercrime Advisory Council (NCAC) and the National Information Technology Development Agency (NITDA), demonstrate a commitment to addressing cyber threats at the national level. Additionally, awareness campaigns and capacity-building programs aimed at promoting cybersecurity best practices and digital literacy are helping to raise awareness and empower individuals to protect themselves from cyber threats.

However, these efforts must be sustained and expanded to effectively mitigate the negative effects of cybercrime and restore Nigeria's reputation on the global stage. This requires a multi-stakeholder approach involving government agencies, law enforcement authorities, civil society organizations, and international partners working collaboratively to strengthen cybersecurity measures, address socio-economic vulnerabilities, and promote Nigeria as a responsible and trustworthy actor in cyberspace. Only through concerted and sustained efforts can Nigeria overcome the challenges posed by cybercrime and reclaim its standing as a respected member of the global digital community.

4.2 DISCUSSION OF THE FINDINGS

Prevalence and Nature of Cybercrime in Nigeria:

The research findings reveal that cybercrime is rampant in Nigeria, encompassing various illicit activities such as phishing scams, online fraud, identity theft, and malware attacks. Participants highlighted the pervasive nature of cybercriminal activities in their communities, with many reporting personal experiences or knowledge of individuals affected by cybercrime incidents. This prevalence of cybercrime not only poses significant challenges to individuals and businesses within Nigeria but also tarnishes the country's reputation in the international community. The findings underscore the urgent need for comprehensive measures to address cyber threats and safeguard Nigeria's digital ecosystem.

Socio-Economic Factors Driving Cybercrime:

The research findings shed light on the socio-economic factors driving individuals to engage in cybercriminal activities in Nigeria. High unemployment rates, economic inequality, and limited job opportunities were identified as key drivers pushing some individuals, particularly youth, towards cybercrime as a means of survival or enrichment. Additionally, digital literacy gaps and lack of awareness about cybersecurity best

practices were highlighted as contributing factors, making individuals more susceptible to falling victim to cybercrime or being recruited into cybercriminal networks. Addressing these socio-economic drivers requires holistic interventions that not only create economic opportunities but also empower individuals with the knowledge and skills to navigate the digital landscape safely and responsibly.

Experiences of Returned Illegal Migrants:

The findings pertaining to returned illegal migrants who have been involved in cybercrime abroad reveal the profound challenges they face upon reintegration into Nigerian society. Stigmatization, social ostracism, and difficulties finding legitimate employment opportunities were commonly reported experiences, reflecting the enduring impact of their involvement in cybercriminal activities abroad. These experiences not only exacerbate the reintegration process but also contribute to negative perceptions of Nigeria's international image, reinforcing stereotypes about the country as a source of cybercrime. To address the challenges faced by returned illegal migrants, targeted support programs and rehabilitation initiatives are needed to facilitate their reintegration and mitigate the negative implications for Nigeria's reputation.

Diplomatic Ramifications:

The study highlights the diplomatic ramifications of cybercrime on Nigeria's international relations and foreign policy objectives. Instances of cyber attacks originating from Nigeria can strain bilateral ties, undermine trust and cooperation with foreign partners,

and damage Nigeria's reputation as a responsible member of the global community. Diplomatic engagement and international cooperation are therefore crucial in addressing cyber threats collaboratively and promoting mutual understanding and trust among nations. These findings emphasize the importance of proactive diplomacy and dialogue to address mutual concerns and foster cooperation in combating cybercrime at the regional and global levels.

Effectiveness of Current Strategies and Interventions:

The study reveals mixed findings regarding the effectiveness of current strategies and interventions in mitigating the negative effects of cybercrime and restoring Nigeria's reputation on the global stage. While efforts have been made to enhance cybersecurity measures, promote awareness, and strengthen law enforcement capabilities, significant challenges persist, including enforcement gaps, resource constraints, and institutional capacity limitations. Addressing these challenges requires sustained political will, investment in cybersecurity infrastructure and human capital, and collaboration with international partners to develop and implement comprehensive, evidence-based strategies to combat cybercrime effectively.

CHAPTER FIVE

SUMMARY, CONLUSION AND RECONMENDATIONS

5.1. SUMMARY OF THE FINDINGS

The study was concerned about the influence of cyber crimes on the image of Nigeria within the international community, which birthed the objectives of identifying the the types of cyber crime which comes in various form; another objective of the study was to identfy the fundamental causes of cyber crimes among young people in Nigeria and to find out its effect on the image of Nigeria within the international community; finally the study sought to assess the case study of Hushpuppi and how this incidence has affected the image of Nigeria within the international community. From the survey that was carried out on this issue, the following are the findings of the study;

1. The findings of the study help to sehd light into the understanding that the cyber crime comes in various kinds or formats and these crimes comes through; Hacking of people's email and bank account Credit card fraud, Software piracy Cyber identity theft, cloning of website/Phishing, Sweet heart swindle (Social network) or relationship scam; among many possible other formats are variants in which cyber crimes present itself.

2. The study also discovered that that cyber crimes is not an independent variable, rather it is an independent variable that is birthed as a result of other socio-economic issues such as Unemployment, poverty, corruption, weak laws; among many possible factors; and these issues have been identified to be factors responsible for the increase in cyber crimes among Nigeria Youths.
3. The study further discovered that Nigeria is daily loosing its image within the international community as a result of the prevalence of cyber crimes among its youthful population, which affectes the ability of the country to relate cordially with other country. In certain cases, it has been identified that their country who make it difficult for Nigerians to come into their country either for business, research or educational purposes due to the image of the country being tainted by cyber crime among other factors.
4. Finally, the study delved into te issue of Hushpuppi and how his arrest for cyber crime has affected the image of the country and also served as a influence for Nigerian youths who do not seem to back down despite the reality of this arrest and many more being done by the EFCC.

The study therefore informed that cyber crime is proven to be on danger to the countrys image and relevance within the global world and it is important that to address this issue requires the the need to prioritize a fundamenmtal approach over cosmetic approach of arresting those caught within the confines of cyber criomes. Rather more investment should be done towards addressing the social conditions that

makes young Nigerians to see cyber crime as one of the lucrative way out of poverty and ameliorate the conditions that pushes young Nigerians into cyber crime.

5.2. CONCLUSION

The remarkable development in human history through computer technology has no doubt brought transformation in all aspects of life, especially in communication and information technology. However, the embracement of the internet by Nigerians has come with a lot of fraudulent acts. Individuals, groups, companies and government establishments have been found to be defrauded through the internet. Nigerians are valued in terms of what they possess and command economically. Conversely, those without economic success are undervalued and the pressure to achieve success is intensified. This necessitated some Nigerian individuals to devise survival strategies to attain economic success, thereby causing them to indulge in cybercrime. However, this has put Nigeria under negative scrutiny and that is not good for our image in international relations. Therefore, beyond the task of the EFCC trying to fight cyber crimes and other related offence, there seems to be a missing link the role of EFCC and the reduction in cyber crime, which spells new trajectory that there need to be more approach or trajectory that the govenrment and society need to employ in other to address and reduce cyber crime in Nigeri which is discussed in the nect heading.

5.3. RECOMMENDATIONS

Based on the findings and conclusion of this study, the following recommendations are made:

1. Despite the activities of EFCC raiding young Nigerians who were aledged to be involved in cyber fraud and the parading of these young people in public, the menace of cyber fraud continue to persist in various formats, this tells that there are more fundamental factors that are left unattended to, which according to the findings of the study have proven to be issues such as unemployment, poverty, corruption amiong many other issues, therefore it becomes expedient for the government to embark on deliberate macro economic approach to address the fundamental cause that pushes youth into cyber crime, by creating an alternative lucrative means to make wealth that they wont have to see criminality as the easiest and feasible way out of lack and wants. Polices such as Modern Agriculture, Engineering, Tech etc should be enabled for young people to purse and make meaninging outcome from their lives.
2. Education is the most vital weapon for literacy; as such seminars and workshops should be organized from time to time with emphasis on internet safety. This will make the individuals learn to keep their personal information safe and youth will flee cybercrime.
3. The study shows that youths involved in internet fraud are either in tertiary institutions or have graduated from tertiary institution. It is therefore, recommended that curriculum which will include courses on internet fraud, internet management and its

prevention should be introduced to both tertiary and secondary schools to take care of the present social changes.

4. For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb internet fraud, there is need for them to understand both the technology and the individuals who engaged in this criminal act.
5. Cyber criminals' assets should be confiscated by the government if discovered. There should be imposition of 25 year-jail term for cyber-crimes. This will serve as deterrence to those youths who may want to indulge in such crime.
6. Internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they will not only be well informed about the current trends in cybercrimes, but also be security conscious.

5.4. SUGGESTION FOR FURTHER STUDIES

1. A study can be carried out to determine the effect of internet fraud on Nigeria populace using a wider scope of study.
2. A study can be carried out concentrating on students alone and their use of internet sites to determine the level of decadence this may cause on the Nigeria system and on the international system.
3. A study can also be carried out to examine cybercrime rates and other fraudulent act on the part of Nigerian youth and its effect on the global world and in international relations.

REFERENCES

Abiola, J. (2013). The Impact of Information and Communication Technology on Internal Control's Prevention and Detection of Fraud.

Adebayo, H. (2015, october 8). Premium times. Retrieved from http://www.premiumtimesng.com/news/top-news/191241-u-s-indicts-9-nigerians-overonline-romance-fraud.html

Adeoti, J. O. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. Journal of Social Sciences, 27(1), 53-58.

Adomi, E. E. (2008). Combating cybercrime in Nigeria. The Electronic library, 716-725.

Affairs, O. o. (2015, july Monday). Retrieved from TheUnited States Department of Justice: http://www.justice.gov/opa/pr/six-nigerian-nationals-extradited-south-africa-mississippiface-fraud-charges

Aina, A. (2008). The Internet and Emergency of Yahoo boys sub Culture in Nigeri. International journal of Cyber Criminology, 368-381.

Allison, S. F. (2003). A case study of identity theft (Doctoral dissertation, University of South Florida).

Aliyu, O. T. (2011). Social Organization of Internet Fraud among University graduates in Nigeria. Cyber crime journal, 860-875

Anderson, D. S., Fleizach, C., Savage, S., & Voelker, G. M. (2007, August). Spam scatter: Characterizing internet scam hosting infrastructure. In Usenix Security (pp. 1-14).

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

Antes, J., Conley, J., Morris, R., Schossow, S., Yee, Z., & Fang, F. (2008). Cyber Crimes: Real Life and in the Virtual World.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyber psychology, Behavior, and Social Networking, 14(12), 759-763.

Azeez, N. A., Iyamu, T., & Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In Computer and Information Sciences II (pp. 411-418). Springer London.

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa—Cybercrime and criminality in Ghana. Journal of Information Technology Impact, 11(2), 85-100.

Bocij, P. (2006). The dark side of the Internet: protecting yourself and your family from online criminals. Greenwood Publishing Group.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. Journal of Criminal Justice, 32(5), 477-493.

Burrell, J. (2008). Problematic empowerment: West African Internet scams as strategic misrepresentation. Information Technologies & International Development, 4(4), pp-15.

Brunton, F. (2013, May 19). Boston Globe. Retrieved from https://www.bostonglobe.com/ideas/2013/05/18/the-long-weird-history-nigerian mailscam/C8bIhwQSVoygYtrlxsJTlJ/story.html

Chawki, M. (2009). Nigeria tackles advance free fraud. J. Inf. Law Technol, 1(1), 1-20.

Clough, J. (2015). Principles of cybercrime. Cambridge University Press.

Cohen, A. K. (1955). Delinquent Boys; The Culture of the Gang.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.

Duah, F. R. A. N. C. I. S. C. A. (2013). Growing Global Threat of Cyber Crime: Implications for International Relations (Doctoral dissertation, University of Ghana).

E.E, A. (2008). Security and software for cyber cafes. Ibadan: Emerald group publishing limited.

E. JOSEPH, A. (2016). Cybercrime definition. Retrieved from Computer Crime Research Center: http://www.crime-research.org/articles/joseph06/

Ebenezer, J. A. Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience.

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. Business Intelligence JournalJanuary, 93-98.

Ejiofor, C. (2015). Retrieved from Naij.com: https://www.naij.com/68635.html

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. Human Ecology, 8(4), 389-406.

Freeman, C. (2016, 02 05). Retrieved from The Telegraph: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/nigeria/12143510/Nig erians-reputation-for-crime-has-made-them-unwelcome-in-Britain-says-countryspresident.html

Fried, R. B. (2001). Cyber scam artists: a new kind of. con. Crime scene investigator network.

Goutam, R. K., & Verma, D. K. (2015). Top Five Cyber Frauds. International Journal of Computer Applications, 119(7).

Hastings, D. (2014, february 4). www.nydailynews.com. Retrieved from Daily News: http://www.nydailynews.com/news/world/nigerian-man-arrested-case-dead-australianwidow-article-1.1601806

Hees, B. v. (2015, September 8). Nigerian jailed for online dating scam. Retrieved from iOL: http://www.iol.co.za/news/crime-courts/nigerian-jailed-for-online-dating-scam-1912847

Higgins, G. E. (2010). Cybercrime: An introduction to an emerging phenomenon (p. 3). McGraw-Hill Higher Education.

Igwe, C. N. (2007). Taking Back Nigeria from 419: What to Do about the Worldwide E-mail Scam--advance-fee Fraud. iUniverse.

International Mass-Marketing Fraud Working Group. (2010). Mass-marketing Fraud: A Threat Assessment.

Keyser, M. (2001). Explanatory Report to the convention on cyber crime. Budapest: European treaty series

Koong, K. S., Liu, L. C., & Wei, J. (2012). An examination of Internet fraud occurrences. Retrieved on 15th July.

Kshetri, N. (2006). The simple economics of cybercrimes. Security & Privacy, IEEE, 4(1), 3339.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. Third World Quarterly, 31(7), 1057-1079.

Kunz, M., & Wilson, P. (2004). Computer crime and computer fraud. Report Submitted to the Montgomery County Criminal Justice Coordinating Commission.

Longe, O. B., & Chiemeke, S. C. (2008). Cyber Crime and Criminality in Nigeria: What Roles Are Internet Access Points in Playing?

LONGE, O. B., CHIEMEKE, S. C., ONIFADE, O. F. W., & Longe, F. A. (2009). Camouflages and Token Manipulations-The Changing Faces of the Nigerian Fraudulent 419 Spammers. African Journal of Information & Communication Technology, 4(3), 12.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Technology Impact, 9(3), 155-172.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Technology Impact, 9(3), 155-172.

McGuire, M., & Dowling, S. (2013). Chapter 2: Cyber-enabled crimes—fraud and theft. Cybercrime: A review of the evidence.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

McQuade, S. C. (2008). Encyclopedia of cybercrime. Greenwood Press.

Nakamura, L. (2013). Cybertypes: Race, ethnicity, and identity on the Internet. Routledge.

Newman, G., & McNally, M. M. (2005). Identity theft literature review. Washington, DC: National Institute of Justice.

Ngo-Ye, T. (2013). Stress from Internet Fraud and Online Social Support. Stress, 5, 18-2013.

Ogwezzy, M. C. (2012). Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria. AGORA Int'l J. Jurid. Sci., 86.

Ojedokun, A. A. (2005). The evolving sophistication of Internet abuses in Africa. The International Information & Library Review, 37(1), 11-17.

Okeshola, F. B., & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state of Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Olugbodi, K. (2010). Fighting Cyber Crime in Nigeria. Retrieved September 10, 2011 from http. www. guide2nigeria, com/news_articles_About_ Nigeria.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cybercrimes and cyber laws in Nigeria. The International Journal of Engineering and Science (IJES), 2(4), 19-25.

Oriola, T. A. (2005). Advance fee fraud on the Internet: Nigeria's regulatory response. Computer Law & Security Review, 21(3), 237-248.

Oyesanya, F. (2005, May 25). Nigerian Internet 419 on the loose. Retrieved from http://www.nigeriavillagesquare.com/articles/nigerian-internet-419-on-the-loose.html

Oyesanya, F. (2004, March 28). Nigerian Internet on the loose. Retrieved from http://www.nigeriavillagesquare.com/articles/nigerian-internet-419-on-the-loose.html

PA, M. L. A. B., CATILOGO, P. A. C., & DEL ROSARIO, P. E. M. the incidence of cybercrime among youth social network sites users. Editor’s Note, 62.

Park, W. Digital Jewels," The 2014 Nigerian Cyber Threat Barometer Report," 2014.

Peel, M. (2006). Nigeria-related financial crime and its links with Britain. London: Chatham House.

Premium times. (2016). Retrieved from http://www.premiumtimesng.com/news/165608-police-nab-first-class-honours-graduateothers-over-internet-fraud.html

Reich, P. C. (2008). Cybercrime, Cybersecurity, and Financial Institutions Worldwide.

Ribadu, N. (2004). Obstacles to effective prosecution of corrupt practices and financial crime cases in Nigeria. House of Representative Committee on anti-corruption, national ethic and values, Kaduna, November, 2324.

Robins, A. (2010). Prevent, protect, pursue – a paradigm for preventing fraud. Computer fraud and security, 5-11.

Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation.

Saulawa, M. A. A., & Abubakar, M. K. (2004). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. Economic Times, 1.

Scam Watch. (2015, December). Retrieved from SCAMWATCH.COM: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

Singh, R., Singh, P., & Parveen, F. Cyber Crimes: The Rampaging Threat.

Smith, R. (2010). Identity theft and fraud. The Handbook of Internet Crime. Devon: Willan Publishing, 273-301.

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). Nigerian advance fee fraud. Canberra: Australian Institute of Criminology.

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). Principles of criminology. Rowman & Littlefield.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), 860.

Van De Walle, N., & Smith, D. J. (2007). A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria.

Vanguard Nigeria. (2010, October 27). Retrieved from http://www.vanguardngr.com/2010/10/internet-13-years-of-growth-from-ground-zero-innigeria-from-1960-1996

Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Vol. 4). Polity.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. Security Journal, 28(4), 443455.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15(3), 181-183.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15(3), 181-183.

Whitty, M. T., & Buchanan, T. (2012). The Psychology of the Online Dating Romance Scam. A Report for the ESRC. available online at www2. le. ac. uk/departments/media/people/monica-whitty/Whitty_romance_scam_report. pdf.

APPENDIX

INTERVIEW SCHEDULE.

SECTION A: DEMOGRAPHY OF THE RESPONDENTS

1. **GENDER:** Male ( ), Female ( )
2. **AGE:** 18 – 28 ( ), 29 – 39 ( ), 49 and Above ( )
3. **EDUCATIONAL BACKGROUND:** Primary ( ), Secondary ( ), Tertiary ( )
4. **RELIGION:** Christian ( ), Muslim ( ), African Traditional Religion ( ), None ( )

SECTION B: Interview Schedule Research Question

Research Question 1: Prevalence and Nature of Cybercrime in Nigeria

1. Can you describe any experiences or encounters you've had with cybercrime in Nigeria?
2. What types of cybercriminal activities have you observed or heard about in your community?
3. How do you perceive the impact of cybercrime on Nigeria's reputation in the international community?

Research Question 2: Socio-Economic Factors Driving Cybercrime

1. What socio-economic factors do you believe contribute to individuals engaging in cybercrime in Nigeria?
2. How do unemployment rates, economic inequality, and digital literacy levels influence the prevalence of cybercrime?
3. Have you or anyone you know been driven to cybercrime due to socio-economic challenges?

Research Question 3: Experiences of Returned Illegal Migrants

1. Can you share your experiences as a returned illegal migrant who may have been involved in cybercrime abroad?
2. What challenges did you face upon returning to Nigeria, particularly in terms of reintegration into society?

3. How do you think the involvement of returned illegal migrants in cybercrime impacts Nigeria's international image?

Research Question 4: Ramifications on Diplomatic Relations

1. In your opinion, how does cybercrime affect Nigeria's diplomatic relations with other countries?
2. Have you observed any diplomatic tensions or strains resulting from cyber incidents originating from Nigeria?
3. How do you think Nigeria's reputation as a responsible member of the global community is affected by cybercrime?

Research Question 5: Effectiveness of Interventions

1. What measures do you think are currently in place to combat cybercrime in Nigeria?
2. How effective do you believe these strategies and interventions are in mitigating the negative effects of cybercrime?
3. What additional measures do you think could be implemented to restore Nigeria's reputation on the global stage?