CYBERCRIME AND NIGERIA'S DIPLOMATIC REPUTATION IN DIASPORA

[1]Timothy Edem Sunday, [1]Atairet Clifford Atairet and [2]Willie, Clement Etti

[1]Department of Public Administration
Akwa Ibom State University
timothysunday998@gmail.com

[2]Department of Sociology and Anthropology,
Evangel University Akaeze, Ebonyi State

https://doi.org/10.60787/AASD-v2i1-34

Abstract

Cyberspace and its facilities have over the years become an indispensable tools that fast tract the growth of modern societies which Nigerian is not an exemption. Sadly, it has also become an avenue through which Nigeria loses her integrity, reputation and trust in the global sphere because of some illicit activities perpetuated by some Nigerians. This study examined cybercrime and its implications on Nigeria's image in diaspora. Exploratory research method was used in the study and data were obtained exclusively from secondary sources. Edwin Sutherland's Differential Association theory was adopted as the study's theoretical framework. Finding indicates that cybercrime has become a prevalent phenomenon in Nigeria where some Nigerian youths indulged in to harness wealth using cyber tools. It is also reveals that Nigeria's image has been greatly tarnished in the international community due to activities of few Nigerians who engage in cybercrime. Accordingly, the study recommends, amongst others, that adequate cyber securities should be put in place by government authorities responsible for cyber technology, and that the current legislation on cybercrime should be enforced through proper equipping of the anti-graft agencies.

***Keywords**: Cybercrime, internet, diaspora, scammers, and Nigeria image*

Introduction

The advent of Information and Communication Technology (ICT) has made the world a global village where every nation, including Nigeria, is striving to attain a high level of technological innovation. ICT has over the years brought tremendous changes and innovation to human society and is regarded as a major component in what is known as globalisation which connect the world with a much diversified ownership (Ige, 2008). Information can be assessed in any part of the globe with the help of the computer network and it is the easiest way of assessing data for research and other findings. Latest information needed by researchers is often found in the internet while examinations can be conducted through the Net and results released through the same means (Ezeani, 2010). As Africa's most populous nation (Atairet, 2020), Nigeria has not been left behind among other climes that embrace the emergence of modern information and communication technology though she clinched to it lately. With the emergence of ICT Nigerian like others learned various ways of disseminating information to any part of the world with just a click or touch of a button. The internet has become part and parcel of human existence in recent time and has brought an enormous transformation to every aspect of human lives, including education, banking and finance, business, government, health and social lives.

Nigeria has a considerable internet audience in Sub-Saharan Africa. But unfortunately, the emergence of ICT has come with its concomitant negative perils to individuals, societies and

governments in general. With the porous nature of internet security in Nigeria, criminal elements seem to take advantage of the penetrable nature of the unsecured network to perpetuate various crimes, including cybercrime. Cybercrime is also referred to as cyber fraud and it is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. All cybercrimes involve both the computer and the person behind it and its victims. In a broader sense, it is illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. Cybercrime, therefore, represents an extension of the conventional criminal behaviour alongside some novel illegal activities (Dennis, 2014).

Over the past two decades, the degree of cybercrime has increased significantly since the advents of the internet and digital revolution in Nigeria. Cybercrime has constituted a serious social problem to nations where its impacts are felt by both the rich and the poor. This category of crime has of recent become a prevalent phenomenon in Nigeria and a lucrative business which some youths see as a means of livelihood. Notably, cybercrimes are of various categories in Nigeria, including hacking, internet frauds, online scam, ATM or credit card fraud, piracy, identity theft spamming, cyber stalking and cyber defamation, among others. The attendant effects of cybercrime are not only felt by residence of the country, but also constitute threat to potential foreign investors. Most especially, Nigeria's integrity and external image in diaspora might have been reduced to mud due to her high perceived rates of internet fraudsters. Perpetuators of cybercrime in the country do not only carry out their heinous activities within the shores of Nigeria, but traverse beyond the country borders with series of online crimes perfected across the internet, thus tarnishing the image of the country. It is from this backdrop that the paper seeks to appraise the implications of cybercrime on Nigeria foreign image.

Theoretical Framework

Differential association theory, propounded by a renowned Sociologist, Edwin Sutherland in 1939, was adopted as a theoretical framework. According to this theory, Sutherland maintained that criminal behaviour is learned through social interactions, and to describe this learning process, Sutherland developed the concept of differential association. The theory suggested nine fundamental principles that explain the processes whereby a person becomes involved in crime. The propositions of the theory are as follows (Brown *et al*. 2001):

i. Criminal behaviour is learned. *It* is learned through the interaction with other people in a process of communication.

ii. The principal part of the learning of criminal behaviour occurs within intimate personal groups.

iii. When criminal behaviour is learned, the learning includes; techniques of committing the crime, which are sometimes very complicated or very simple; the specific direction of motives, drives, rationalisation, and attitudes.

iv. The specific direction of motives and drives is learned from definitions of the legal codes as favourable or unfavourable.

v. A person becomes delinquent because of an excess of definitions favourable to the violation of the law, over definitions unfavourable to violation of the law. Differential associations may vary in frequency, duration, priority, and intensity.

The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all the mechanisms that are involved in any other learning. While criminal behaviour is an expression of general needs and values, it is not explained by those general needs and values, since non-criminal behaviour is an expression of the same needs and values.

According to Brown *et al.* (2001), the principle that criminal behaviour is learned provides the foundation for differential association. This expressly rules out heredity, human nature, and innovation as the causes of aberrant behaviour. This means that people are taught how to

behave, or misbehave in a social context. Most internet fraudsters and cybercriminals operating in Nigeria acquire these skills through social context and interacting with friends and peers. Economic and Financial Crimes Commission (EFCC), of recent, has discovered and raided several institutions (schools) where cybercriminals were undergoing training. This shows that criminal behavious are neither inherited nor inherent in human nature, but are acquired though interacting in a social context. The principles of differential association specify that criminal behaviour is learned primarily in interaction with significant others such as family and friends. In line with this theory, it is quite apparent that cybercriminals are not illiterate nor novice, but perpetrators of cybercrime are well trained in the field of computer sciences and are vested with advance skills on networking and internet connectivity, they spend much time surfing the internet with the sole aim of discovering a new method of criminal behaviour. In the course of doing this, they are acquiring technical knowledge and skills which they use in perpetuating their heinous acts.

Interestingly, learning the techniques of committing crimes are said to be much less important than acquiring a mindset that is conducive to criminal behaviour. While a particular mindset is essential, familiarity with technique relates to the type of crime perpetrated and to succeed in committing the offence without detection. Some crimes, such as internet fraud and scamming, entail the acquisition of complex techniques. To be able to succeed in this criminal behavior, considerable skills are needed and must be mastered to be able to pursue these criminal paths. Learning the motives and drives, which result in a relatively constant desire or persistent urge to do illegal things is, on the other hand, a requisite of criminal behaviour. Similarly, learning rationalisations and attitudes that define criminal behaviour as acceptable, supports criminal behaviour.

Conceptual Explanations

Cybercrime

Cybercrime, like any other social phenomenon, has been subjected to different definitions depending on the background of the scholar. Smith et al (2004) indicated that it is often complicated in getting a unique and consistent definition of cybercrime. This is because different institutions, departments, organisations and agencies have given different definitions in accordance to their situation and place. Scholars from criminology, IT experts, psychology, sociology, police and other security analyst have defined cybercrime as a crime aided by the computer or a crime in which the computer network plays a significant role. Cybercrime is a split word which can be better understood by understanding the split meaning of cyber and crime. The word “cyber” comes as a prefix that denotes a relationship with information technology, computers or computer network and “rrime” is defined as a deliberate act which is considered as an offence and punishable by law. They are deliberate and illegal act committed by a person or group of persons using computer as a tool or target to carry out their heinous aim.

Cybercriminals use computer either as a target or as a tool to perfect their ambition. Alkaabi and Obaid (2010) opined that traditionally, the term cybercrime referred to crimes over networks, especially the internet but the term has increasingly become a general term or replacement for computer crime. Perpetrators of cybercrime see computer network as a safe haven for executing their heinous agenda by robbing victims of their hard earned resources. Cybercrime can also be seen as an unlawful act perpetuated using the computer either as a tool, target or both. In essence, this definition is simple and precise. It sees cybercrimes as crimes committed using computers or against computers. Ekemezie and Ngene (2004) assert that computer crimes are illegal act committed against computers or telecommunications or the use of computer or telecommunication to accomplish an illegal act. From the foregoing, it is obvious that cybercrime has to do with any activity conducted in the cyberspace intent on defrauding individual and organizations and/or putting computers out of effective order.

Cybercrimes are crimes/evils that arise as a result of growing dependence on computers.

Diaspora

The concept "diaspora" comes from the ancient Greek word "*dia speiro"* meaning "to-sow-over". It is seen as a large group of people with a similar culture who has since moved out to places all over the world. Safran (1991) opined six basic characteristics in his definition of diaspora. According to him, for something to be called as diaspora there should be a dispersal from homeland to two or more foreign regions; those people who are away from their homeland have a collective memory about their homeland; they have a belief that they will always be outrageous in their host state; they idealize their putative ancestral home; there is a belief that all members of that society should be committed to the maintenance or restoration of the homeland; and a strong ethnic group consciousness with a belief in a common fate. Diaspora can further be seen as a community of people from the same homeland that have been scattered or have migrated to other land.

Cohen (1995), in his assertion, believes that diaspora should also include scattering groups with aggressive or voluntary purposes; a strong tie to the past or a block to assimilate; diasporas should be defined positively rather than negatively; people of diaspora have also a common identity with co-ethnic members in other countries such as colonial settlers, overseas students, refugees, and economic migrants. Citizens of a particular country living in diaspora represent the identity of their home country. Therefore, their actions, attitudinal behavior, and personalities are attributed to their country of origin. Image of a country is truly depicted and often rated by the actions and ways their citizens behave in diaspora.

External Image

In psychology, the external image (also alien image, foreign image, public image, or third-party image) is the image other people have of a person, i.e., a person's external image is the way they are viewed by other people. It contrasts with a person's self-image; how the external image is communicated to a person may affect their self-esteem positively or negatively. Image is the mental picture, idea, impression or the perceptions of a person, organisation, institution or government by others (Kotler, 1997). An external image is the totality of all perceptions, feelings, and judgments that third parties make about an individual. These interpersonal perceptions are automatically linked to earlier experiences with the person being observed, and with the feelings arising from these interactions and evaluations. The image that others have of a person shapes their expectations of this person, and significantly affects their mutual social interaction. A person's external image or more precisely, how this image is communicated to the individual, and how others react to the individual as a result of his or her external image, significantly affects the person's self image. Positive, appreciative external images strengthen an individual's self-confidence and self esteem. In extreme cases, negative or conflicting external images can cause mental illness.

Anton (2011), cited in Sulaiman et'al (2016), described external image as the entirety of all perceptions, feelings, and judgments that people make about others. It is how we perceived others. This perception springs from earlier experiences or contacts with the person or organization and the outcome of this contacts and evaluation. The way we perceive and judge people modifies our interaction with them. The external image of a nation can be viewed as a way in which other countries of the world perceive citizens of a particular. Behaviours of citizens of a particular country can create a good or bad image for their home country. No nation is an island; every nation depends on others for survival. In the quest to meet the needs of its citizens, nations of the world have involved in international treaties and conventions aimed at building trust and reputation among nations of the world. However, these reputations can be tarnished as a result of the ways citizens behave and are assessed by other countries. Therefore, a country's image is seen as a mirror which can be viewed and examined. This explains why Ogwu (2005), cited in Sulaiman et al (2016), argued that a nation's

reputation is a critical asset and, therefore, a vital component part of its national power. Image is one of the most valuable assets individuals, organizations and governments would want to protect and nurture. Good reputations and impressions an individual, organization or government has can attract supports and assistance from others, especially in a time of need or emergency.

Forms of Cybercrime

Cybercrime comes in various forms and perpetrators use one or more of the following forms to carry out their heinous activities:

i. **Hacking:** Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. It also involves the use of stolen passwords, codes or security loopholes to forcefully gain access or break into organizations, individuals or government computer to steal or have access to secret information. Simply put, hacking is an attempt to exploit a computer system or a private network inside a computer. In the same vein, hacking is defined as the act of compromising digital device to gain unauthorized access to a computer system or network in other to carry out illegal act to the detriment of the owner. Hackers often have unauthorized access to or control over computer network security systems for some illicit purpose. Hackers write or use readymade computer programs to attack the target computer. Some hackers hack for personal monetary gains by stealing credit or debit card information, transferring money from various bank accounts to their own account (Kejal, 2011).

ii. **Online Scam:** Online scam comes in different categories which include investment fraud, lottery scams, employment scams and charity scams. It is targeted at the general public with the aim of defrauding them of their incomes. Cybercriminals devise various means by soliciting for sensitive information from their victims that might help them secure a lucrative investment, winning lottery and securing a better job opportunity. Fraudsters usually create authentic looking websites or blog. The purpose of these websites is to make the user enter their personal information. The information is then used to have access to their business and bank account. Most cybercriminals use potential job seekers as their target. The fraudsters will post a fake job listing, often promising high salaries and flexible working conditions, to lure in potential victims. They will then ask for personal information or payment upfront for various reasons in order to offer them a non-existing job opportunity in multi-national corporations.

iii. **Spamming:** Spamming is the process of sending irrelevant or unsolicited messages to a large number of internet users, for illegitimate advertising, and other activities such as phishing, and spreading malware. Spamming is used for sending fraud mail, phishing campaigns, identity theft, and for sending malicious executable file attachments, links to malicious websites and phishing websites for illegitimate activities. Through such process, both the network operators and unsuspecting users are dangerously exposed to the technological tricks of the spammers. E-mail spamming is becoming a serious issues amongst businesses due to the overhead costs it causes, not only in regards to bandwidth consumption but also to the amount of time spent in downloading or eliminating spam mails (Alhaji et'al, 2016).

iv. **Identity Theft:** Identity theft occurs when criminals use a victim's personal information to commit criminal acts. Identity theft is also known as called phishing. It involves stealing personal information from unsuspecting users and also an act of fraud against the authentic, unauthorized businesses and financial institutions. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name. Daniel (2015) explained that there are diverse forms of systems which are used by identity fraud offenders to defraud victims. Cyber criminals commit identity theft by using sophisticated cyber-attack tactics, including social engineering and malware. Identity theft can also result from rudimentary tactics with criminals stealing mail, digging through

dumpsters, and listening to phone conversations in public places.

v. **Piracy**: Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs (Longe, 2004). Piracy is one of the most prevalent cybercrimes committed by most internet users. Pirates may obtain from online source an original version of a software, movie or game and make copies of them. They may sell these products directly to potential buyers or upload it on their internet page for people to download without the knowledge of the manufacturer. Software piracy is the illegal copying, installation, use, distribution, or sale of software in any way other than what is expressed in the license agreement. The software industry is facing huge financial losses due to the piracy of software. Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available. Similarly, freeware, a type of software that is copyrighted but freely distributed at no charge, also offers little incentive for piracy.

vi. **Malware**: Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network; leak private information; gain unauthorized access to information or systems; and deprive access to information, which unknowingly interferes with the user's computer security and privacy. Simply put, malware is malicious software designed to interfere with a computer's normal functioning. Malware is designed to evade antivirus software detection algorithms. Malware can also be installed on a computer "manually" by the attackers themselves, either by gaining physical access to the computer or using privilege escalation to gain remote administrator access. More specifically, malware is categorically used to attack government or company websites to collect protected information to interrupt their process and procedures to their advantage. Malware after installation can be launched to disrupt the smooth functioning of a computer system, thereby paving way for cybercriminals to gain direct access to personal details such as personal identification numbers, bank details, debit card pin, and security passwords of the user.

vii **Dating/Romance Scams:** Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out romance scams are experts at what they do and will seem genuine, caring, and believable. Great Britain has the highest victims of romance scam. A research in 2012 showed that more than 230,000 people may have fallen victims of romance fraudsters in Great Britain alone (Whitty & Buchanan, 2012). The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money. Dating or romance scam entails posing as a potential date or love partner on the internet in order to connect with someone. A fake picture of someone exceptionally attractive is frequently used to lure people to respond to love propositions. To lure someone into a scam, a fake profile is built with false information. Emails and other messages are exchanged once someone responds or appears receptive to a romantic relationship. Over time, trust is earned. Following the establishment of confidence based on false pretenses, solicitations for money or other items begin. Asking someone to donate money or presents is a form of dating fraud. Scammers may seek to lure victims overseas, placing them in potentially perilous situations with terrible effects.

Causes of Cybercrime

Ninalowo (2016) opined that cybercrime is caused by many factor and the culprits are warmly welcome and received by certain individuals and social institutions after making money through this unapproved means. Below are some of the reasons people indulge in cybercrimes:

a) Attitude of Getting-Rich-Quick

Humans are free beings capable of making any choice without any form of encumbrances. However, some people, out of greediness and lack of contentment, choose to cut through the illegal ways of making money. Shehu (2014) revealed that most people especially the poor want to bridge the wider gap of poverty through cybercrime. They are very keen and determine to make money by whatever means available within the shortest period of time which often pushes them to cybercrime. Meke (2012) indicated that people who are poor are more engaged in cybercrime than the rich people. Thus, poverty is a propeller of criminal behavior; many poor people engage in criminal activities in order to overcome poverty and also compete with the rich people.

b) Growth in *E-commerce* and *E-businesses*

With the advent of internet and internet connectivity, electronic commerce and electronic marketing become prevalent phenomena that boost easy exchange of goods and services. The growth of E-commerce and internet banking has a replica effect on the development of cybercrime. Most financial institutions have embraced the innovation offered by ICT especially in their day-to-day transactions and meeting their clients' needs. These initiatives come with some level of risk which gave birth to online scams, ATM skimming and identity theft.

c) Weak Cybercrime Laws/ Legislation

Crime rate is apparently on the increase in any country with weak legislation. Cybercriminals are more rampant and prosper in a clime with weak and ineffective legislation. Okeshola and Adeta (2013) believed that the menace of cybercrime prevail more on places where there are not strict and stringent laws to deal precisely with cybercriminals. The perpetrators of cybercrime mostly go unpunished in countries with weak laws and others are driven into committing the same since there is no law prohibiting the practices of cybercrime. Ani (2011) concluded that weak laws inspire people to ignore the consequential effects of committing virtual crime. Unavailable legislation and extant laws to prosecute the offenders of cybercrime have propelled some youths to indulge in various cybercrimes without considering the implications of their actions.

d) Unemployment/Poverty

The increased rate of unemployment in Nigeria is apparently one of the factors responsible for cybercrime in the country, as most unemployed graduates of higher learning see cybercrime as a lucrative business to meet ends need. Most graduates of higher institutions who spent many years in the university and remained unemployed are more prone to committing cybercrime, especially those studying computer sciences and other internet-related courses. High rate of youth unemployment can easily influence the youth to engage in crimes such as stealing, robbery, and cybercrime (Okeshola & Adeta, 2013; Warner, 2011). It is also a known fact that poverty seems to have a symbiotic relationship with crime. It could be because of their poor background, they could not stand firm to protect their integrity (Atairet, 2023). Some youths resort to cybercrime as a means of livelihood and survival in poor economic conditions they found themselves.

e) Lack of Parental Control

Poor parental control contributes to increased cases of cybercrime. Evidence from Adejoh et al (2019) disclosed that some parents indirectly support their children by ignoring interrogate their means of sustenance. Most children are shielded by their parents and are not questioned about their source of wealth. Some parents seem to be in support of their children when they notice they are cybercriminals. Some parents may not have any idea about their children sources of wealth, but those who know may lack the courage to report their children to the security agencies. Kanayo, (2024) urged parents to inculcate the habit of questioning their kids on where and how they get things, stating that lackadaisical attitude was breeding more corrupt mindset in their children. He further stated that parents should be mindful of accepting expensive gifts from their kids, especially when they are not actively doing anything substantial.

f) Accessibility to Internet and Technology

Easy and cheap access to internet service and the benefits which come forthwith contribute to increased cases of cybercrimes. The introduction of modern internet facilities and electronic gadget tends to be an easy step for one to indulge in cybercrime. Easy access to internet broadband services coupled with availability of personal computers and other hand held mobile gadget offer people the opportunity to commit various types of online crimes (Adejoh *et al.,* 2019). People tend to spend much of their time surfing the internet and chatting on various social media like Facebook, Whatapps, Twitter and Instagram, among others, especially with the availability of cheap data services from the Internet Service Providers. The frequent access to these internet resources has lured many into committing various cybercrimes like love/romance scam, spamming and identity theft.

g) Peer Pressure

Peer group pressure plays a pivotal role in criminal behaviour of individuals. Confirmation from Adejoh *et al.* (2019) and Obiri (2015) revealed that youths who are involved in this scamming business are students. There is high rate of cybercrime among students most of which are students of higher institutions. The perceived influence by friends and relations lured many into committing various cybercrime, as they want to live a flamboyant and luxurious lifestyle like their colleagues in and off campus. These groups of gullible and desperate youths might have seen their colleague displaying their wealth, driving exotic cars, building mansions and living a flamboyant and expensive lifestyle, and they will want to emulate same without knowing the source of their wealth and will end up becoming a cybercriminal.

h) Fame, Influence and Societal Recognition

Self-actualization and recognition are among the theories of needs as opined by Abraham Maslow. Every individual would want to stand out and be respected by members of the society. Thus, in a bit to gain these fame and influence, many people indulge in cybercrimes which they see as a fastest means of making money and displaying their egoistic personality. Hassan *et al* (2012) identified fame as one of the causes of cybercrime. It is apparent that some societies put much recognition and weight on people with money and properties and these people are held in high esteem as men that matter. Wealthy people are celebrated and given special recognitions at events and occasions. These recognitions and respect are what drive many young people to see cybercrime as the most lucrative business of making much money within a shortest period of time in order to be recognized and respected in the society.

An Overview of Some Cases of Cybercrime in Nigeria

Nigerians' involvements in internet fraud have become a topic of discussion over the years and have occasionally made headlines in the national and international dailies. Government agencies like the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and other Related Offences Commission (ICPC) and other agencies responsible have made it a point of duty to apprehend, investigate, prosecute and convict perpetrators of cybercrimes in the country. Iroanusi (2022) opined that Nigeria's anti-graft agency, EFCC, in 2021 had announced that it has convicted total number of 2,220 persons while in the year 2022; the anti-graft agency had convicted 2,847 persons guilty of cybercrime. The convicted persons are mostly Nigerian youths who have engaged in various criminal activities associated with cyberspace. The most famous case of cybercrime is the involvement of a prominent Nigerian named Ramoni Igbadole Abbas, widely known as Hushpuppi.

The arrest of Hushpuppi; Jacob Ponle, known as Woodberry; and ten other Nigeria by the experts of the FBI, INTERPOL, and the Dubai police in the United Arab Emirates has reopened the unpleasant conversation about international cybercrimes. According to Olowolagba (2020), Hushpuppi was arrested in Dubai for allegedly hacking into the United States (US) unemployed database and defrauding the US of over $100

million meant for native Americans in the battle against coronavirus. In the same vein, Erezi (2020) pointed out that the Nigerian social media influencer Hushpuppi conspired to launder hundreds of millions of dollars from Business Email Compromise (BEC) fraud and other scams, including schemes targeting a U.S. law firm, a foreign bank and unnamed English Premier League soccer club. It was further noted by Erezi that Hushpuppi laundered hundreds of million dollars from other fraudulent schemes and computer intrusions, including one scheme to steal €100 million (approximately $124 million) from an English Premier League soccer club.

Bukola et al (2023) observed that Nigerian banking customers have lost whooping N51 billion savings to fraud, even as cybercriminals are now targeting Fintech bank customers to defraud them. Between 2019 and July 2023, banking customers lost N50.5 billion to banking-related fraud. With over N9 billion lost to fraud in the banking system as of July 2023, there were indications that the figure could rise further as cybercriminals are intensifying their effort to defraud customers of Fintech banks across the country. A report by Financial Institutions Training Centre revealed that Nigerian banks customers lost a total of N2.72bn to fraud in the first and second quarters of 2022. Between July and September 2020, banks according to Nigeria Inter-bank Settlement System PLC, lost N3.5bn to fraud related incidents, representing a 534 percent increase from the same period in 2019 when it was N552m. In 2018, commercial banks in Nigeria lost a cumulative N15bn to electronic fraud and cybercrime. This was a 537 percent increase on the N2.37bn loss recorded in 2017. In the same period in 2018, over 25,043 bank customers and depositors lost N1.9bn to cyber fraud, with fraud incidents rising by 55 percent from the previous years. In September 2022, suspected fraudsters during a three-day cyber-attack hacked a customer's account domiciled in an old-generation bank and transferred N523.337 million from the account to 18 different accounts in the same bank (George, 2023).

In another development, George (2023) observed that some hackers have intruded into Babcock University website; a private Christian University owned and operated by the Seventh-Day Adventist Church. He noted that hackers have broken the site's firewall and take full control of the website and even posted pornographic materials. The hackers requested visitors to the website to click on a link to chat live with pornstars. Some tech experts believe that it must have been a ransomware attack, where a hacker or group of hackers, take over a site and the real owners are required to pay a ransom to retrieve the site. It was further revealed that in 2015, the Federal University of Technology, Owerri, Imo State's website was hacked by a syndicate identified as the Nigerian Cyber Army, known for its illicit acts of breaching cyber security. Interestingly, government agencies were not left out of these detestable acts of cybercrime. George (2023) further noted that barely months after the National Population Commission opened up its portal for recruitment and other needs, and weeks before a national census scheduled to hold, hackers invaded the NPC servers. This was aimed at frustrating the effort of government at obtaining accurate figures for economic planning and other related matters.

Independent National Electoral Commission (INEC) also recorded same fate when its site was invaded by hackers in the just concluded 2023 general election. The Federal Government's Information Technology revealed that it has successfully blocked over 200 cyber-attacks during the presidential and National Assembly elections on February 25. More so, the former Minister of Communication and Digital Economy Prof. Isa Pantami revealed that a total of 12,988,978 cyber-attacks originating from both within and outside Nigeria were recorded in the country. This attack came just a few weeks after more than 12.9 million internet-based criminal attacks were launched on Nigeria during the presidential and National Assembly election (Adaramora, 2023).

Cybercrimes committed by Nigerian nationals portray a certain get-rich-quick syndrome which has become a deified, noticeable trend mostly exhibited to varying degrees across social media platforms. Exotic cars are flaunted, designer

wears rocked, glittering accessories are customary looks across verified pages and profiles, as if to separate those that have "made it" from those trying to stay as legitimate and clean in their professions. That these self-acclaimed "made men" have millions of followers on their social media accounts portrays the alternate universe we live in, where the disenfranchised see them as role models to aspire to become. Yet, there is a profound truth to be gleaned from this aforementioned syndrome. Cybercrime is spreading at a fast pace, with new trends constantly emerging. The enforcement actions led by Nigeria and coordinated by INTERPOL send a clear message that cybercrime will have serious repercussions for those involved in it, particularly in Nigeria.

Implications of Cybercrime on Nigeria's Image in Diaspora

The question of Nigeria's image in diaspora has generated discourse and debates in international arena. The country, over the years, has been battling to save her long nurtured image and reputation in the international arena that has been ruined by few of her citizens who engaged in various cybercrimes. Although the introduction of ICT in Nigeria was aimed at bringing digital transformation to the country, it is believed that every development has its positive and negative effects. ICT penetration in Nigeria has been embraced with open arms and has become a source of livelihood to most households, an ease of doing business for companies and private sectors, and also a panacea for efficient and effective public service delivery for government agencies and parastatals. As observed by Atairet (2022), the growth of any organisation directly depends on the quality of service such organisation delivers. However, the proliferation of internet services has come with its adverse effects to various internet users vis-à-vis Nigeria's image in diaspora. In other words,

"the Internet has opened up a new window for the development of a new criminal sector of fraud.

The situation is so bad now that young secondary school leavers, undergraduates and graduates are finding cybercrimes as a catalyst to reach their life aspirations. The varieties of application offered by the internet, such as, electronic mailing, 'chat' systems and Internet messaging (IM), often serve as good grounds for carrying out immoral and other deceitful activities by the criminals (Adeniran, 2008). This has greatly affected the image of the country in the international arena. Eze and Ezedikachi (2021) observed that the image a country portrays in the international system and in relations to foreign states plays a big role in determining its standpoint, recognition and credibility in the international system. The issue of internet fraud is not favorable to a country's image and reputation. It portrays a level of involvement in criminal activities which scares away investors, discouraging local and foreign investment which is not good for the economy. It causes erosion in international and public confidence concerning the country's financial sector. It discourages hard work in academic settings which is understandable, especially as it is assumed that most perpetrators of internet fraud are students of tertiary institutions. An average Nigerian is seen to be a suspected fraudster in a country of their destination. Consequently, they are being ill-treated, deprived of some rights and privileges and, most times, physical assault are being meted to them.

Eze-Michael and Ezedikachi (2021) further observed that the situation of Nigeria's image is in direct comparison with the famous saying that "one bad apple spoils 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. According to Mboho and Udoh (2014), the country known as Nigeria was once known as one of the countries with sound moral diplomatic reputation in the early period of post-colonial era. Cybercrime is seen as an automatic indictment of Nigerians and Nigeria's character, just as the international image of the country lies critically at

the selective mercy of western propaganda. It has equally fostered an unconscious guilt that most Nigerian citizens have to bear across all international institutions as Nigerians. Also, its implications have been even more damaging: mails emanated from most Nigerians are rejected, work or studies are denied with reckless abandon, and Nigeria's green international passports are treated with utter disdain. An average Nigerian is judged based on the country's perceived unscrupulousness than on the merits of an individual character.

Interestingly, Chinedu (2021) asserts that Nigeria was ranked 16th among the countries most affected by internet crime in the world in 2020. According to Chinedu, the U.S Federal Bureau of Investigation (FBI) said victims of such scams globally lost $4.2 billion in 2020, compared to $3.5 billion lost in 2019. The top five crimes reported include phishing, non-payment/non-delivery, extortion, personal data breach, and identity theft. To most international community, the sight of a typical Nigerian would give a wrong perception of a criminal presence. Most Nigerians are perceived as drug pushers or fraudsters who cannot be trusted in anyway. This misconception has spelt doom to innocent Nigerians in diaspora who are doing their legitimate business, as most of them are denied the rights given to other nationals and treated unfairly when compared to other nationals. Cybercrime gives bad image to countries that are mostly engaged in it. Widespread fraud is spreading like wild fire from Nigeria throughout the world as unscrupulous Nigerians at home and abroad further tarnish their country's growing international reputation as a place where crime and corruption flourish unchecked.

The activities of cyber criminals have adversely tarnished the image of Nigeria in international arena and made the country to loss her integrity. Issues of cybercrime have discouraged potential foreign and local investors who seek to transfer their resources and wealth of experience for the development of the country. The continuous involvement of Nigerians in cybercrime has led to a situation in which many genuine businessmen and contractors have lost many business opportunities and have become less worthy in the business community the world over, (Nlerum and Okorie, 2012). The fear and lack of confidence that cyber criminals have created in the minds of foreign investors towards Nigeria and Nigerians coupled with corruption and lack of social amenities, explain the gross lack of employment in Nigeria because while old industries are closing down, new ones are not springing up as investors kept their distance from the country (Jakarta Post, 2003).

Abah (2000) posits that the inhumane treatment meted to Nigerians living in the diaspora is unquantifiable in terms of battered image, mistaken identity, victimization, stereotyping and unavoidable circumstantial police brutality sometimes leading to death. Most genuine Nigerian citizens in diaspora have been subjected to unfair treatment, injustice and abuse of their rights. The activities of few miscreants who are characterized with negative social values and attitudes have painted a bad image on the country, (Mboho and Effiong (2024). Though most Nigerians choose countries like United Kingdom, United States of America, Turkey and few others as their second home, their welfare and safety cannot be guaranteed as they are noted and nicknamed fraudsters and scammers who cannot be trusted in whatever businesses they engage in.

Fidrus (2004) notes that some Nigerians have been imprisoned unjustifiably due to stereotyping, which presumably had caused judges to sometimes overlook genuine claims of innocence and meted out unjust punishments to some of these innocent Nigerians. It has also led to situation in which some Nigerians who happened to be at the wrong place at the wrong time were lumped together with criminals with the consequences that they are made to pay for the crimes of their fellow countrymen, especially if the main culprit was able to escape at the time of his/her arrest. With the activities of these internet scammers, life has been uncomfortable to most Nigerians as they are constantly subjected into serious security scrutiny and unnecessary harassment by security units even at first arrival at the country of their destinations.

Conclusion

The evolution of internet and the spread of computer network have brought tremendous change and innovation in every segment of the society. Though the presence of internet was aimed at providing the users with basic internet tools for business, education, banking, research and development and also in agriculture, the benefits have been usurped by miscreants who take advantage of porous computer network to perpetuate different forms of criminal behaviours. The implications of this criminal act, which is primarily known as cybercrime, are not limited to the victims of the crime but the impacts are felt nationally and internationally. Obviously, cybercrimes are mostly perpetuated by youths; especially unemployed young school leavers, i. due largely to greed, get-rich syndrome, peer group pressure and societal influence, among others. The implications of this nefarious crime have direct consequences to both national development and international diplomacy. II. Cybercrime is a threat to the nation's economy and national development. Cybercrime, unlike other crimes, has an international outlook, as nations with high records of cybercrimes iii. are often susceptible and stigmatized and their citizens are subjected to rigorous investigation and inhumane treatment when they find themselves in other countries.

Over the years Nigeria has recorded some IV. cases of cybercrimes, most of which are committed at the international arena. Some of the high profile cases of cybercrime have blatantly tarnished the image of Nigeria v. and brought bad reputation and embarrassment to the nation. Thus, Nigeria's integrity is being dragged to the mud. Despite various efforts by different security apparatus like the EFCC and ICPC in collaboration with the INTERPOL to mitigate and probe perpetrators of cybercrime, Nigerians living in diapora have continued to tarnish the country's image by engaging in these nefarious acts of cybercrimes even with the imminent precipice of embarrassment it has brought to other good Nigerians living abroad.

Recommendations

The following recommendations are proffered to stem the tide of cybercrime by Nigerians and its effects on the country's image in the international space:

Adequate cyber securities should be put in place by government authority responsible for cyber technology. This is to reduce the spread of cyber criminalities in the cyberspace.

Government security apparatus like the anti-graft agencies in Nigeria and in Diasporas should be on red alert to checkmate and arrest perpetrators of cybercrime.

Employment opportunities should be provided for the teaming youths; especially graduates of various higher institutions, as higher percentage of cybercriminals are unemployed graduates.

Legal framework should be strengthened in order to foster quick justice system and the conviction of internet fraudsters.

Proper education and awareness should be made on the danger of cybercrime and its negative implications on Nigerian's image abroad.

References

Abah, P. (2000). Nigeria: Family wants N300m from Indonesia Govt. P. M. News. Academic community. JAAS XXXII, 1-2. Brill, Leiden.

Adaramola, Z. (2023, December 28). *How Cyber-attacks exposed Nigeria's IT Security Vulnerability In 2023. Daily Trust.* http://dailytrust.com

Adejoh, S., Alabi, T., Adisa, W., & Emezie, M. (2019). Yahoo boys phenomenon in Lagos metropolis: A qualitative investigation. *International Journal of Cyber Criminology, 13*(1), 1–20.

Adeniran, I. (2008). The Internet and Emergence of Yahoo-Boys Sub-Culture in Nigeria. *International Journal of Cyber Criminology 2*(2), 368–381.

Alhaji, B., Hassan, A.,& Mohammed, J.(2016). Information and communication technology, cybercrime and the administration of criminal justice system in Nigeria. In Yusuf, Y.M. (ed.) *Current themes on Nigerian law and practice.* Maiduguri: University of Maiduguri, Chapter 25, pages 416-431.

Alkaabi, A., & Obaid, S. (2010). *Combating computer crime: an international perspective*, (Doctoral Thesis on Information Security Institute, Faculty of Science and Technology, Queensland University of Technology).

Ani, L. (2011). Cybercrime and national security: the role of the penal and procedural law. *Law and Security in Nigeria*, 200-202.

Atairet, A. C. & Ndaeyo, E., (2022) Grievances Redress Procedure and Job Retention in Nigerian Civil Service – An Appraisal. *AKSU Journal of Administration and Corporate Governance* 2(3)

Atairet, A.C (2020) Implementation of Local Economic Empowerment Strategy (LEEDS) in the health and Education Sectors. Akwa Ibom state, Nigeria- An Assessment. *International Journal of Technical Research & Science*. Vol. X

Atairet, A.C (2023). An Assessment of the Administrative Ethics Sustainable Service Delivery in Akwa Ibom State Civil Service, Nigeria. http://www.researchgate.net/publication/378691769

Brown S., Esbensen F.,& Geis, G.(2001). Criminology: *Explaining crime and its context 4th edition*: Cincinnati, OH, Anderson publishing Co.

Bukola A., Ibeh R., & Sivowaku B. (2023, November 27). *Fintech: Nigerian Lose N51bn to Cybercriminals.* Leadership News online. http://www.leadershipnews.com/fintech/

Chinedu A. (2019, March 18). *Nigeria ranked 16th in FBI global cybercrime victims report*. The Cable. www.thecable.ng

Cohen, R. (1995). Rethinking 'Babylon': *Iconoclastic Conceptions of the Diasporic Experience*. New Community, 15.

Daniel, E. (2015). *Cybercrime in Ghana A Study of Offenders, Victims and the Law.* Doctoral dissertation, University of Ghana.

Dennis, M. (2014). Cybercrime. In Encyclopaedia Britannica. Retrieved from http://www.britannica.com/EBchecked/topic/130595/cybercrime.

Ekemezie, W., & Ngene, N. (2004). *Computer and Information Technology.* Enugu: Kinsman

Erezi, D. (2020, July 3). *Hushpuppi conspired to defraud Premier League Club of $124 million.* The Guardian News. http://www.theguardiannew.com

Ezeani, C. (2010). Information Communication Technology: An Overview. In Evarest C. Madu and Chinwe Nwogo Ezeani (Eds.) Modern Library and Information Science for Information Professionals in Africa.

Eze-Michael & Ezedikachi. N. (2021). Internet Fraud and its Effect on Nigeria's Image In International Relations. *Covenant Journal of Business & Social Sciences (CJBSS),* Vol. 12 No.1, June, 2021

Fidrus, M., (2004). Judicial review for Nigerian on death row begins. Jakarta Post.

George, G. (2023, April 2). *Bank customers, companies lose billions to Nigeria's weak cybersecurity.* Punch Newspaper. http://punching.com

Hassan, A., Lass, F., & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), 626-631.

Ige, O. (2008). Secondary school students' perceptions of incidences of Internet crimes among school age children in Oyo and Ondo States, Nigeria. *A Master dissertation in the Department of Teacher Education, University of Ibadan*.

Iroanusi Q. (2022, October 27). *Over 2,800 persons convicted of cybercrime in 2022*. Premium Times Online News. https://www.premiumtimes.com/news

Jakarta Post, (2003). On advance fee fraud. The displacement of the Nigerian. Jumare, I.M., 2001

Kanayo, K. (2024, February 7). *Question source of your children's wealth.* Daily Post Newspaper. dailypost.ng/2024/02/07/question-source-of-your-childrens-wealth-kanyo-o-kanayo-warns-parents.

Kejal V. (2011) Cybercrime & its Categories: *Indian Journal of Applied Research. Retrieved from https://www.researchgate.net/publication/274652160*

Kotler, P (1997), *Marketing Management: Analysis. Planning, Implementation and Control,* New Helhi: Prentice Hall Inc.,

Longe, O.(2004): Proprietary Software Protection and Copyright issues in contemporary Information Technology. (M.Sc. Thesis) Unpublished. Federal University of Technology, Akure, Nigeria.

Mboho, K.S. and Udoh, U.S. (2014). Resource control: A panacea a for sustainable peace and development in the Niger Delta Region of Nigeria. *IOSR journals – international organization of scientific research, Journal of Business and Management, Vo. l16,* pp. 33-38.

Mboho, K., and Effiong, U. (2024). Social Values, Negative Attitudes and Conducts in Nigeria. In: I.V.O. Modo and Kingdom Sunday Mboho (Eds). *The Perspective of Nigerian Peoples and Culture*. ICIDR Publishing House, Ikot Ekpene.

Meke, E. (2012). Urbanization and Cyber Crime in Nigeria: Causes and Consequences. *European Journal of Computer Science and Information Technology*, *3*(9), 1-11.

Ninalowo, A. (2016). *Nexus of state and legitimation crisis*. Lagos: Prime Publications.

Nlerum, F. E.; Okorie, N. U. (2012). Youth participation in rural development: The way forward. *Spanish Journal of Rural Development, 3,(1), p. 1*

Obiri, N. (2015). *An Investigation of Youth in Cybercrime in the Ayawaso East Constituency of Greater Accra* (Doctoral dissertation, University of Ghana).

Okeshola, F., & Abimbola, K. (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.

Olowolagba F. (2020, June 13). *Interpol breaks silence on Hushpuppi arrest, reveals next action.* Daily Post News. http://www.dailypostnews.com

Safran, W. (1991). Diasporas in Modern Societies: Myths of Homeland and Return. *A Journal of Transnational Studies*, 2,3.

Shehu, A. (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research, 3 (7),* pp 169-180.

Smith, R., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Criminal Justice Matters, 58(1), 22-23.

Sulaiman L., Ishowo, L.& Muhammed, A. (2016). Cybercrime and Nigeria's External Image: A Critical Assessment *Africology: The Journal of Pan African Studies*, vol.9, No.6.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, *5*(1), 736.

Whitty, M., & 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.