Trends, Patterns and Consequences of Cybercrime in Nigeria

[1]Akeem Olalekan AYUB & [2]Linus AKOR (PhD)
[1,2]Department of Sociology, Faculty of Management and Social Sciences, Federal University Gusau, Zamfara State
Corresponding Author: linusakor1963@gmail.com / linus.akoryusuf@fugusau.edu.ng

Abstract

Advancement in information and communication technology (ICT) has created room for the emergence of cybercrime. Access to computers, the internet and security vulnerabilities in cyberspace have made the perpetration of cyber-related crimes more pervasive. The advent of mobile phones and other computer devices in Nigeria and the provision of internet services by accredited Global System for Mobile Communication (GSM) providers has endeared the internet to many Nigerians. Unfortunately, several functionalities of web browsers are vulnerable to cyber-attacks, thereby exposing internet users to cybercrime victimization. While several crimes are daily committed through the internet, many Africans and indeed, Nigerians, are yet to develop adequate technical capacity and knowledge to mitigate cyber criminality. Cybercrimes in Nigeria are executed through identity theft, hacking, phishing, software piracy, etc. This paper examined the trends, patterns and consequences of cybercrime in Nigeria. Relying on secondary data sources, the paper noted that successive Nigerian governments have attempted to combat cybercrime through the promulgation and deployment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. The Nigerian police and the Economic and Financial Crimes Commission (EFCC) have waged continuous war against cybercriminals by arresting and prosecuting many suspects. However, despite government's efforts, consistent tactic updates and changes in strategies have frustrated the apprehension of many cybercriminals. The paper recommends constant training and retraining of law enforcement agents to tackle the menace. Internet users should secure their computer system by enabling firewalls, guarding against revealing personal details, and ignoring emails requesting them to verify their information or confirm username ID or password.

Keywords: Computer; Cybercrime; Cybercriminal, Cyberspace; Internet

Introduction

The development of the internet and seamless access to computer-aided technology have created different opportunities for work and business activities, as well as for those who take advantage of the internet revolution to engage in illegal activities. The onset of information communication technology and online communication has also produced a dramatic surge in the incidence as well as the emergence of new trends and patterns of internet-enabled criminal activities. Longe et al. (2008)

claimed that advancements in technology and the internet have radically changed the reproduction, distribution, control, and dissemination of information, while Arora (2016) noted that the transmission speed of computer networks has made it easy to cheaply and instantaneously send information across the world within a twinkle of an eye. In 2017, 3.8 billion people used the Internet, accounting for 51% of the world's 7 billion people, up from 2 billion in 2015. According to Cybersecurity Ventures, by 2022, there will be 6 billion Internet users, or 75% of the estimated worldwide population of 8 billion, and by 2030, there will be more than 7.5 billion Internet users, or 90% of the expected global population of 8.5 billion (Morgan, 2017).

Cybercrime is any criminal activity conducted with the aid of a computer either as a target or a means for executing certain crimes. The crime involves computer manipulation, sabotage, espionage and the illicit use of a computer device. Morgan (2017) reported that cybercrime remains a threat to every firm in the world and constitutes a serious problem to humanity. Cyber-attacks have significant global consequences. Cybercrime, for example, was said to have cost the global community $6 trillion per year by 2021, up from $3 trillion in 2015, signifying the largest transfer of economic wealth in history and more profitable than the worldwide trade in all major illegal narcotics combined, according to Cybersecurity Ventures. In their analysis titled "2017 Crime Report," Cybersecurity Ventures, the world's premier researcher and publisher covering the global cyber market, recognized cyber-attacks as the fastest rising crime in the United States, adding that their scale, sophistication, and cost are all increasing. According to Opaluwa (2016), cybercrime in Nigeria cost the country $9.3 billion.

Cyber-attacks have led to the breaching of the privacy of many computer users, including their photos, login credentials or medical histories (Choo, 2007). Such attacks have been carried out against persons by tricking them to download malicious files and programs (Systematic, 2016). Cyber-attackers use various means to access people’s computers or organizations’ networks without authorisation. Attacks can be active, such as a brute-force attack that determines a user’s password, or passive, such as a web-based attack that waits for a user to visit a malicious webpage in an attempt to infect the user’s computer with malicious code. Motivations for such attacks range from gaining financial profit, stealing sensitive information, disabling a network, establishing a command and control (C&C) server, or using the system as a launching point for future attacks (Cruz, 2013; Global Forum on Cyber Expertise (GFCE), 2020; Harvy, 2017).

The success of cyber-attacks is dependent upon the poor security habits of the public which is capable of exposing their personal and sensitive data. Strong passwords are not enough to prevent cybercrime due to website vulnerability to a breach of data. More worrisome are the attacks in 2015 in which sophisticated social engineering was used to bypass the two-factor authentication systems designed to safeguard users (Symantec, 2016). One fraudster, however, was able to acquire access to email accounts without raising the suspicions of the victims by going through a legal password-reset process and acting as Google through SMS.

Arising from the foregoing, this paper examined the trends, patterns and consequences of cybercrime in Nigeria. To put the discussion in proper perspective, the paper is divided into several parts. After this introduction, part two reviews relevant literature on the subject of cybercrime, while part three deals with the methodology and theoretical framework .The forth part is the discussion section which interrogates the causes of cybercrime, consequences of cybercrime and attempts by the Nigerian government to mitigate cybercrime. The fifth section brings the paper to a close by way of conclusion and recommendations.

Literature

Trends and Patterns of Cybercrime

There are many types of cybercrime. To that extent, it is very difficult to isolate all types of cybercrime because every day, new and more sophisticated trends arise. One particular pattern can associate with other patterns. For instance, hacking a system is related to identity theft or cyber terrorism. Ribadu (2007) averred that website cloning, internet purchases, false representations, and electronic businesses are the commonest forms of cybercrime in Nigeria, while Olugbodi (2010), identified identity theft, financial fraud (alias Yahoo-Yahoo), credit card theft, fraudulent electronic mails, website cloning, cyber harassment, cyber laundering and malicious attacks through viruses, worms and Trojans as other examples. Some of the typologies of cybercrime are examined below:

Hacking

This pattern of cybercrime is the unauthorized access to computer systems or networks by highly skilled computer programmers or hackers. The process involves testing and exploring computer systems or the practice of accessing and altering other people’s computers without their knowledge (Denning, 2001). The exploration of other people’s computer systems by hackers is performed either out of curiosity or competition with their peers. Whenever these hackers successfully launch an attack, they are seen as experts, become more respected among their fellow hackers, their reputation grows and they gain more powers even with no formal education. Hacking may be carried out with honest intentions when trying to steal information to stabilise a country or with criminal intent to defraud unsuspecting individuals (Urbas & Choo, 2008). People's electronic information, stored in removable storage media, computer hard disks, etc. cannot easily be stolen or hacked without computers and communication systems. It could be either physically appropriating the data or meddling with them via the virtual media (Rughani, 2011).

Aransiola and Asindemade (2011) revealed that hackers exploit the weaknesses and loopholes in operating systems to destroy data and steal important information from a victim's computer through the installation of several backdoor programs (password hacking software) on the victim's machine that enables the hackers to gain constant access to resources including credit card information. Hackers can also monitor what people do on their computers and can also import files from them. Where hackers target the stealing of passwords, it is called password sniffing and is done through the installation of programs that monitor all traffic on areas of a network used by a particular system they intend to penetrate. The first 128 bytes or more are collected by password sniffers on each network connection of the network under monitoring (Thomas & Loader, 2000). Accordingly, the sniffer collects the password information when the user name and password are typed as required while using certain common Internet services like file transfer protocol (FTP) or Telnet.

The activities of hackers are not only restricted to sniffing passwords and usernames but also include cracking into bank systems for the transfer of money to the bank accounts that belong to them. Their ability to successfully hack into bank systems, enables them to illegally transfer large amounts of money and this is a thing of serious concern for the banking sector. Most of the companies and banks do not disclose that they have always been victims of hacking because of the fear of losing customers and shareholders. Urbas and Choo (2008) observed that hacking in the form of cyber-theft is the most common and the most reported of all cybercrimes because it quickly results in loss of large cash to the victims and profit to the hackers. The secret information of a company, especially on its modus operandi and plans, that are important, can also be hacked.

In Nigeria, hacking is not a new phenomenon. The Independent National Electoral Commission (INEC) reported that its website was hacked during the 2015 general elections and attempts were made to access information critical to several government parastatals (Muhumuza & Olukoya, 2019). This implies that the election infrastructure of Nigeria remains vulnerable to cyber-attacks even though effort has been made to prevent future occurrences. Globally, national elections have been disrupted by hackers through direct hacking of officials' databases and the engineering of fake news (GFCE, 2020). Cases abound where online voting systems are breached and manipulated for desired results by a particular political party. Take, for instance, some Nigerian politicians have been alleged for trying to hack the INEC server to manipulate election results. According to Muhumuza and Olukoya (2019), the likes of former Senator Dino Melaye; former Speaker of House of Representatives, Yakubu Dogara; erstwhile Senate President, Bukola Saraki; and former presidential candidate, Atiku Abubakar, were once alleged to have hired Hushpuppi to hack into INEC server to manipulate the result. However, the allegation was dispelled and described as irresponsible and cheap politics.

Software piracy and Cyber-plagiarism

Piracy, which is also called intellectual property theft involves the illegal reproduction and distribution of software applications, games, movies and audio CDs (Longe et al., 2008). The term "Copyright" means little or nothing to the average Nigerian. Omodunbi, Odiase, Olaniyan and Esan (2016) observed that a lot of money is made from piracy including the provision of pirated software's cracks. Generally, privateers (pirates) purchase from the Web an original product, film or game and illicitly make duplicates of the product accessible online for others to download and use without the notice of the patent owner. This is known as Warez or Internet theft. In Nigeria, the use of the internet has practically made the distribution of pilfered materials possible and contributed to financial misfortunes on the part of the victims. This type of cyber-attack may be the most difficult to combat because it appears to help the average person as well (Fafinski, 2008). The benefits are derived by the common man through the illegal and cheap purchase of cracked software, games, films, among others, that would have been impossible or difficult to be purchased through standard and legal means. For instance, getting a licensed plagiarism software such as Turnitin is very costly to be purchased by individuals but there are lots of cracked plagiarism checkers' software on the internet that can be accessed without payment.

Omodunbi et al. (2016) described cyber-plagiarism as the copying and pasting of online information into any document format without acknowledging the original writer or owner. 'Copy and Paste' remains the popular phrase for referring to cyber-plagiarism or information copied without due acknowledgement of the original source. In Nigeria, cyber plagiarism is reportedly perpetrated in educational institutions by students and lecturers through self-alteration, appropriation and adoption of information found on the internet (Arora, 2016). Oftentimes, students of higher institutions engage in this act without sanctions from regulatory agencies to deter further occurrence.

Spamming

Spamming is the indiscriminate sending of unsolicited bulk messages to large lists of email addresses through electronic messaging systems for the promotion and advertisement of products and websites (Denning, 2001). This is sometimes referred to as email bombing because large numbers of emails are usually sent to potential victims (an individual, a company or mail servers), which sometimes result in system crashing (Graycer, 2020). E-mail spam is a form of spam widely recognized and applied to media abuses such as Usenet newsgroup spam, wiki spam, instant spam in blogs, messaging spam, web search-engine spam, mobile phone messaging spam, junk fax transmissions, Internet forum spam, online classified ads spam, social networking spam, file-sharing network spam and television advertising.

The cost implication of email spamming including high bandwidth consumption, huge time spent downloading or eliminating spam mails, makes it more worrisome amongst businessmen and women (Harvy, 2017). Spammers are formulating progressively propelled strategies to avoid spam filters, for example, change of the substance of the email and the utilization of symbolism that can hardly be identified by these spam filters. An e-mail extractor is used by culprits of spamming to separate all users of a specific domain, though commonly associated with yahoo mails. The consent of the recipient is not the aim of the sender; hence, emails are sent indiscriminately.

Malicious software/malware (Trojans, Viruses, Worms, Logic Bomb, Bot)

Malware refers to software that attackers use to steal confidential information, destroy data, disrupt computer operations, or gain access to the network from the compromised system (Harvy, 2017). Types of malware include viruses, worms, Trojans, spyware, and ransom ware, among others, and they are spread through the use of a variety of tools such as email, drive-by downloads, and infected files (Harvy, 2017). They can also exploit existing vulnerabilities to infect systems. They are malicious programmes that get onto the computer without the knowledge of the users or owners and pose a major threat to the users. Longe et al. (2008) revealed that writers of software find it amusing to write programs that exploit security flaws and see the level of its widespread. Generally, malware software appears to be safe and legitimate, however, when downloaded, it infects and destroys computer systems, especially valuable information. Lewis, Kaufman and Christakisin (2008) identified ‘Rabbit’ and ‘Bacterium’ as examples of malicious software destroying the victim’s system.

Cyber identity theft, phishing and cheating

Identity theft is a criminal activity in which someone pretends to be somebody and retrieves vital information about someone. Identity theft fraud is the assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of action (Fafinski, 2008). Identity fraud can be used to commit drug, firearms and e-crime offences. It encompasses the gaining of money, goods, services or other benefits through the use of a false identity (Australian Centre for Policing Research [ACPR], 2006). Bourgeois and Bourgeois (2020) noted that hiding one’s identity or faking the identity of another user on the Internet is called spoofing in the IT world. Similarly, phishing is used to describe an act of sending false e-mail or web pages to internet users, establishing it as a legitimate enterprise to steal private information which can then be used for identity theft. Phishing is simply an alteration of the word "Fishing". Here, the perpetrator is the fisherman, the email is the bait and the targeted victim is the fish. The stolen information is then used for the criminal’s benefit.

Identity fraud is staged by someone who gains access to other people’s personal information and uses it for his benefit. This ranges from stealing online banking account login and password by a cyber-fraudster to accessing personal information of a person’s automatic teller machine (ATM) and using it to amass a lot of money. The Federal Bureau of Investigation [FBI] (2011) revealed that fraudsters steal ATM card pins and numbers by hiding cameras in places like eateries when making payments through the Point of Sale, POS, or the ATM posts where withdrawals are made. Accordingly, ATM skimming which involves the placing of an electronic device on ATMs for scooping information from the user’s bank card’s magnetic strip is employed when transactions are made through them. Computers and the users are deceived or tricked.

Wall (2007) noted that credit card numbers are unlawfully obtained to order goods or services online. In some cases, a false bank webpage is designed to collect a person's account information, or calls are made with the pretence of being what the fraudster is not, with the aim of cheating or defrauding the caller. The worrisome part of identity theft or fraud is that information (e.g. passwords, credit card and social security numbers, other personal or corporate information) are illegally copied from an individual or business enterprise. Ultimately, the individual who stole such information will be prosecuted by law if apprehended. Cyber fraud and cheating are also perpetrated in the forms of contractual crimes, job offerings, etc. (Rahman, 2012).

Cyber fraud remains a lucrative and illegal business in cyberspace. In Nigeria, web links are designed to unlawfully access users' data (PINs and personal details) by requesting naive computer users to fill online forms (Unini, 2019). In Nigeria, cyber fraudsters send emails through conventional messages and social media platforms to claim that a potential victim has been named as a beneficiary for the will of an estranged relative and stands the chance of inheriting millions of naira and large property. An individual may also be phished through online charity, where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Fraudsters also host fake charity social network pages built for soliciting money from unsuspecting individuals. Sometimes, they claim that a particular person is sick and needs money for medical bills. They even go as far as displaying pictures evidencing the sick condition of the person on fake websites. Hence, the donation from kind-hearted individuals, who get unknowingly exploited, profits the cybercriminals.

There is also a cheat/scam in which people become victims of cyber fraud by being sent an email or SMS claiming that they have won lottery tickets or online lottery they never registered for or entered. These scams lately include the State Department's green card lottery. Rahman (2012) revealed that bogus cashier's check has been used to defraud people through advertising items for sale on the Internet or posting items that do not exist or are damaged, by asking the victims to contact a particular number and pay some amount of money into an account. Currently, in Nigeria, sales of non-existent products are increasingly commonplace on the webs. Omodunbi et al. (2016), also noted that the purchase of items over the internet can be misleading due to ingenuity or absence of the products. Where individuals fall victim to this kind of fraud, the fraudsters make more money.

The Western Union money transfer scheme has also been used to perpetrate cyber fraud in Nigerian banks (Wall, 2007). Western Union money transfer is an online money transfer service that allows customers to send and receive money from all over the world via Western Union Agent locations. Fraudsters use foreign names that are not recognised by any bank and align with compromised banking staff to access funds. A successful fraud cannot be easily executed without an insider within the bank. This is because the facilitation of payment is dependent upon the insider who does not alert the relevant security agencies. For every successful fraudulent transaction, the insiders also get their share. It was in a bid to checkmate such fraudulent practices that the Central Bank of Nigeria (CBN) introduced the Bank Verification Number (BVN) scheme in 2014, to prevent cyber theft and other crimes. Notwithstanding such policy intervention, the perpetration of such illegal activities continues (Ebem et al., 2017).

Ebem et al. (2017) averred that the BVN project was introduced to enhance financial security which was already failing to arrest password and pin theft. Accordingly, during the heat of registration for BVN, customers' bank accounts were suspended to enable them obtain the BVN within the stipulated timeframe. However, during the interval, cybercriminals were reported to have impersonated legitimate bank staff by contacting unsuspecting bank customers, requesting their bank details, and promising to unlock their suspended bank accounts. This resulted in the loss of a substantial amount of money after the accounts have been activated by the bank when the customer eventually registered and obtained the BVN. To date, cyber fraudsters are known to be visiting sites like 'harvest' phone numbers and truecaller.com, to access registered phone numbers. Text messages are sent to such phone numbers, telling the owners that their BVN registration was incomplete and therefore, request for the first or last names of the owners. The financial information (ATM pin, account number, etc.) of the owners of these numbers is required to rectify the issue observed and to which correct response eventually results in their being defrauded.

Website Jacking/Cloning

Website jacking is a process by which hackers hijack or gain access and control over the website of another while website cloning is the creation of a fake copy-cat website (Bourgeois & Bourgeois, 2020). The creation of fake websites that appears original but targeted at internet users who are ignorant of the legitimate company web address is also taking another level in Nigeria. In this case, internet users are made to believe that a particular website is an actual website they are intending to visit. However, their credit card details become stolen when they impute their information on the website of the fraudsters while purchasing or ordering goods. The information stolen by the fraudsters would then be used to defraud the victim or sold to others who are interested in defrauding people through their credit cards.

When a particular website is hijacked, the information is mutilated or changed by the hijacker (Abiola, 2019). This is purposely done to either fulfil certain objectives including ideological, political, economic, social, or psychological, among others. Website hijacking has been reported in Pakistan in which the site of the Ministry of Information Technology was hijacked by Pakistani hackers who placed some offensive matter and obscene materials on the website (Dashora, 2011). Again, the website of the Bombay crime branch was reported for web jacking. Furthermore, the website for 'goldfish' was hijacked and the information about the goldfish got changed, leading to the demand of US $1 million as ransom.

While the hijacking of websites is a rare case in Nigeria, the cloning of websites is common. Take, for example, the Department of State Services (DSS), which has repeatedly drawn Nigerians' attention to the behaviour of some unscrupulous elements copying legitimate government websites in order to swindle innocent Nigerians. Cybercriminals use the official names of specific Ministries, Departments, and Agencies (MDAs) to deceive susceptible people through website cloning. According to Ijeh (2019), the National Youth Service Corps (NYSC) and the Nigeria Social Investment Trust Fund (NSITF) have both been victims of decoys used by fraudsters to manipulate their victims. Similarly, Ripples Nigeria (2021) reported that cloned email address of the Economic and Financial Crimes Commission (EFCC) was allegedly used to send messages to defraud unsuspecting victims while the senders posed as officers of the Commission.

Indecent exposure to obscene materials and child pornography

Today, the internet has been used for promoting child pornographies and obscene or immoral materials. Cyber-pornography is committed in cyberspace by individuals who create, distribute, display, import or publish obscene materials that depict children to be engaging in sexual acts with adults (Omodunbi et al., 2016). Cyber-pornography is classified as a criminal offence because of its associated harm to individuals and society. The Internet is flooded with several unwanted and immoral materials including pornographic pictures and videos, basically against children. The promotion of pornography is done with the help of computers and the internet to create websites that are solely used for producing these obscene and immoral materials. The obscene materials are watched or downloaded through the Internet and may harm and corrupt the mind of adolescents.

A popular case of child pornography in Nigeria is the case of two suspects that were arrested by the Nigeria Police Interpol National Central Bureau, for engaging in international child pornography. The offenders were alleged to have sexually abusing minor girls, recording the crime on camera and sharing it on an international Whatsapp group chat called "Pervertidos," which is owned and maintained by a Brazilian named Adriana (Adewole, 2021). Accordingly, forensic analysis conducted by the police team on the devices confiscated from the suspects showed a series of pornographic/erotic recordings with minor females that the suspects published on the internet for a price in US Dollars. The Cybercrime Act 2015, prohibits anyone from procuring child porn on their computers, recruiting and coercing children online for sex.

Attacks via Smartphones

Unsafe surfing is one of the most popular attack vectors for smartphones (malware, phishing, spear phishing). According to IDC’s Worldwide Quarterly Mobile Phone Tracker (January 27, 2016), more than 1.4 billion smartphones were bought in 2015, and out of six new phones, five were running Android while one in seven running Apple’s iOS operating system (Framingham, 2016). Dunn (2020) estimated that by the end of 2020, there would be 6.4 billion smartphone subscribers worldwide. This suggests that practically everyone will have access to a phone. In 2014, the number of new vulnerabilities discovered in mobile software increased by a whopping 214 percent globally (Framingham, 2016).

Smartphones are becoming a more appealing target for cybercriminals who are investing in more complex attacks, such as ransom ware. Mobile virus that is capable of collecting personal information or extorting money from victims while also posing a threat to the world's future (Dunn, 2020). The increasing rise of mobile malware, which primarily targets Android devices, is alarming. According to Symantec (2016), in Nigeria, more than one in every seven mobile devices is presently infected with mobile malware. More than 60% of online fraud is committed via mobile platforms, while 80% of mobile fraud is committed via mobile apps rather than mobile web browsers (Dunn, 2020). Today, mobile phones, especially smartphones and iPhones, are vulnerable to cyber-attacks because they are used by most people to manage and handle their financial operations including sensitive data out of home network security. There is an increased risk of smartphones getting attacked if they are stolen or lost due to the sensitive information stored on them (Coony, 2012).

Internet time thefts and data and airtime time (DAT) theft

Internet thefts or bandwidth thefts are usually carried out when the Internet surfing hours paid by a particular victim are used up by an unauthorised person. The unauthorised person tries to get access to the username and password details of the victim. The account details can either be accessed illegally or legally for a stipulated period through proper awareness and consent of the user. The prevalence of internet time theft in Nigeria today is made possible by the wireless network and open Wi-Fi connection, especially one without a password for internet access (Longe *et al*., 2008). A subscriber is generally billed on the amount of bandwidth consumed. Meanwhile, a criminal may be using the victim's internet account, without his/her awareness for free internet access. An illegal activity conducted by the freeloader can be traced back to the victim since his account or IP address will be found in the activity logs (Longe *et al*., 2008).

Similarly, cybercafés have developed means of connecting to the network of internet service providers. In Nigeria, cybercafé operators run at no cost by connecting to the network of some ISPs of other people without being detected (Ndubueze et al., 2013). Similarly, gaining access to thousands of unlimited airtime and mobile data is common with today's youth in Nigeria. This act is done to avert the necessary payment for data and airtime. The major problem of internet time and data theft is the financial loss to the victims, which may be an individual or organisation.

Methodology

This paper is theoretical in nature. In other words, it relies on secondary sources of data. Secondary data were gathered from diverse literature sources such as research reports, institutional publications, journals, magazines, newspapers and the internet.

Theoretical Anchorage

This paper is anchored on a triangulation of three theories, viz, Control, Structural strain and Cultural transmission theories. Each of these theories is examined hereto, in relation to the phenomenon of cybercrime.

Control Theory

The point of departure of the control theory is that deviance is the outward manifestation of the failure of social control. Proponents of the theory argue that life is full of temptations and engagement in deviant acts such as cybercrime may be fulfilling or rewarding to the perpetrators. The theory noted that people conform to societal norms because such a society has mechanisms for enforcing compliance by its members, adding that where such mechanisms are weak, there is a high probability of deviation. Durkheim, one of the proponents of the theory explained that societies with strong social bonds are more likely to exercise greater control and extract conformity from their members. Conversely, weak collective sentiments as a result of weak social bonds are likely to produce weaker levels of conformity, culminating in deviant acts such as cybercrime.

Structural Strain Theory

The central thesis of the structural strain theory is that deviance is the outcome of social strain that puts pressure on people, especially the socially deprived, to deviate. Credited to the American sociologist, R.K. Merton, the theory argues that crimes such as cybercrime may result from a perceived imbalance in the social system. According to the theory, deviant behaviour, in this case cybercrime, may occur on a large scale when a value system extols, certain important critical success goals for the citizenry while the social system rigorously severely limits or utterly closes direct connections to approved modes of achieving these goals for a significant part of same citizenry. Put differently, it is the same society that creates opportunities and assures individuals of the means to actualise such opportunities that also blocks access to achieving the means or goals, thereby creating a sense of confusion or anomie. Under such circumstances, those who feel short-changed devise disapproved criminal means such as stealing, banditry, kidnapping and cybercrime to achieve their goals.

Cultural Transmission Theory

The cultural transmission theory, better known as ‘differential association’ theory, assumes that deviant behaviour is learned through a process of interaction with others. According to the theory, criminal behaviours such as cybercrime is learned like any other type of behaviour. Edwin Sutherland who is the arrowhead of this theory asserted that deviant, abhorrent or criminal behaviour is learned through ‘differential association’ with particular people such as those who commit cyber-related offences. Bello (2017, p.178), identified expressions such as ‘birds of the same feather always flock together’ or ‘he was a good kid until he started going out with bad guys', as examples of how interactions with people with criminal tendencies can predispose otherwise law-abiding people to engage in criminal acts such as cybercrime.

Discussion

Causes of Cybercrime in Nigeria

Cybercrime related offences made their road into Nigeria in the 1990s. Such crimes were generally referred to as Advance Fee Fraud, or simply '419'. Advance fee fraud was a means by which some dubious Nigerians deceived foreigners into parting with their money by promising them non-existent oil contracts. Fraudsters perpetrate such illicit acts by sending emails to their prospective victims whom they promise oil well contracts and demand upfront payments to facilitate the process. Most times, the foreigners are invited into Nigeria and treated to make-believe official receptions during which they are made to sign fictitious contract papers. However, after being put through such make-belief shady deals and upon return to their country of origin, the foreign businessmen would later discover to their discomfiture that they have been coned by Nigerian fraudsters who, thereafter, discontinue further communication with their victims.

Beyond the Advance fee fraud or 419 scams, the growth in information communication technology has led to an unprecedented rise in other cybercrime offences such as extortion, identity theft, cyber trespassing, digital piracy and email scams, among many others. The intensity and level of cyber criminality in Nigeria is not only unprecedented and alarming but also does not show sign of abating any time soon.

Toure (cited in Bello, 2017), summed up the causes of cyber criminality in Nigeria to include but not limited to: a materialistic value system in which many Nigerians worship and celebrate wealth without asking whether such wealth was acquired through fair or foul means and the get-rich-quick syndrome, peer group influence, the influence of the mobile phone revolution and socioeconomic pathologies. At other times, such crimes could be induced more by malice rather than the profit nexus, especially where computer devices themselves are the target while some are for the inner desire of revenge for some perceived wrongs and the illicit desire to invade other people's private financial transactions or information.

For Abdulkareem (2009), cybercrime in Nigeria is rooted in poverty, unemployment and corruption. According to him, Nigeria's harsh economic realities characterised by youth unemployment and other vicissitudes have pushed many youths into using social media applications like Yahoo mail, Google chat, Whatsapp, Badoo, Instagram, Facebook, etc. as strategies to defraud unsuspecting victims as well as commit other heinous crimes such as kidnapping, murder, stalking, etc. The consensus is that most of the young people apprehended for such crimes were of poor family background and unemployed.

The poverty causes crime 'theory' has its limitations, because it is not always the poor or the youth that get involved in crime and criminality. The Economic and Financial Crimes Commission (EFCC) and the Independent Corrupt Practices Commission (ICPC) have prosecuted many wealthy and high profile Nigerians for indulging in different forms of crime. In particular, a serving minister was in 2013, alleged to have been involved in a recruitment scam in which his ministry was believed to have defrauded 676,675 Nigerian job seekers by charging each of the applicants N1000 as an online processing fee for recruitment into the Nigeria Immigration Service (NIS). The Minister in question and other accomplices are currently being prosecuted by the EFCC.

Consequences of Cybercrime

The costs of cybercrime are enormous and mindboggling. Studies have identified cybercrime costs to include destruction of data, loss of productivity, thefts of money, intellectual property and personal data, disruption of business activities, restoration and deletion of data and systems, reputational harm and embezzlement (Morgan, 2017).

In Nigeria, cybercrime causes a lot of damage to the country's international image and reputation. Many Nigerians who travel outside the shores of the country are daily subjected to undue stigmatization and name-calling because of the activities of some Nigerian cybercriminals. Many Nigerians are treated without honour, respect and dignity, because some foreigners see and treat people of Nigerian extraction as scammers, fraudsters, dupes, 419ers, etc. Such demeaning characterization has done incalculable damage to the international image of Nigeria.

One of such Nigerians who has dragged the country's name in the mud is Ramon Abbas, commonly known as Hushpuppi, a 39-year-old Instagram celebrity and social influencer. In the United States of America, Hushpuppi is facing criminal accusations for allegedly conspiring to launder money collected from business email compromise frauds and other schemes totalling $178.7 million. He is considered by America's Federal Bureau of Investigation (FBI) to be one of the world's high profile fraudsters and faces a prison sentence of up to 20 years in the US after pleading guilty to money laundering. He is reported to be one of the richest Nigerian socialites with an estimated net worth of $35.5 million (The360report, 2022).

In financial terms, cybercrime has done grave damage to Nigeria's economy as the country is believed to have lost an estimated $9.3 billion to cybercrime in addition to other potential financial losses emanating from erosion of consumer confidence and the stalling of foreign direct investment. Frank and Odunayo (2013) lamented that more than $80 billion is lost to software piracy annually in Nigeria describing the trend as one of the fastest-growing online scams largely perpetrated by young Nigerians.

Similarly, the Economic and Financial Crimes Commission (EFCC) disclosed that as at September 2021, 80 percent of its 978 convictions were connected to cybercrime and cybercrime related offences. Mr Abdulrasheed Bawa, Executive Chairman of the EFCC, noted that the 'boom' in cybercrime offences in Nigeria is reinforced by the switch over to what he described as "e-society" where everything is done electronically , like e-payment, e-ticketing, e-voting, e-banking, e-payment, e-registration, which had made e-dealings vulnerable to cyber-attacks and negative consequences of security threats.

Speaking in Lagos, at the Cyber Secure Nigeria Conference 2021, themed "The Future of Cyber Security in Nigeria's Digital Transformation", the EFCC boss lamented that global financial damages and losses from cybercrimes reached $6 trillion by 2021 adding that cybercrimes cost businesses, government agencies and consumers, including those in Nigeria, more than $1 trillion in 2020. The amount, according to the EFCC's helmsman accounted for about one percent of the global Gross Domestic Product (GDP). Mr Abdulrasheed added that while about $945 billion was lost to cyber incidents for the period under reference, $145 billion was spent on cyber security (The Guardian, 2021).

Attempts by the Nigerian Government to Fight Cybercrime

Successive Nigerian governments have made diverse attempts to curb the menace of cybercrime. Such attempts recorded debatable degrees of success. Huge sums of money are often budgeted annually to give the anti-cybercrime and other forms of criminality fight the necessary fillip as part of government's drive to encourage local and foreign investors/investments. By far the most significant push in the battle against cybercrime, is the promulgation of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015. The provisions of the Act are meant to curb the notorious activities of cybercriminals vis-à-vis their implication on the country's local and international image. The Act has eight major parts including objectives and application of the law, protection of critical national information infrastructure, offences and penalties, duties of financial institutions, administration and enforcement, arrest, search, seizure and prosecution, jurisdiction and international co-operation and miscellaneous (Suleiman et al., 2017, p. 355).

While the Act contains eight major parts, part three which isolated offences and penalties is particularly relevant. Offences covered by this section include those against critical national information infrastructure, computer-related forgery and fraud, cyber terrorism, identity theft and impersonation, child pornography and related offences, cyber stalking, cybersquatting, among others. Like many pieces of legislation, the implementation of the Act has been confronted with some challenges which are narrowed down to lack of harmonized global cybercrime laws, weak access to internet evidence and an increase in the number of internet users (Suleiman et al, 2017).

Aside the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015, Nigeria's National Security Adviser (NSA), Retired Major- General Babagana Mungonu, also revealed that the government has established a National Cyber Security Policy and Strategy Roadmap to address emerging threats in the cyber domain and enhance progressive use of cyberspace in Nigeria. According to the Guardian (2021) the NSA made the disclosure in Lagos at the Cyber Secure Nigeria Conference 2021, with the theme "The Future of Cyber Security in Nigeria's Digital Transformation"

The fundamental aim of the National Cyber Security and Strategy Roadmap is to have a harmonized security strategy that would respond to the dynamism of the national security threat landscape. The document listed five key national cyber security threats which pose significant challenges to the country and are inimical to Nigeria's national growth and security. These include cybercrime, cyber-espionage, cyber conflict, cyber terrorism and child online abuse and exploitation. However, despite the existence of government-induced cybercrime mitigation interventions, cybercriminal activities in Nigeria have not shown any significant sign of abatement.

Conclusion

This paper concludes that cybercrime is a global challenge that victimises people of all backgrounds and classes. It has nonetheless, become a persistent source of concern to both the citizens and the Nigerian government. Nigeria is associated with two things globally, oil and princes (the *yahoo boys* phenomenon), which potentially hold the promise of wealth and prosperity through the use of the internet, especially social media. The paper has shown that cybercrimes are perpetrated through several means including phishing, cyber terrorism, hacking and internet theft, among others.

Cybercriminals are smart, intelligent and dynamic youngsters who employ several methods to consummate their atrocities by consistently updating their tactics, to understand the psychology of potential victims. These include the victims' gender, age, economic status and occupational group. The state of mind and ego of the vulnerable are often manipulated by cybercriminals to successfully prey on them. Unfortunately, cybercrimes are patterned in such a way that it is quite difficult to apprehend many of the perpetrators.

Recommendations

Based on the foregoing discussions and the conclusion arrived at, the following recommendations are made for policy guidance and possible implementation:

i. Internet users should secure their computer systems by enabling firewalls that are capable of blocking connections from suspicious traffic and probably keep the system out of some types of viruses and hackers. Anti-virus/malware software should be installed and regularly updated to prevent viruses from infecting the computer.

ii. Internet users should protect their electronic identity by being cautious when giving out personal details such as name, phone number, address, or financial information on the Internet. It is advised that computer and internet users find out the security status of websites when making online transactions. They should also ensure that privacy settings are enabled when accessing social networking sites, like Facebook, Twitter, YouTube, etc.

iii. Internet users should note that using public Wi-Fi, exposes unprotected electronic devices to cyber-attacks. Hence, users should be conscious, while conducting sensitive transactions on such networks.

iv. Internet users should avoid being scammed by being sensitive to or not replying to emails that request them to verify certain information or confirm their username user ID or password. They should also guard against clicking links or opening files emanating from suspicious sources, no matter how genuine they may seem or appear.

v. Relevant government agencies should intensify the training and retraining of law enforcement agents with the sophistication necessary for dealing with the scourge of cybercrime.

vi. The Federal Government should ensure the due enforcement of the relevant sections of the Cybercrime (Prevention, Prohibition, etc.), Act of 2015 by ensuring that apprehended cybercriminals are promptly prosecuted to serve as deterrent to other potential internet fraudsters. The prosecution of such criminals will also serve to restore public confidence in the fight against cybercriminals a swell as attract foreign direct investment (FDI) in the country.

vii. Both the Federal and State Governments in Nigeria should formulate and sustain policies that address the socio-economic challenges bedevilling the youth, by focusing on creating sustainable employment and empowerment opportunities to mitigate poverty.

viii. Nigerians should learn to name and shame cybercriminals by publicly denouncing them, instead of uncritically celebrating known fraudsters with questionable sources of wealth.

References

Abdulkareem, S. (2009). *A study of the nature and extent of cybercrime in Kano metropolis.* An unpublished M.Sc. dissertation submitted to the Department of Sociology, Bayero University, Kano.

Abiola, A. (2019). What Nigerians lose yearly to cybercrime. *The Hope Newspaper.* Available at: https://www.thehopenewspaper.com/what-nigerians-lose-yearly-to-cybercrime/. Accessed on: 19/12/2021.

Adewole, S. (2021). Police arrest two for Int’l child pornography. *The Punch.* Available at: https://punchng.com/police-arrest-two-for-intl-child-pornography/. Accessed on 18/11/2021.

Advance Fee Fraud and Other Fraud Related Offences Act 2006, Laws of the Federation of Nigeria.

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. Doi: 10.1089/cyber.2010.0307.

Arora, B. (2016). Cyber Crimes Schemes and Behaviours. *Perspectives in Science*. Available at: https://www.researchgate.net/publication/304907065_Cyber_Crimes_Schemes_and_Behaviors/. Accessed on: 12/12/2021.

Bello, K. (2017). "Information Communication Technology and Cyber Crime" in P.N. Ndubueze (Ed.). Cyber criminology & Technology Assisted Crime Control: A Reader. Zaria: Ahmadu Bello University Press.

Coony, M. (2012). *10 common mobile security problems to attack.* Available at: https://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html. Accessed on: 18/11/2021.

Cruz, A. (2013). Cyber Crime and How It Affects You. *Cyber Security Tips*, *7*(1). (No page number provided).

Cybercrime Act (2015). *Laws of the Federation of Nigeria.* Lagos: Federal Government Press.

Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

Denning, D. (2001) "Activism, and Cyber terrorism: The Internet as a tool for influencing Foreign Policy," in John Arquilla and David Ronfeldt, ed., Networks and Net wars. p. 241

Ebem, D.U., Onyeagba, J.C. & Ugwuonah, G.E. (2017). Internet Banking: Identity Theft and Solutions - The Nigerian Perspective. *Journal of Internet Banking and Commerce*, *22*(2), 1-15.

Fafinski, S. (2008). *UK Cybercrime report.* Available on: http://www.garlik.com. Accessed on: 01/01/2022.

Frank, I. & Odunayo, A. (2013). Approaches to cyber security issues in Nigeria: Challenges and solutions *International Journal of Cognitive Research in Science, Engineering and Education*, 1 (1), 100-110.

Global Forum on Cyber Expertise (2020). Strengthening cyber capacity and expertise globally through international collaboration. Available on: https://thegfce.org/. Accessed on: 02/01/2022.

Graycer, A. (2000). *Nine types of cybercrime.* Available on: http://aic.gov.au/conference/other/graycer_adam/2000-02-cybercrime.html. Accessed on: 02/01/2022.

Harvy, C. (2017). Types of Malware and How to Defend Against Them. *Security Planet.* Available on: https://www.esecurityplanet.com/malware/malware-types.html. Accessed on: 13/11/2021.

Ijeh, M. (2019). *DSS Raises the Alarm! Nigeria Government's Official Website is Being Cloned.* Available on: https://metrowatchonline.com/dss-raises-the-alarm-nigeria-governments-official-website-is-being-cloned/, Accessed on: 16/2/2022.

Longe, O.B, Chiemeke, S.C., Fashola, S., Longe, F & Omilabu, A. (2008). "Internet Service Providers and Cybercrime in Nigeria – Balancing Services and ICT Development" Retrieved from https://www.intgovforum.org/cms/documents/contributions/general:contribution/2008-1/349-longe-o-b-et-al-isp-and-cybercrime-in-nigeria-lgf-contributions/file. Accessed on: 10/11/2021.

Morgan, S. (2017). "2017 Cybercrime Report" .Available at: https://www.cybersecurity.com. Accessed on: 27/02/2022.

Muhumuza, R. & Olukoya, S. (2019). *Nigeria in battle against fake news ahead of elections.* Available at: https://thegrio.com/2019/02/13/nigeria-in-battle-against-fake-news-ahead-of-elections/. Accessed on: 16/11/2021.

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cybercrime victimization among internet active Nigerians: An analysis of socio demographic correlates. *International Journal of Criminal Justice Sciences*, *18*(2), 225-234.

Olugbodi, K. (2010). *Fighting Cyber Crime in Nigeria.* Available at: http//www.guide2nigeria,com/news_articles_About_ Nigeria. Accessed on: 10/11/2019.

Omodunbi, B.A., Odiase, P.O., Olaniyan, O.N., & Esan, A.O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology*, *1*(1), 37-42.

Opaluwa, T. (2016). "Cybercrime in Nigeria: The fight rages on". *The Leadership*. February 27.

Ribadu, N. (2007). A welcome address presented at the West African sub-regional meeting on advance fee fraud jointly organized with INTERPOL at the EFCC Training and Research Institute (TRI) Karu, Abuja. *Current Trends in Advanced Fee Fraud in West Africa*, Available at: www.efccnigeria.org/index. Accessed on: 16/1/2021.

Rughani, C.P. (2011). *Cybercrime. To Study Various Cyber Crime with Activity and Suggest Solution of Cyber Crime.* Thesis submitted in partial fulfilment of the requirement for the degree to Master of Computer Application from the Indian B.H.Gardi College of Engineering & Technology.

Suleiman, I.M., M.A. Ishaq, M.A. & Rabiu, B.I (2017), "The Nigerian Cybercrime (Prohibition, Prevention, Etc.) Act 2015" in P.N. Ndubueze (Ed.). Cyber Criminology & Technology Assisted Crime Control: A Reader. Zaria: Ahmadu Bello University Press.

Symantec (2016). Cyber Crime & Cyber Security Trends in Africa. Global Forum for Cyber Expertise (GFCE) Initiative. Available at: https:// www.cybercrime and cyber security trends in Africa. Accessed on: 18/12/2021.

The Guardian (October 7, 2021). "80 % of EFCC's 978 Convictions Cybercrime Related" Available at: www.guardian.ng Accessed on: 28/3/2022.

The 360 Report (2022). Hushpuppi. Net worth and biography. https://the360report.com. Accessed: 28/02/2022.

Unini, C. (2019). Cyber Defamation: Be Careful About What You Post Online. *The Nigeria Lawyer*. Available at: https://thenigerialawyer.com/cyber-defamation-be-careful-about-what-you-post-online/. Accessed on: 11/11/2021.

Urbas, G. & Choo, K.R. (2008). *Resource materials on technology-enabled crime, AIC, Canberra.* p.83; AIC, High tech crime brief: Hacking offences, AIC, 2005, p.1.

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.