Efforts in Combating Cyber Crime and Criminality in Nigeria

Pereware Aghwotu Tiemo   Digitemie-Batubo Beleudaara Nelly
The University Library, Niger Delta University Wilberforce Island, Bayelsa State, Nigeria

Abstract

Since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Cyber crime is the most complicated scourge in the cyber space. Many nations are battling to protect their cyber space from criminals, for national security and integration. As a result of this, efforts are being made by governments to protect their citizens and image from online crime. This paper therefore examines some previous reports of cyber crime cases, some types of cyber crimes, channels through which cyber crimes are perpetrated in Nigeria. Methods of receiving payment, cybercrime as a threat to Nigeria economy and efforts in combating cyber crime and criminality in Nigeria.

Introduction

The advent of information and communication technology (ICT) facilities such as the internet has brought positive transformation to all aspects of life. It is a major factor on which the world depends to support economic growth, innovation and social development. There is no denying the fact that internet has changed the way we do things. It has become a driving force in every aspect of human endeavour. The internet is growing rapidly by the day with more and more people, schools, organizations, industries using it as a tool for business transaction, commerce, health, politics, educational information etc. The internet has brought about considerable improvement in efficiency in business processes in the society. Although the Internet has several benefits, it also has a bad side that has brought about occasional sadness and anguish due to abuse, misuse and subversion.

The flip side, however, is that since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Cyber crime is the most complicated problem in the cyber space and many nations are battling to protect their cyber space from criminals, for national security and integration.

Cyber crime refers to unlawful practices carried out using computers, electronic and ancillary devices. It involves disruption of network traffic, email bombing, distribution of viruses, identity theft, cyber stalk and cyber squatting (Fanawopo, 2004). Similarly, Ifukor (2006) sated that cyber crime includes all forms of crime committed through the use of the internet. They are referred to as internet fraud. This means using one or more components of the internet such as chart rooms and emails among others, to present fraudulent solicitation to prospective victims or to defraud individuals or financial institutions.

According to Laver (2005) drug cartels, organized crime, international money launderers and computer hackers are unleashing themselves on the information high ways and they are becoming even more successful. There is also a mounting concern about cyber terrorism through the use of computers sabotage. This is one of the fastest, growing criminal activities on the planet. Organised crimes are using cyber space more frequently to target credit cards information and personal and financial details for internet fraud.

In Nigeria, and other parts of Africa, the perpetrators of this illegal act have even upgraded their nefarious activities from the physical to the mystical, in what can be described as Yahoo Yahoo+. This involves using occult powers to target individuals for their scams. This, undoubtedly, has increased Nigeria`s notoriety in the world rating on cyber- related offences (Atili 2011).

This paper focuses on previous reports of some cyber crime and criminality cases in Nigeria. Furthermore the paper x-rayed some types of cyber crimes, channels through which they are perpetrated in Nigeria, methods of receiving payment and cyber crime as a threat to the Nigerian economy, efforts being made to combat cyber crime and criminality and implication for library services in the country.

Previous Reports of Some Cyber Crime and Criminality Cases in Nigeria.

Several cyber crimes have been committed within and outside Nigeria. Some of these criminals when caught were reported in the national dailies. Among those report were, the case of a suspected hacker who was arrested by the Nigerian Customs Services for breaking into their work station to download vital information from the Customs computer. The intension of the suspect was to use the information to release goods to owners at a cheaper rate in the clearance office (Oritse and Clement, 2011).

Ogwuda (2008) also reported that friends and associates of Delta State Governor were swindled of large sums of money by a gang of fraudsters who shoot off the Governor`s personal mobile phone on the 7th and 8th of January, 2008 in collaboration with some staff of MTN, making it impossible for the Governor to make or receive calls. They used the Governor`s line to send messages asking for financial assistance. It was initially believed that, it was a network failure with the hope that the service would be eventually restored. When this was not forthcoming an enquiry was made and it was found out at the MTN office that a report was made by an unknown person of the loss of the line. A bank account was open under a cover name and they lured victims to pay some specified amount of money into it bearing in mind that the text message was coming from the mobile phone of the Governor. The fraudsters involved were arrested by the State Security Service.

In May/June 2011, swindlers uploaded some fake West African Senior Secondary Certificate Examination question papers. The fraudster had requested that any candidate interested should send the sum of N1,000 through mobile phone recharge card to his phone number. This was done through face book (Olugbile, 2011).

In Nigeria, majority of the fraudsters are mainly university students and school drop outs, using cyber cafes to swindles their victims. Aborisade (2009) reported that the Nigeria Police arrested five undergraduate students of the University of Abuja and University of Port Harcourt for allegedly using the internet to access the site of some banks and transferring money from other people`s account into their own account.

In Onitsha, the Economic and Financial Crime Commission (EFCC) invaded some cyber cafes on the 2nd of April, 2008 and arrested some fraudsters popularly known as Yahoo Boys and ceased some of the cyber cafes computers for allowing frauds to be perpetuated in their cyber cafes (Ujumadu, 2008).

Famutimi (2014) reported that hackers defaced the home page of the Nigerian Army although they could not gain access to the recruitment portal. This was done through phishing, weak passwords or software vulnerabilities. It was not clear whether the hackers were able to gain access to the Nigeria Army databases or not. This hacking group have been notorious since 2012, defacing website belonging to the National Examinations Council and that of the EFCC. Similarly, it was reported that the State Security Services network was hacked and record consisting of their names, addresses and next of kin, phone numbers, profession, date of birth and other details of the agents such as their spouses, children and family members were posted on the internet on August 12th, 2012 (Punch Newspaper, 2012).

The General Overseer of The Redeemed Christian Church a very popular church in Nigeria, said that some people were impersonating him on face book, demanding money from members of the public to be paid into a bank account operated by them (Akinkuotu, 2012). In the same vein, a one time Minister of Finance raised an alarm over cyber fraudsters laying claims to her identity on face book. Over 127 scammers used her name fraudulently to dupe people online. They operated with fake facebook account (Famutimi, 2014)

On July 22, 2012, a young female undergraduate student of Nasarawa State University was gruesomely murdered by some scammers. It all started when she accepted their friendship request on facebook. The student was lured into a business proposal. Unknown to her, the business idea that was sold to her was meant to scam her. She travelled to Lagos to meet the scammer where she was murdered (Yusuf, 2012).

Cyber crimes in Nigeria among the youths are done with passion. Sunday Punch (2011) reported that youths were being charged to court for defrauding victims of millions of Dollars internationally. According to the report, a 26 years old male graduate student of the University Ado-Ekiti, with his American accomplices, allegedly scammed their victim the sum of $620,225.04. He was charged to the High Court in Akure by EFCC for conspiracy and obtaining money under false pretence.

Types of Cyber Crimes and Criminalities in Nigeria

There are various types of cyber crime and criminalities worldwide but the notable ones in Nigeria are as following:

Automated Teller Machine (ATM) Frauds: This is a threat to online payment system in the nation's banking sector. The current rise in ATM fraud has made members of the public lose confidence in this technology that is meant to provide convenience and quick means of withdrawing cash at any point where there is ATM for business transaction. According Obiano (2009) one of the frequent causes of ATM fraud is when customers are careless with their cards and pin numbers as well as their response to unsolicited e-mail and text messages to provide their card details.

Online Identity Theft: Online theft is also a major type of cybercrime. Nowadays, people use the internet to shop online using their sensitive data information such credit card details, date of birth, home address, bank details, etc. on the Internet Criminals target these items of information and use them to siphon money or to buy things online in the victim's name without his or her knowledge.

Copy Right Theft: Cyber criminals also target copyrighted content online. They download moves or software and distribute them without proper permission from the owners. They normally download the software and crack the code and use the software without buying. This act is also a part of software piracy. The following types of work constitute cyber crime of Software Piracy.

i. Cracking the key of any software.
ii. Using unlicensed software in your personal computer.
iii. Using single licensed software to multiple computers.
iv. Distributing such type of software to other persons (Tripahi, 2015).

Hacking: It is an act by which a person`s computer system or network is broken into without the knowledge or permission of the owner, in order to retrieve, steal vital information or corrupt the system, for the actual owner. The persons doing the hacking are called hackers or crackers, cracking refers to unauthorized access to data. Crackers or hackers have a good knowledge and understanding of computer programming language and systems. Hackers misuse their knowledge by committing online crime. There are many types of hackers like Black Hat Hackers, Grey Hat Hackers, White Hat Hackers etc. However, the White Hat Hackers, use their skills and knowledge for better purposes and check the security of any offline or online system.

Terrorism and Organised Crime. There is also a growing concern about the potentials for misuse of ICT by terrorists. Like in Nigeria, a Boko Haram ICT expect was arrested by the Nigerian military for configuring computer images website and internet accesses that enable the group to fight media and psychological operations. It was discovered that the ICT expert was the backbone of the signals and communication links of the late impersonator, Mohammed Bashir who always posed as Abubakar Shekau, whenever he was talking on "U" tube (Omonobi, 2014).This has made cyber-terrorism a strategic issue because the technologies can be attacked, and can also be used to support terrorism in the same way ICTs are used by predatory cyber criminals.

Copycat Website: This is another means internet criminals in Nigeria use in defrauding their victims. They imitate genuine national and international organization websites. Their imitation could be in the same format with similar website names in order to lure people to believe that there is an employment, lottery, auction or investments opportunity in order to get the victims` personal information to defraud them. According to Akande (2011) auction fraud is a misrepresentation of a product advertised for sale or the non-delivery of a product purchased from online auction sale. The employment and investment frauds also aim at defrauding the people that there are jobs available for them and their personal information is used to defraud them. The investment frauds are tricks in making fraudulent claims that they grant loans with low interest with fee attached to it first before you can be granted the loan. After the fee has been paid, the so called business ends.

Scam Mails: This is the most popular online fraud in Nigeria known as advance fee fraud letter. It is also referred to as 419. It derived it name from the Nigerian Criminal Code. Akande (2011) said that the scammers send unsolicited emails or fax messages to victims. The subject matter contained either a money laundering or illegal proposal, which always involved a large amount of funds usually millions of US dollars. The scammers would promise their victims a healthy percentage of these funds as commission as soon as the funds were out of the country. The victims were encouraged to send their personal data such as bank details and other identifying information without delay to the scammers. Having sent these items of information, the victims would feel assured that the business would be genuine. This is also followed up with phone calls from the scammers who would later start to demand money from their victims by telling them all sorts of lies.

Channels Through Which Cyber Crimes are Perpetrated in Nigeria.

There are various channels through which cybercrimes are perpetrated in Nigeria, some of these channels are:

Cyber Cafes. Aginam (2005) noted that cyber criminals use the cyber cafes as their major office to send email to their unsuspecting victims. In most cyber cafes in Nigeria, cyber criminals send hordes of electronic mails to both local and foreign victims with all forms of business proposals that never existed. These cyber criminals operate from the cyber cafe any time of the day, especially in the night when they have unlimited access with some form of discount rates in relation to the money they pay to the owners for the services. Obuh and Babatope (2011) further stated that in some cyber cafes, a number of systems are dedicated to fraudsters popularly known as Yahoo Yahoo boys for the sole purpose of hacking and sending out fraudulent mails.

Mobile Devices. In January 2010, the Nigeria Communications Commission (NCC) ordered all GSM operators to register all subscriber identification module (SIM) cards of subscribers. This is to track fraudsters using their mobile devices to connect to the internet for criminal acts. This exercise was successful in Nigeria. However, some of these fraudsters connive with the agents of the GSM operators to register with fake information in order to use the SIM to have access to wireless internet services for fraudulent act at their own convenience using mobile devices such as smart phones, tablets and laptops. According to Emeka (2007) and Obuh and Babatope (2011) Yahoo boys now sit in the comfort of their homes using these devices any time of the day to perpetrate criminal activities.

Methods of Receiving Payment

These are some of the methods used in receiving payments among scammers:

Electronic Money Transfer: Scammers insist that their victims should transfer money using Money Gram and Western Union. Once the money is transferred, they quickly rush to the bank to claim the money.

Payment into Foreign Account: These scammers have foreign connections with other scammers in England, United States, Canada and other nations. They lure their victims to pay the money into their cohorts` foreign account. With this, their victims believe it is a genuine business (Ayodele, 2015). When the money is paid, their cohorts transfer it to the scammers account or wire it through Western Union, having deducted his/her percentage.

Cybercrime As a Threat to Nigerian Economy.

The activities of cyber criminals in Nigeria have continued to harm the economy and cast a slur on the nation`s image. People around the world are finding it difficult to do online business with Nigerians. Some of the cybercrime threat to Nigerian economy are:

Lack of Trust: Trust plays a major role in facilitating long term online business customer relationships. It evolves around a series of transactions, and if the end users` experience are positive, trust is likely to stabilise, grow and encourage end users to use online services more extensively. The commonest complain about online business is that most of the goods and services delivered are not as good as they were promised to be. Unlike the traditional purchasing channel where the buyers can inspect the goods before paying (Salo and Karjaluoto, 2007). Online business does not give room for that, it is what you order online that you receive.

Defamation of Image: With increasing level of cyber crime in Nigeria, other nations do not trust Nigerians, and this leads to defamation of image. The image of Nigerians will be tarnished and the global community will view the other side of the coin (Hassan, Lass, and Makinde, 2012). The country is finding it worrisome, as a large number of Nigerians are arrested in connection with fraudulent online financial transactions. The result of this is that the reputation of our dear nation has been seriously dented abroad. The situation has become so bad that cyber crimes are now referred to as the ‘’Nigerian Internet Scams’’ largely by the foreign news media (Ayantokun, 2007).

Impediment to the Growth of Online Shopping. The prevalence of internet fraud in Nigeria remains one of the challenges hindering the rapid growth of online shopping within and outside the country. Other nations are afraid to shop online in Nigeria, while Nigerians are also afraid to shop online (Affe, 2010). Online shopping affords people high quality, authentic products from the producers, since they are shopping directly with them. Considering the internet fraud perpetuated by some Nigerians, it is difficult having confidence on online shopping. According to Adomi and Igun (2008) Nigerian Internet Services Providers (ISPs) and email providers are already being black listed in email blocking list systems across the internet. Some corporations are blocking entire internet network segment and traffic that originate from Nigeria.

Efforts in Combating Cyber Crime and Criminality in Nigeria

Nigerian government has adapted different measures in combating cyber crime and salvaging the image of Nigeria from the negative consequences of cyber crime. Some of the methods adopted are as follows:

Compulsory Registration of Subscriber Identification Module (SIM) Cards. In January 2010 the Nigeria Communications Commission (NCC) ordered all GSM operators to register all SIM cards of subscribers as part of measures to deal with rising insecurity problems associated with cyber crime through the use of mobile telecommunication.

According to Amaefule (2011) the registration of SIM cards by GSM operators will enable them to have a central database of users of GSM and to identify the owners of every line. International terrorism, fraud, robbery and other criminal acts involve extensive communication through text messages or voice calls. Nigeria is also witnessing increasing incidents of threats and fraud launched daily on it citizens and others using the mobile phone (Ochaa, 2010).

The Economic and Financial Crimes Commission. This commission, in the last three years has recovered the sum of N 26.5 billion from perpetrators. The recovery was done in collaboration with the Crime Agency of the United Kingdom. The EFCC has intercepted more than 12,000 scam mails that were intended to swindle their recipients of various sums of money.

State Security Services (SSS). The nation`s State Security Service has partnered with the GSM operators to track down people using cell phones for criminal acts and GSM agents registering fake data and the user of the SIM. In Nigeria, cyber criminals use phones in sending threats of assassination and abduction to opponents. The SSS are seriously tackling these crimes (Adebayo, 2006).

Registration of Cyber Cafes in Nigeria. All cyber cafe operators have been adviced to register their cafes with the NCC and EFCC, to install acceptable hardware surveillance. The architecture of cybercafé must be done in such a way that all computers are exposed (Nkenga, 2006). This will help in monitoring cybercafé operators who allow fraudstars to use their services to perpetuate internet crime.

Tackling Illicit Financial Transactions: The Central Bank of Nigeria (CBN) directed all banks to stop accepting foreign currency cash deposits from customers both within and outside Nigeria`s shores, without proper documentation. This is to prevent illicit financial flow in our banking system. This is against the backdrop of a report by the Washington-based Global Financial Integrity group which ranked Nigeria as one of the 10 largest countries known for illicit financial flow in the world. The report claimed that about US$ 15.7 billion (N3.09 trillion) illicit funds go through Nigeria banking system annually. This is scandalous and these funds are traceable to money laundering, terrorism financing, illicit drug trade and oil theft (Daily Sun, 2015).

Cyber Crime Act: In 2015 Cybercrime bill was signed into law in Nigeria. This cybercrime act is meant to address email bombing, cyber terrorism, computer trespass, computer offences against minors, illegal communication using electronic messages, unauthorised modification of the content of any computer, intellectual property, computer vandalism, misuse of devices, data interference etc. This act was designed for the protection of national information infrastructure, computer systems and electronic communications against attacks by hackers. The bill also empowered security agents to intercept, record and seize electronic communications between individuals, especially during criminal investigations. Security officials can also intercept and record personal emails, text messages, instant messages, voice mails and multimedia messages.

Other efforts in combating cyber crime and criminalities in Nigeria are the Nigeria Cyber Working Group (NCWG) and Nigeria Cyber Security Incident Center (NCIC) where cyber crime incidents can be reported (Tiemo and Charles- Iyoha, 2008).

Implication for Library Services.

Academic libraries provide relevant information to the university community for their daily activities. In libraries there are computers connected to the internet for users in sourcing information. Libraries have websites which are used in communicating to their users, subscribe to various online databases, use software to manage their day to day activities, deposit internally generated resources in their institutional repositories. All these and many more make libraries sensitive places where users may face cyber attacks or might commit Internet crimes (Kumar 2013). It is also noted from this study that most of the modern online crimes perpetuated are done by students in higher insinuations and unemployed graduates.

Benson (2001) states that libraries are confronted with security issues such as various attacks, users guessing password, deleting files and corrupting records, either accidentally or on purpose, users accessing programmes they should not, stealing equipment, and generally messing around with programme setting.

Similarly, Tiemo, Bribena and Nwosu (2010) found out that access to Internet in the library used for their study was not pass worded. This meant that users were not restricted to the use of the internet to source information. It could be said from the foregoing that libraries in Nigeria and other nations where there is unrestricted access to the internet, can be attacked by hackers or used as an access point for scamming people if not well secured. Libraries should therefore, secure their systems against hackers and spread of computer virus.

Conclusion

It must be noted that cyber crime is a global phenomenon. Some nations are putting modalities in place to have this crime checked in order to enhance their economy, create good image and a lasting relationship with other nations. In Nigeria, much is still needed to be done such as funding of all agencies set up to bring cyber crime under control, use of modern ICT equipment in tracking cyber criminals, training of more ICT personnel in the area of hacking, computer virus, tracking cyber criminals, training of lawyers in all aspect of internet crime in order to prosecute cyber criminals. To help put cybercrimes under check, government should adequately fund agencies to fight cybercrime in Nigeria. Media campaign should be embarked upon by government to educate citizens on the dangers of internet fraud to the nation, the cyber criminals and intended victims. All cyber criminals caught by the law enforcement agencies should be reported to the Nigeria Cyber Security Incident Centre (NCIC) where their personal details can be recorded in the database and processed for further action according the Cyber crime Act of Nigeria. It is also recommended that libraries should secure their internet access. Library users who want to use the internet should have a pass word that can be used in identifying the users. Librarians' should also monitor the use of their network. Libraries should also embark on creating awareness well as educating individuals on the dangers and consequences of using library network for cybercrimes.

References

Aborisade, S. (2009). Fraudster: police arrest five undergraduate. *The Punch Newspaper*, pp.8

Adebayo, S. (2006, November 10). SSS partners GSM operators to stem crime. *Punch Newspaper*, pp. 8

Adomi, E. E. & Igun, S. E. (2008). Combating Cybercrime in Nigeria. *The Electronic Library.* 26(5), 716-725.

Affe, M. (2010, June 15). Online shopping portal decries prevalence of internet fraud. *The Punch newspaper*, pp.25

Aginam, E. (2005, 14 December). Cybercrime on the increase? Vanguard newspaper pp3.

Akande, A. (2011, March 14). A century of notorious scam mails and fraudsters. *Punch Newspaper*, pp.12

Akinkuotu, E. (2012, August 30). Face book fraudsters using my name. *Punch Newspaper*, pp.6

Amaefule, E. (2011, August 7). SIM card registration: danger of last minute rush. *Sunday Punch Newspaper*, pp 22

Atili, A. (201, August 25). Want ! law for tackling cyber crime. *The Nations Newspaper,* pp.41

Ayantokun, O. (2007, August 22). Tackling online fraud in mobile internet access regime. *Tribune Newspaper*,

Ayodele, O L. (2015). Cybercrime : way forward in Nigeria. *International Journal Economic Development,* 15(10), 56-71

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: *An International Journal of Police Strategies and* Management, 29 (3), 408-433

Daily Sun. (2015, August 13). Tackling illicit financial transactions. *Daily Sun Newspapers,* pp.17

Emeka, A. (2007, June 27). Why EFCC is losing war on web scam. *Vanguard Newspaper,* pp.34

Fanawopo, S. (2004). FG moves to enforce cyber crime laws

Famutimi, T. (2014, April 14). Hackers still on the prowl, attack. *The Punch Newspaper*, pp.14

Famutimi, T. (2014, October 12). 127 scammers use my name fraudulently. *Punch Newspaper*, pp.14

Hassan, A. B., Lass, F.D & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects and the way out. *ARPN Journal of Science and Technology*. 2(7), 626-631 Retrieved from http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf.

Ifukor, M. O (2006).Cybercrime: a challenge to information and communication technology (ICT). Communicate: *Journal of Library and Information Science.* 8(2) 38-49

Laver, N. (2005, June 21). Cracking down on cybercrime. *The Guardian Newspaper*, pp. 80

Obiano, W. (2009, June 21). How to fight ATM fraud. *Online Nigeria Daily Newspapper*, pp.18

Obuh, A. O. & Babatope, I. S. (2011). *Cybercrime regulation: The Nigerian Situation. In E.E. Adomi* (2011) A frame works for ICT Policy: Government, Social and Legal Issues. IGI Global. Information Science Reference. Pp 98 – 112.

Ochaa, I. (2010, November 10).Reps and SIM card registration: The burden of truth. *Business Day Newspaper*, pp.13

Ogwuda, A. (2008, February 8). SSS nabs fraudsters using Uduaghans GSM line. The *Vanguard Newspaper*, pp.10

Olugbile, S. (2011, May 6). WASSCE: fraudsters post fake questions on internet. The *Punch Newspaper*, pp.15.

Omonobi , K. (2014, September 30). Boko Haram's 'ICT expert' arrested, opens up on links with You-Tube. *Vanguard Newspaper*. Retrieved on 12th August, 2015 from http://www.vanguardngr.com/2014/09/boko-harams-ict-expert-arrested-opens-links-tube/#sthash.0km5KuUV.dpuf

Oritse, G., & Clement, U. (2011, July 19).Customs arrest suspected hacker. The *Vanguard Newspaper*, pp,53

Nkenga , E. (2006). Is ban on night browsing solution to cyber fraud? Retrieved on 12th April, 2015 from 419legal.org/forum/archive/index.php?t652.htm

Punch Newspaper (2012, September 3). Leakage: SSS yet to remove staff records from Internet. *Punch Newspaper*, pp.8

Sunday Punch (2011, March 6). Selling cyber crime with passion. *Sunday Punch Newspaper*, pp.12-13

Tiemo, P. A., Bribena, E., and Nowosu, O. (2010). Internet usage and regulations in Niger Delta University Libraries. *Retrieved on 20th September 2015 from Chinese Librarianship: an International Electronic Journal*, 31. URL: http://www.iclc.us/cliej/cl31TBN.pdf.

Tripahi, U. M. (2015). Types of cyber crime which must be avoided. Retrieved on 12th August, 2015 from http://utsavmtripathi.hubpages.com/

Ujumadu, V. (2008, April 3). EFCC arrest four internet fraudsters. *Vanguard Newspaper,* Pp.14.

Yusuf, A. (2012, September 10). The ugly face of face book. *Tell*, pp. 20