Article

7

The Challenges faced by Criminal Justice System and the Role Players in Combating Cybercrime in Nigeria

Chiji Ezeji, PhD[1]

Abstract

Cybercrime is a new wave of criminality confronting the law enforcement clusters of the world. The modus operandi of cyber criminals is different from those of conventional thieves and fraudsters. It is a new area of crime that many law enforcement agencies are ill-equipped and under-funded to deal with. The rapidity of innovations in the computer era also makes it extremely difficult for investigators to catch up with criminals who exploit the net for their nefarious ends. The Criminal Justice of Nigeria and its counterpart in other nations are faced with challenges of cybercrime which includes jurisdictional problem; the borderless space of the internet, when a crime is committed on the internet the question arises as to which national legislation should be used to investigate and prosecute the perpetrators? Therefore, it is crucial that the criminal justice of Nigeria adopts proactive measures in detecting and preventing cybercrime, thereby enhancing reduction of the victimization of law abiding citizens. The paper adopted qualitative method. Interview technique was used in obtaining data from twelve carefully select-officials of the Nigeria Police Force forensic unit, detective unit, crime prevention and investigative unit. The officials were selected because of their expertise in the research topic. Amongst the following are the findings: the paper identified the simplicity of the network, the anonymousness of the users of the World Wide Web makes it difficult to trace the criminals, and cyber criminals impersonate others by using the password of such persons to enter network for criminal purposes. The challenges associated with electronic banking and commerce is that criminals use encryption to conceal evidences, thus, requiring the law enforcement agents to decrypt such evidences before using them for investigations and prosecutions. The following recommendations were suggested in this paper : the law enforcement agencies should establish a regime of constant training and retraining for their operatives, including computer crime detectives, preventers, and investigators. There is an urgent need for more globally coordinated action against cybercrime just as there is need to establish a working group of experts to address cybercrime problems in Nigeria, as well as need to organize various national/international

[1] Chiji Ezeji, PhD is with the Department of Criminology and Security Studies, Caleb University, Imota, Lagos, Nigeria, +2349016127010 clezeji@gmail.com

conferences and seminars on cybercrimes so that best practices can be shared.

Keywords: Combating, Cybercrime, Criminal Justice System, Phishing, Nigeria, Role Players, Detection, Prevention, Investigation, Prosecuting and Techniques

Introduction

The Nigerian community is increasingly relying on the internet and related information technology tools for personal usages, communication, conducting business activities and other benefits. While these developments allow for enormous gain in productivity, efficiency and communication, these tools could be used by criminals to orchestrate various nefarious activities, engage in the destruction of organizations and individual rights and privacy, property and national assets (Wolfpackrisk, 2018). The rapid growth of the internet and its wide acceptance globally has led to victimization of users and poses serious security threats, both in Nigeria and globally as there have been incidences of different internet enabled crimes known as cybercrimes, frequently committed daily in form of fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime poses threats to various institutions and people who make use of the internet either through their internet enabled computers or mobile devices (Symantec Cloud Intelligence, 2019).The escalation of incidences of cybercrime in the society is condemnable and must be addressed properly. Cybercrime has adverse effects on peoples' lives, including socio-economic condition of the nation and its international reputation. This paper focuses on identifying challenges facing criminal justice system and the role of players in combating cybercrime in Nigeria. Detection, prevention, investigation, and prosecuting techniques are highlighted to enhance effective tackling of cybercrimes in Nigeria.

Research Problem

Lack of skilled experts hinder effective management of applications related to cyber security while inadequate protection from attacks due to internal and external influences (personnel) may create vulnerability within public/private organizations and governmental departments. External attacks are on the rise and have been causing extensive damages to companies and organizations in Nigeria. There are cyber-criminal organizations and syndicate groups in Nigeria and outside its borders that cause damages to individuals, corporate organizations and government offices in the form of extortion, blackmail, spreading of viruses, DOS, malware and ransom ware attacks directed at their targets. Phishing seems to be the most common cyber invasion targeting most sectors in Nigeria. Inadequate control and abuse of systems privileges are other cyber risks faced by Nigeria's financial sector and some government ministries.

Others include malicious software (malware) attacks which seem prevalent in Nigeria and are used in creating support systems to conduct specific cybercrimes such as Denial of Service. Malware is distributed by the social media. This has also become a popular means of attack. Malware is prevalent and has been detected where incidences of information theft or espionage takes place. Cyber criminals make use of techniques such as malicious software and viruses that attaches itself to normal files and consequently reproduces itself to cause damages to a computer system or network. Other techniques such as Worms, Trojan and Backdoor programmes are also used to gain access to a computer system or network at a later date or time. Viruses and malicious software can also be transported by cyber criminals; through a variety of mechanism like emails. E-commerce fraud is also predominant in South Africa. This involves criminals making use of internet and computer networks to defraud victims by posting items that do not exist, thereby deceiving people and defrauding them of their money (Kovacich & Boni, 2016). According to Deloitte Cyber Security (2019), there is an increase in identity theft which involves the use of email or web pages to convince victims to reveal their personal or financial information and the stolen information is used to further perpetrate other crimes. Web hacking crimes used by criminals to deface government or corporate websites has risen. This act is conducted to embarrass and to prove the insecurity of an organisation or government. Hack-tivism, another major cyber-crime is an act by hackers which involves the use of computers and the internet to conduct resistance against a government or cooperation. Hacktivists conduct DOS attacks, intrusion, and web defacing to make a point in their political views. Ezeji, (2018) reports that cyber espionage involves the utilization of computers to aid the act of stealing sensitive information; these activities are mostly sponsored by a state or other corporation attempting to damage a rival company. Therefore, the problem this study focuses on is the exploration of the impact of cyber-attacks on individuals, organizations and government institutions and the challenges confronting criminal justice and law enforcement clusters in combating, detecting, preventing, investigating and prosecuting cybercrime in Nigeria.

Research Objective(s)

This study examines the challenges confronting the criminal justice and law enforcement clusters in the combating, detection, prevention, investigation, prosecution of cyber criminals in Nigeria. The subsidiary objectives are to:

- identify the role players in cybercrime detection, prevention and investigations;
- ascertain the challenges confronting the criminal justice officials in the investigations and prosecutions of cybercrime;
- identify the incidences and seriousness of cybercrime in Nigeria; and
- advocate clarity on law/legislation with regards to cybercrime in Nigeria.

Conceptual Framework/Literature Review

Concept of Cyber Crime

Cybercrime is the criminal usage of computer network or systems for criminal purposes. It also refers to any crime that involves a computer and a network. The computer may have been used in committing a crime or it may be the target. It can also be described as crime committed on any internet enabled device. Net crime refers to criminal exploitation of the internet (Ezeji, 2018).Thomas and Loader (2015) use the term "cyber-crime to refer to computer related activities which can be carried out by global electronic networks which are either illegal or are viewed as such by some parties (examples of cyber-crimes are classified as Hackers). Cyber hackers also known as computer tinkerers are people who enjoy computer as a hobby or professionals who frequently have illegal or unauthorized access to computer systems and cause damages to the systems or information contained in the system. The Electronic Communication and Transaction Act 25 of 2002, seeks to introduce statutory criminal offences relating to information system and includes: Unauthorized access to data interception of or interference with data, computer-related extortion, fraud; and forgery. Hi-tech crime is the illegal usage of information and communication technology against persons, property, organizations or networked computer system (ECT Act, 25 of 2002).

According to the Nigeria Cybercrime Bill, 2013, Cybercrime could be defined as any illegal activity that uses a computer as its primary means. It also includes any illegal activity that uses a computer for the storage of evidence. Cyber-crimes include crimes that have been made possible by computers, such as network intrusion and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism. This bill also provides measures towards safeguarding the nation's presence in cyberspace while ensuring protection of critical national infrastructure. Furthermore, the bill provides for the prohibition, prevention, detection, response, investigation and prosecution of cyber- crimes and other related matters (Vanguard Newspaper, 2014).

Cyber Crime Prevention Theories

According to the stipulation of United Nations, crime prevention must be properly planned and evaluated in order for it to succeed. The programme should be cost effective and the following should be taken into consideration: the socio-economic, political and cultural settings and circumstances of the community within which it is being implemented; the development phase in which the community finds itself, with special reference to changes taking place or that may take place and the particular traditions and custom of the community (United Nations, 2017).

In the Nigerian context, cyber related crime prevention programmes should be properly planned, especially now that recent innovations and technological advancements have added shifts in the method of orchestrating criminal activities such as the crimes committed in the cyber system. It is necessary that when crime prevention programmes are planned, consideration should be given to cyber-crime because of its dynamic nature (Ezeji, 2014). Louw (2017) postulates that in order to plan and implement successful cybercrime prevention programmes, the following steps should be adhered to: Phase one entails conducting of safety audit which should start by identifying specific crime prevention strategy through information gathering from different sources, identifying the institutions already involved in crime prevention, analyzing the physical and social characteristics of the environment, decide which crime problems have the highest priority and ensure that the contributing factors causing crimes are identified. In step two, the following crime prevention strategies should be developed: selecting and grouping of the prioritized into focus areas, identifying probable solutions for the prioritized crimes, identifying of partners who can help with the implementation, selection of the most appropriate programme and refining it, and getting support for the planned programme from local and provincial authorities, the police and relevant organizations. In phase three, the strategy should be managed and implemented; programmes should be developed with specific goals, time frames and budgets, ensure that there are sufficient funds to manage programmes. Phase four involves monitoring and evaluation; there is a need to ensure that monitoring and evaluation are budgeted for, ensure that the objectives of the programme are clearly set out, identify techniques for evaluating the success of the programme and develop a framework for evaluation (Louw, 2017).

In support of the above assertion, Pease (2016) pointed out that effective cybercrime prevention strategy involves identifying an appropriate prevention programme, implementing the programme and evaluating the effectiveness of the programme. Furthermore, effective cybercrime prevention requires collaborative efforts between the criminal justice role players, who must also adopt proactive and intelligence based policing strategies to enhance the effective prevention of cyber- related crime.

Investigation of Cybercrimes/Applications of Investigative Principles

Criminal investigation can be defined as a systematic search for the fact with the primary purpose of finding a positive solution to the crime with the help of objective and subjective clues. Van Heerden (2017) describes objective clues as the factual proof and subjective clues as the evidence offered by people that is, victims, complainants, eye witnesses and culprits who are directly or indirectly involved with the crime. During cybercrime investigation and detection a thorough search must be initiated which includes extensive search of each cyber system/computer terminals or servers and all computer related hardware and software. Obviously, the investigator must ensure that cyber system/computer contents are identified in his or her search warrant documentation. During the search for information, evidence may be found in hard drives, compact disks, tape drives, local area network servers, and magnetic tape, or backup media. If a computer has a fax/modem, evidence may be held in any data with which the computer has interfaced. Investigators should take caution in applying the above principles, so potential evidence are not compromised or lost during investigations (McEwan, 2017).

McEwan (2017) asserts that a comprehensive search is not restricted to locating and seizing physical objects. Evidence may be in the form of corroborative and peripheral evidence which would assist in creating or supporting the suspect's personality, frame of mind or state of paraphernalia. However, in ordinate security or secrecy paraphernalia, suspicious absence of things one would expect to find look for what is there and what is not there. When investigating a crime committed via network and telecommunication devices, the investigator should have in mind that criminals may launch an attack for various reasons such as trading and sharing information e.g. documents, photographs, movies, sound files, texts and graphic files, and software programmes. Furthermore, cybercrime perpetrators may conceal their identity, assume another's identity, identify and gather information about the victims, distribute information, coordinate meetings with the members in anticipation to launch attacks on victims. Sources of information needed in the investigation of a case may be located anywhere in the world and may not be readily available to the investigators. Such evidence include: the computers of both the victims and suspects data and records on the work stations/servers/routers of the third parties such as businesses, government entities and educational institutions and internet service providers.

Moreover, investigations vary in scope and complexity, evidence of cybercrime may be found in the electronic devices in numerous jurisdictions and may encompass multiple suspects and victims. Complex evidentiary issues are frequently encountered on the internet and networks investigations. Therefore, investigators must be very cautious when searching for cyber-crime evidence (McEwan, 2017).

Crime Scene in Cybercrime Investigation

During cybercrime investigation, the investigator should not be in haste rather, should ensure that the investigative procedures are complied with. Investigators should be aware that the internet enabled device or a computer may hold untold amount of related information (Kopelev, 2017).

In any cybercrime scene, if the investigator or detectives are not computer compliant, an Information Technology (IT) specialist who is willing to help, might be contacted for his or her expertise to help extract evidence. Casey (2016) argues that obtaining evidence in respect of cyber related crimes, interviewing and interrogation techniques are basically the same as for other crimes. The major difference is in the types of evidence involved. Casey (2016) warns that "the biggest difference between traditional evidence is its tangible evidence. Cybercrime evidence itself is fragile, electronic evidence can be altered, damaged or destroyed simply by turning the computer on or off at the wrong time." The researcher opines that investigators should be cautious when handling fragile evidence to prevent evidence loss and contamination.

Research Methodology/Justification of Participants and methods of data interpretation

This paper adopted qualitative method using interview techniques as method of data collection. About twelve carefully-select officials of the Nigerian Police were interviewed. They include three high ranking officials from forensic unit; three officials from the detective unit; three officials from crime prevention unit; and three officials from crime investigating unit. The above participants were selected because of their vast knowledge in the research topic. After data collection, the responses of the participants were recorded on the tape recorder and translated verbatim.

Findings and Discussions

Role Players in Addressing Cybercrime

According to Van Heerden (2017), the cybercrime investigator is required to safe keep and identifies the physical evidence (e.g. computer, cyber system) which was used in committing the crime. If the investigator fails to safe keep the computer used in committing the crime, the evidence would be tampered with and may not be admissible in court. Continuity of possession begins as soon as physical evidence has been found at the scene of the crime and persists until the article is produced as evidence or proof in the court, and the handling, and handing over of samples and their return after scientific analysis.

All the respondents agreed that the Nigerian Police Act provides that the investigator(s) gathers evidence during investigation, collects necessary and available information regarding the crime. An investigator's duties include: communicating with witnesses and prosecutors processing the crime scene and assisting in preparing cases for court proceedings, identifying and tracing witnesses, identifying and tracing suspects, individualization of crime, taking statements to prove the case, preparing dockets for court, arresting and charging suspects and assisting in the prosecution

Three respondents (R 4,7, 9) from the forensic unit of Nigeria Police stated that the objectives of an investigation are: identification of the crime and perpetrators, collecting and preserving evidence in a systematic and legal manner, individualization of crime, arresting criminals, recovering stolen properties, involvement in the prosecution process by preparing witnesses for trial and assisting the prosecutor, solving crime by establishing who, what, when, why, where and how the crime was committed, and also ensuring that all statements are obtained and all exhibits are properly secured.

The New Shorter Oxford English Dictionary defines cyber/computer forensic:

> as the application of forensic science techniques to computer based materials. In other words, forensic computing is the method of identifying, preserving, analyzing and presenting digital evidence in a way that is up to standard for legal proceedings. The use of the science is, in the opinion of many, one of the best ways in which cyber-crime and computer enabled abuse can be combated (Oxford Dictionary, p. 342).

Van Rooyen (2018), points out the procedures that should be followed by computer forensics in the recovery, collection, examination and analysis phases. The three "absolutes" for forensic investigators handling computer evidence include certainty, no changes should made to the information, take precautions while gathering evidence, the original evidence (is actually seized) should never be examined before a bit-level image has been made. Computer forensic experts should be able to testify technically to the integrity of the evidence. In support of the above view point, a respondent (R3), asserts :

> the attribute of digital computer evidence; (digital evidence) can play a direct role in identifying and apprehending offenders, thus helping investigators establish linkages between people and their online activities. These attributes when combined with traditional investigative techniques can be helpful in providing necessary clues to tracking down offenders.

A respondent argues that attributing cyber activities to a particular individual can be challenging. For example, logs showing that a particular internet account was used to commit a crime do not prove that the owner of that account was responsible for the commission of the crime as someone else may hack into his account and use it for criminal activities. The responder suggested that when dealing with specific suspicious activities emanating from the computer or cyber systems, it is necessary that forensic experts use forensic investigative steps/tools to place the person at the key board and confirm that the activities on the computer were those of the suspect. Respondent (R12), states :

> The National Prosecuting Authority Act provides that during the process of prosecution and adjudication cybercrime, the decision to prosecute depends on whether there is sufficient and admissible evidence in providing the reasonable prospect of a successful prosecution and establishing a prima facie case. If evidence to prosecute

> is insufficient, the prosecutor would request for further investigation from the police. If there is adequate or sufficient evidence the prosecutor may decide to institute criminal proceeding, decide on the charge, decide whether or not to oppose bail, decide to withdraw the charges/stop the prosecution if evidence is not reliable.

Digital evidence can help answer questions in an investigation ranging from the whereabout of a victim at a given time to the state of mind of the offender. It is necessary that evidence on computers and networks be included (whenever feasible) in crime reconstructions. Investigators must be careful when interpreting the abstracted behavioral evidence that is stored in computers (Van Heerden, 2017).Respondent (R9), states :

> "when dealing with cyber-related issues, it is necessary to seek corroborating evidence from multiple independent sources. The risk of missing or misinterpreting important details highlights the importance of utilizing the scientific method to reach objectives."

Challenges to Criminal Justice System /Law Enforcement

The government's non provision of basic amenities such as jobs; health, transportations, safety and security for her citizens have indirectly led to a high rate in cybercrime. There is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should be strictly adhered to (Deloitte Cyber Security, 2019).Furthermore, respondent (R11), states:

> "cybercrime can only be reduced, cannot be easily and completely wiped out, However, collaborative efforts of individuals alongside with government intervention could go a long way to minimize it to a reasonable level"

Majority of the interviewees agreed that some of the problems confronting the law enforcement and criminal justice in addressing cybercrime is jurisdictional challenges; they pointed out that internet is a borderless space and cybercrime can be committed from any cyber system place in the world. Another difficulty they pointed out is the simplicity of the network because the internet is easily accessible. Respondent (R2) from the crime investigation unit asserted that:

> "The problem confronting criminal justice officials in addressing cybercrime is the anonymousness of the users of the World Wide Web, criminals on the internet are difficult to trace in view of the fact that the users of internet are anonymous."

Most of the respondents were of the opinion that the challenges come from money laundering and tax evasion. Electronic banking and commerce afford ample opportunities for criminals to launder funds derived from fraudulent activities and evade payment of taxes on taxable goods bought or sold, because records are not kept for tax regulators to verify. Respondent (R4) asserts:

> "The criminal justice is faced with the challenges of encryption; encrypted information prevents third parties from getting access to information that is not meant for them, criminals use the same means to conceal evidence, the law enforcement agents have to decrypt such evidences before making use of such evidences for investigations and prosecutions."

The researcher argues that cybercrime is a new wave of illegality confronting the law enforcement agencies of the world and the modus operandi of cyber criminals are different from that of conventional thieves and fraudster. It is also a new area of crime that many law enforcement agencies are ill-equipped to deal with. The rapidity of innovations in the computer industry makes it more difficult for investigators to catch up with criminals who exploit the net for their nefarious ends.

Incidences and Seriousness of Cybercrime in Nigeria

Majority of the interviewees stated that cybercrime incidences have risen in Nigeria due to the fact that most people engage in online activities for different purposes. They also stated that a large number of them are internet addicts who cannot control themselves because of their social relations and interactions between them and their groups. They also pointed out that there is an increase in reports of intimidation, harassment, intrusion, fear, and violence experienced through information technologies, hacking, spamming, identity theft, child pornography, cyber bullying, and cyber stalking.

Respondent (R5) pointed out that cyber criminals have targeted select-individuals, organizations and the government. Cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. The intention of cyber criminals is to cause damage to the reputation of the bank by denying service to users, sabotaging data in computer networks of organizations.

Most of the respondents agreed that there have been increase in scams relating to bank verification number (BVN). Biometric identification system was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimized. It was detected that fake and unauthorized text messages and phone calls have been sent to various users demanding personal information such as their account details, phishing sites were also created to acquire such information for fraudulent activities on the bank account. Respondent (R8) who is a senior investigator in the forensic unit of NPF pointed out that:

> "Implementation of BVN in Nigeria has afforded the fraudsters, opportunities to extort money and to carry out other fraudulent activities."

All the respondents agreed that phishing scams have become one of the fastest growing cybercrimes in Nigeria. Fraudsters have devised means to mimic authorized organizations and retrieve confidential information from clients. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. They believe that another wave of cybercrime threatening Nigeria's economy is that fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM.

Respondent (R9), a high ranking Nigerian Police officer, report:

> "A method known as ATM skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card magnetic strip whenever a customer uses the machine."
>
> Most of the interviewees pointed out that internet order frauds involve fraudster, inputting stolen cards numbers on the online commercial sites to order goods. They pointed out that credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Hacking is predominant in Nigeria, hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs.

All interviewees agreed that E-commerce is greatly threatened by the rapid increase of e-crimes. They were of the view that there is an increase in software piracy (Intellectual Property Theft), Cybercriminals make money from illegal sales of pirated copies of software and even go as far as providing cracks for pirated software. The internet has created a platform for almost anonymous, free and illegal distribution of pirated materials in Nigeria. Some of the respondents agreed that there is increase in Data and Airtime Time (DAT) theft from service providers and it is a very rampant scam among the youths of today. They were of the view that the educational sector in Nigeria suffers greatly from electronic crimes which are perpetuated mostly by students in tertiary institutions. They pointed out that cyber plagiarism is prevalent which is an act of alteration of peoples idea without citing the author, copying and pasting online sources into word processing documents without reference to the original writer /owner. Respondent (R4) from the detective unit of NPF, pointed out;

"Cyber-pornography is predominant in Nigeria. It is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults."

All the interviewees converged that most of the social networking sites such as Facebook, Twitter, LinkedIn, WhatsApp and Instagram serve as fertile grounds for cybercriminals who use the platform to launch new attacks. They reported that fraudulent people host fake social network pages for charity soliciting for money and are involved in cyber-stalking, harassment and blackmailing as well as scam. Threatening and blackmailing are also carried out on the internet by fraudsters against targeted victims. According to one respondent from the crime prevention unit of NPF:

> "Social hijacking is a major crime all over the world, many social networking pages have been hi-jacked by hackers who demand money in turn for releasing the personal social page. These fraudsters go as far as sending messages from the authorized page to friends and family requesting for money or any other kind of assistance."

Law/legislation use in addressing cybercrime in Nigeria

Nigeria Cybercrime Bill, 2013, provides measures towards safeguarding the nation's presence in cyberspace while ensuring protection of critical national infrastructure. Furthermore, the bill provides for the prohibition, prevention, detection, response, investigation and prosecution of cyber-crimes and other related matters (Vanguard News, 2014).

All the interviewees converged that the Constitution of Federal Republic of Nigeria 1999, provides that the objectives of the police services are to prevent, combat and investigate crime and to maintain public order, protect and secure the inhabitants of the republic and their property; and to uphold and enforce the law. Moreover, a respondent noted that public laws govern relationships between states and examples of such laws include the law of peace and war, international treaties and international organization such as the United Nations. This means that public law has to do with the relationship between the state and the subject, as well as with the relationship among citizens. Criminal law forms part of public law, i.e. those norms which have a bearing on the relationship between government (state) and subject.

Majority of the interviewees agreed that imprisonment should be imposed on cybercrime offenders, and the punishment should be proportionate to the offence committed; punishment should be specific; and the same goes for fines. They pointed out that if a penalty clause provides for a fine or imprisonment, the court has discretion to impose either a fine or imprisonment.

According to Ewepu (2016), a bill was passed in 2015 which provides for the protection and punishment of offenses committed on the electronic system, including fraud and other cyber related crimes. The full implementation of the bill brings a strategic approach to addressing cybercrime. The highlights of the bill includes a-seven-year jail term for offenders of different types of computer related fraud, computer related forgery, cyber pornography, cyber-stalking and cyber-squatting. The Bill defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. The bill also provides for a legal framework to punish cyber criminals thereby protecting and improving electronic communication. The bill specifies all cyber related criminal acts and provides guidelines for the investigation of such offences. The bill, if effectively enforced, will deter and penalize all cybercrime perpetrators, thereby helping in reducing incidences of cyber-crimes, and restore customer's confidence while transacting business online, just as it will also correct the negative impression about Nigeria and the citizens.

Recommendations/ Conclusions

There is need for the Criminal Justice cluster to adopt proactive measures in addressing cybercrimes in Nigeria. There is need to establish a regime of constant training and retraining for the Law Enforcement/Criminal Justice Operatives. Law Enforcement/ Criminal Justice must be equipped with knowledge for tracking cybercrime perpetrators. More globally coordinated action is needed by local and international Law Enforcement/ Criminal Justice to tackle cybercrime related issues. There is need to encourage multinational initiatives in addressing cybercrime. Training courses should be organized for computer crime investigators and training materials provided for ordinary police officers as well as for computer crime specialists. International conferences need to be organized so that best practices can be shared. Preventive measures should be put in place to control the possibility of victimization and cyber abuse. Proactive and intelligence based policing should be adopted for combating cybercrime. It is necessary that the criminal justice system beef up the training of officials who can combat cybercrimes. Nigeria should develop and enhance cyber-intelligence and cyber security measures in order to predict cyber-related threats and deter criminals. The public should be enlightened. It is important that public awareness be raised about information security by encouraging family members to use multiple accounts per person while using non- administrative accounts for day to day activities. When using wireless connections it is advised to make use of robust passwords, use strong security supported wireless devices and not wireless devices that are vulnerable to attacks.

The installation of anti-spyware programme is necessary, and so, universities and tertiary institutions should play a vital role in educating learners. The ministry of education should consider integrating cybercrime awareness into the school curriculum and initiate weekly cybercrime/

social media network campaign in schools around Nigeria. The legislature should enact strict legislation and initiate international cooperation to enhance effective tackling of cybercrimes. The media should follow a concise approach in their report rather than exploiting the fear of ordinary public. Training should be initiated at local police stations to ensure that police officials from early entry constable acquire basic cyber-related crime prevention and investigative skills as well as how to identify, classify and open dockets for computer related crimes. The Government should consider funding of cybercrime researches. Individuals, on their part, should ensure proper security controls and make sure they install the latest security up-dates on their computer systems.

References

Casey, E. (2016). *Digital evidence and computer forensic science, computer and the internet.* (3rd ed.) London: Academic Press.

Deloitte Cyber Security. (2019). *Barometer of cybercrime and analysis of cybercrime.* Retrieved on December 15, 2019 from https://www2.deloitte.com/ng/en/pages/risk/solutions/cyber-security-services.

Electronic Communication and Transaction Act. (2002). *Electronic communication and transaction Act*. The Act that deals with cybercrime and digital evidence. Pretoria: Government Printer.

Ewepu, G. (2016). *Nigeria loses heavily annually to cyber-crime*. Retrieved 12, November, 2019 from http://www.vanguardngr.com/Nigeria-losesn127bn-annually-cybercrime.

Ezeji, C. (2014). *Combating cyber related crimes in South Africa.* Pretoria: Tshwane University of Technology.

Ezeji, C. (2018). Overview of intelligence led policing and crime prevention. Pretoria: Tshwane University of Technology.

Kopelev, S. (2016). *Cracking computer code law enforcement technology*. (5th ed.) Thousand Oaks, Calif: Sage.

Kovachich, G. & Boni, W. (2016). *High technology crime investigators hand book*: Boston: Butterworth Heinemann.

Louw, D. (2017). *Mentoring children guilty of minor first-time crime methods strength and limitations.* (5th ed.) Bloemfontein: Van Schaik.

Mcewan, L. (2017). *Cyber cops, law and order*. (4th ed.) Pretoria: SARP Press.

Mcneil, J. (2016). *Complementary method in education research*. (6thed.) Colorado: Lawrence Erlbaum.

Moore, E. (2011). *Cybercrime investigating high technology computer crime*. (3rd ed.)

Cincinnati, Ohio: Anderson Publishing.

NCPP, Act. (2015). *The Nigerian Cybercrime Prohibited and Prevention Act*. Legislation addressing cyber-crime prevention, detection and prosecutions.

Oxford Dictionary. (2019). *New shorter Oxford English dictionary*. (p. 342). Oxford: Oxford University Press.

Pease, K. (2016). *Crime concentration and its prevention*. Leicestershire, UK: Springer International Publishing.

Symantec Intelligence Reports. (2019). Information on cyber-crime. Retrieved on 27, July, 2019. from www.symantec.com.

Thomas, D. & Loader, B. (2015). C*ybercrime in the information age*. (2nd ed.) London: Sage Publication.

United Nation. (2017). *Compendium of United Nation standards and norms in crime prevention and criminal justice*. New York: United Nations.

Wolfpackrisk. (2019). *Information on cyber-crime*. Retrieved on 27, July, 2019 http://www.symantec.com

Van Heerden, M. (2017). *Parole board administrative action*: An encroachment on decision of the court of law of South Africa. Pretoria: UNISA.

Van Rooyen, H. (2018). The practitioner's guide to forensic investigation in South Africa. Pretoria: Henmar Publication.

Vanguard News Nigeria. (2014). Senate passes legislation on cybercrime. Retrieved 12, October, 2019 from http://www.vanguardngr.com