

CYBERCRIME IN NIGERIA

Okonigene Robert Ehimen, Adekanle Bola

Abstract

In this paper we investigated cybercrime and examined the relevant laws available to combat this crime in Nigeria. Therefore, we had a critical review of criminal laws in Nigeria and also computer network and internet security. The internet as an instrument to aid crime ranges from business espionage, to banking fraud, obtaining un-authorized and sabotaging data in computer networks of some key organizations. We investigated these crimes and noted some useful observations. From our observations, we profound solution to the inadequacies of existing enabling laws. Prevention of cybercrime requires the co-operation of all the citizens and not necessarily the police alone who presently lack specialists in its investigating units to deal with cybercrime. The eradication of this crime is crucial in view of the devastating effect on the image of Nigeria and the attendant consequence on the economy. Out of over 140 million Nigerians less than $5 \times 10^{-4}\%$ are involved in cybercrime across Nigeria.

Introduction

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud [1]. The advent of digital technology gave birth to modern communication hard-wares, internet service and powerful computer systems to process data [2]. Hence, cyberspace has provided a safe haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavour can now freely access and utilize the advantages offered by internet platform. However, information technology revolution associated with the internet in Nigeria has brought about a new wave of crime. A very few criminally minded youth in the country, who are mostly not educated or graduates, are stealing and committing atrocity through the aid of the internet online business transactions. The internet online business services, which ordinarily suppose to be a blessing as it exposes one to a lot of opportunities in various field of life is fast becoming a source of discomfort and worry due to the atrocity being perpetrated through it. Cybercrime has come as a surprise and a strange phenomenon that for now live with

us in Nigeria. Computer crimes encompass a broad range of potentially illegal activities. Generally it may be categorized into two major groups: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device [3-9]. Nigeria was recently identified as the innocent and ignorant passive player in cyberspace knowledge Olympiad [10]. The capture of Al Qaeda's operative, Muhammad Naeem Noor Khan, provided the Pakistani and American Intelligence Authority with some of Al Qaeda's Internet Communication Strategy. It also identified that Nigerian Websites and Email System were used by Al Qaeda to disseminate internet information. This has once again brought up the pertinent questions of the safety and security of Nigeria's national cyberspace. This paper therefore addresses, from our investigation the aspect that deals with cybercrime based on false pretence or impersonation.

An area that is likely to be fertile to the cyber criminals also called "yahoo boys" is the stock exchange market. Proper mechanism needs to be put in place to control the activities of these criminals in this area otherwise Nigeria economy may be brought down, particularly with trading on the country's stock exchange market going online. Without proper security methods in place, it is just like building a house without locks. Any person can gain access. The category and nature of cybercrime in Nigeria is endless. Cybercrime is a global phenomenal that is threatening the economy of nations. It is a major threat in India as it is in Nigeria. Punjab National Bank suffered a loss of close to Rs. 1.39 crore when the computer records were manipulated to create false debits and credits. In bank of Baroda, Rs 2.5 lakh was misappropriated

through the computerized creation of false bank accounts [11]. In Mahanager Telephone Nigam Limited (MTNL) in Delhi, a junior telecom official was charged for reversing electronic telephone meter system thereby allowing some commercials export houses to make overseas calls without the charges being directed to their telephone numbers.

Materials and Methods

We investigated and carried out a critical review of criminal laws in Nigeria. Also an investigation was carried out on cybercrimes, the social economical consequences, the damage or negative impact it had on the image of Nigeria as a nation. We examined the inadequacies of the existing laws in combating cybercrime and profound solution.

Cybercrime

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the Electronic market is opened to everybody it also includes eavesdroppers and criminals. False pretence, finds a fertile ground in this situation. Some perpetrators of this crime usually referred to in Nigeria as “yahoo boys” are taking advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. They may even pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have become a duped. Merchants who take orders from merchandise on credit are also

facing mounting losses from rip offs. Our investigation revealed that “yahoo boys” also take undue advantage of some people that are looking for spouse through the aid of Internet. These criminally minded individuals usually have discussion with their victims via the internet. These criminals pretend to be interested and loving. And before the victim realizes what is happening, the criminals would have succeeded in cajoling them to send some dollars to enable them facilitate traveling documents. These criminals falsify document and tell all sort of lies to get money from their victims, when their victims begin to suspect fowl play, they will immediately stop interacting with them and shift their target elsewhere. Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols. Specific computer crimes are Spam, Fraud, Obscene or offensive content, Harassment, Drug trafficking, and Cyberterrorism [12].

Extant Laws To Combat Cybercrime In Nigeria

Presently, in Nigeria there is no specific law to combat cybercrime. The criminals are just operating freely without any specific law to checkmate their illicit activities. However, there are laws though not directly related to cybercrimes but in a way can to a limited extent be used to deal with this issue. These laws are: Economic and Financial Crimes Commission (Establishment) ACT 2004, Nigerian Criminal Code. The activities of the “Yahoo boys” are sabotage on the economy of the country. To this extend it constitute economic crimes which Economic and Financial Crimes Commission (Establishment) Act can deal with. Economic crime is defined as; “the non- violent criminal and illicit activity

committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to includes any form of fraud, narcotic drug trafficking, money laundering embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse dumping of toxic wastes and prohibited goods e.t.c” [13]. The other available law is the Nigeria criminal code, which can also presently be used to prosecute these criminals. Most of the activities of these criminals bother on false pretences and cheating which sections 419 and 421 of the Nigerian Criminal Code prohibits respectively. Section 418 defines obtaining property by false pretence as follows; “Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation of false in fact and which the other person making it knows to be false or does not believe to be true, is a false pretence”.

Section 419, provides as follows;

“Any person who by any pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years”.

“If the thing is of the value of one thousand naira or upward, he is liable to imprisonment for seven years”. “It is immaterial that the thing is obtained by or its delivery is induced through the medium of

contract induced by the false pretence. The offender cannot be arrested without warrant unless found committing the offence.”

Discursion

The definition of economic crime referred to above is all embracing. It means the jurisdiction of the Commission covers a wide range of criminal activities including fraud. Fraud, the noun variant of fraudulently, is (i) an action or a conduct consisting in a knowing representation made with intention that the person receiving that misrepresentation should act on it (ii) the misrepresentation resulting in the action or a conduct; (iii) an action or a conduct in a representation made with the intention that the person receiving that misrepresentation should act on it and so on and so forth [14].

A fraudulent action or conduct conveys an element of deceit to obtain some advantage for the owner of the fraudulent action or conduct or another person or to cause loss to any other person. In fraud, there must be a deceit or an intention to deceive flowing from the fraudulent action or conduct to the victim or the action or conduct [15].

An offence is said to be committed fraudulently, if the action or conducts is a deceit to make, obtain or procure money illegally. By the fraudulent action or conduct, the criminal deceives his victims by pretending to have abilities or skills that he does not really have, in one word, he is an impostor.

This is why the Commission has been up and doing to prosecute the perpetrators of this crime. Despite the effort of the commission in this regard, it has been difficult to actually bring these boys to book in view of the complexity of the nature of the crime and investigation that needs to be carried out for proper prosecution of a culprit o this crime. Flowing from the provision of section 419,

false pretence means; knowingly obtaining another person's property by means of a misrepresentation of facts with intends to defraud, Therefore, for the offence of obtaining by false pretence to be said to have been committed, the prosecution must prove that the accused had an intention to defraud and the thing is capable of being stolen. An inducement on the part of an accused to make his victim part with a thing capable of being stolen or to make his victim deliver a thing capable of being stolen will expose the accused to imprisonment for the offence [16].

As it has been noted above, no serious impact has been made by our law enforcement agencies to arrest and prosecute these criminals. Nigeria is a place where computer can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime. The Nigerian police simply lack Internet policing capability. Nigerian law enforcement agencies are basically technology illiterate, they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion. It is very common for the police to demand bribe from cyber café operators that owns sites where suspicious activities are taking place and look the other way. There are so many reports on Nigeria cybercrime situations that well-meaning Nigerians are no longer comfortable with anymore. These reports are damaging the dignity of our country as a sovereign nation. They are humiliating and injuriously affecting our international image, our business, our mental – psychology and even our children.

However, these reports points towards the fact that Nigeria is operating on a weakened technology platform and digitally illiterate environment that is in urgent need of expert solution.

Conclusion and Recommendations

From our investigation on cybercrime we observed its threat to the economy of a nation and even peace and security. Therefore there is need for a holistic approach to combat this crime in all ramifications. Our proposal therefore is the need for cyber police who are to be trained specially to handle cybercrimes in Nigeria. In addition, the police should have a Central Computer Crime Response Wing to act as an agency to advise the state and other investigative agencies to guide and coordinate computer crime investigation. We also proposed that the country should set up National Computer Crime Resource Centre, a body, which will comprise experts and professionals to establish rules, regulations and standards of authentication of each citizen's records and the staff of establishments and recognized organization, firms, industries etc.

Forensics commission should be established, which will be responsible for the training of forensics personnel. Above all a comprehensive law to combat computer and cyber related crimes should be promulgated to fight this "monster" to a standstill. Our proposal on the nature of law to combat cybercrime is not included in this paper. We recommend that before anybody enters into any kind of financial deals with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.

References

- Paul Taylor (in ENGLISH). November 3, 1999 ed. Hackers: Crime in the Digital Sublime. Routledge; 1 edition. Pg.. 200
- Ramjit Singh Hunda, Kawajeet Singh and M. D. Singh. 2004. Aspects to Ensure

- Admissibility of Digital Evidence, Law Journal Gurn Nanak dev University Amritsar, Vol. 13, Pg. 1.
- Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. 2006. (eds) Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York.
- Brenner, S. 2007. Law in an Era of Smart Technology, Oxford: Oxford University Press
- Csonka P. 2000. Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet? Computer Law & Security Report Vol.16 no.5.
- Fafinski, S. 2009. Computer Misuse: Response, regulation and the law Cullompton: Willan
- Grabosky, P. 2006. Electronic Crime, New Jersey: Prentice Hall
- McQuade, S. 2006. Understanding and Managing Cybercrime, Boston: Allyn & Bacon.
- McQuade, S. (ed) .2009. The Encyclopedia of Cybercrime, Westport, CT: Greenwood Press.
- The Guardian Wednesday, July 9, 2008 Pg. 39
- Krishna Kumar. 2003. Cyber Laws, International Property and e-commerce Security, Dominant Publishers and Distributors New Delhi.
- Telephone Consumer Protection Act of 1991
- Section 40 of Economic and Financial Crimes Commission (Establishment) Act 2004.
- Bryan Garner. A Dictionary of Modern Legal Usage, 2nd Edition pg. 374
- Kettlewell Wastson (1882) 21 Ch.D 685, R. V. Reigles (1932) 11 NLR 33; Wellham V DPP (1960) 44 Cr. App. R.
- Onwudiwe V FRN (2008) Vol. 6, LRCNCC pg. 334.