Cyber Crimes: Bane of Nigeria's Information Growth and Utilization

Nkechi Anthonia Idoko (Ph.D)[1] & Richard N.C.Ugwuanyi (Ph.D)[2]
Nnamdi Azikiwe Library, University of Nigeria Nsukka
nkechi.idoko@unn.edu.ng[1] nrcugwuanyi@yahoo.com[2]

Abstract:

Objective: This paper identified and discussed the causes and the negative consequences of cybercrimes on the polity of Nigeria. In addition, the paper has the objective of proffering solutions to the threats being posed against information growth by cybercrimes.

Methodology: An exploratory approach was used for this study. First, a conceptual framework was discussed, followed by the examination of the types, causes and effects of cybercrimes.

Findings: The paper found out issues like unemployment, curiosity to learn, and the advent of information communication technology as the factors behind the emergence of cybercrimes. It also found out world-wide neglect of information originating from Nigeria, discouragement of creativity, and insecurity of financial firms in the country as the impact on the polity. Recommendations for vitiating the negative effects were given before the conclusion.

Practical Implication: National information growth and utilization is endangered in an environment where there are no government and public coordinated attacks against cyber criminals. If left unattended to, Internet use will breed information literate criminals who use cyberspace only to do mischief and create disharmony**.**

Originality/Value: The value of this paper lies in its identification and discussion of the types, causes and consequences of cybercrimes in Nigerians' efforts to build a viable information nation. Another value lies in its articulation of the imperatives and innovative strategies for decimating the negative activities of the *i*nternet users in Nigeria.

Type of Research: This study is a conceptual work that discoursed technological development in Nigeria and the birth to social media which in turn has both positive and negative effects on the populace.

Key words: cybercrimes: cyber space: internet abuses: information users.

Introduction

The advent of information communication technology has so wonderfully impacted on the lives of the people of Nigeria that their traditional ways of doing things have radically changed. It has aided communication, constricted the world into a global village and made possible the globalization of knowledge, collaborative research, crimes and criminology. With the appearance and utilization of internet technologies one knows and views live what happens in other parts of the world-good or bad. Information transmission becomes precise and instantaneous.

Internet is made up of millions of computers linked together around the world in such a way that information can be sent from one computer to any other 24 hours a day (Eyitayo, 2008). It is one of the fastest ways of reporting research findings to the world. Latest information needed by researchers is often found in the Internet

while examinations can be conducted through the Net and results released through the same means (Ezeani, 2010).

Even though Nigeria, vis-à-vis other African countries, entered late into modern communications technology, she was not left out in the present rattle race to get highly hooked to the Net in order to understudy and manipulate its negativity and usefulness. Nigerians immediately got neck deep into the knowledge of computer use, and started imbibing other cultures without considering their relevance to the socio-economic development of their country. As Internet enhanced cultural diffusion it equally brought in and perfected many crimes. People learned how to deliver information to any part of the world just at the click of a button.

They learned to bless and to dupe nations, organizations and individuals using computers. Today, every city in Nigeria is quite agog with cyber cafes, and home Internet-hooked computers where people go in to interact with friends. Many go in there for academic activities while others go in to perfect themselves in crimes. Cyber cafes are establishments offering internet services through their computers to the general public. They provide prominent advantages that are quite suitable to fraudsters. These crimes are known as cyber crimes. These are simply crimes committed using computers or committed against computers. Nigerians have so imbibed many of these crimes and perfected in them that their names are making waves globally.

According to Ehime and Bola (2010) and Adetero (2010) there are so many reports on Nigeria cybercrime situations that well-meaning Nigerian's are no longer comfortable anymore with these reports that are damaging the dignity of our country as a sovereign nation. They are humiliating and injuriously affecting our international image, our businesses, our mentalities and psyche.

The impact of these on the people of Nigeria both at home and abroad has become so tremendous that there exists the need to critically examine the consequences with a view to proffering solutions. In doing this, this paper will look at the concept of cybercrimes, their types, causes, consequences, solutions and conclusions.

Conceptual Definitions

According to Kuma (2004) cyber crime is an unlawful act wherein the computer is either a tool or a target or both. In essence, this definition is simple and precise. It sees cyber crimes as crimes committed using computers or against computers Ehimen and Bola (2010) quoted McQuade as stating that computer crime is a criminal activity involving an information technology infrastructure. This includes illegal or unauthorized access; illegal interception that involves technical means of non-public transmission of computer data to and from or within a computer system; data interference that includes 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; misuses of devices, forgery and fraud. This of course is a broad and an all encompassing definition. Ekemezie and Ngene (2004) assert that computer crimes are illegal act committed against computers or telecommunications or the use of computer or telecommunication to accomplish an illegal act. From what have been discussed above, it may be necessary to epitomize that cyber crime has to do with any activity conducted in the cyber space intent on defrauding individual and organizations and/or putting computers out of effective order. Cyber crimes are crimes/evils that arise as a result of growing dependence on computers.

Types of Cyber Crimes

Before the coming of internet technologies, many of the so-called cyber crimes were in existence. They were then committed off line, locally and on mini-scales, examples includes: robbery, rape etc However the advent of ICTs gave them international outlook and popularized them: Internet actually reduced the cost and other barriers in globalizing crimes. According to Early on Technologies (2006) the advent of internet provides the fraudsters numerous advantages like;

- The ability to send out thousands of e-mails daily with minimal financial cost using the addresses harvested by email extractors.
- The ability to gather extensive of contact information using email extractors as opposed to the difficult task of culling contact information from directories in the chambers of commerce in the country.
- The availability of other means of fraud such as credit card scams, lottery scam and many more to engage the time and effort of the fraudsters.

Cyber crimes are those crimes committed against business and non-business organizations, governments and individuals. They are many and of different kinds. This section has been devoted to listing and discussing some of them.

Hacking and electronic trespassing: This crime involves the act of forcefully breaking into organizations, individuals or government computers, using security loopholes or stolen passwords. Their intentions are usually that of stealing money and accessing secret information.

These hackers do a lot of harm to computers and to human beings. They inflict viruses and post deceptive or false information and equally divulge secret information.

Theft of time and information: These kinds of crimes are very common among Nigerian internet users. They very often use their employer's computer time to play games and do all sorts of unlawful activities on the web. These include chatting with dubious intents, posting of provocative and sexually suggestive photographs and online gambling. They divulge organizational and individual's secret and plans for money

Another type of cyber crime is software theft. This involves illegal reproductions of copyrighted software for sale without buying it from the creators of the work. This activity is also called piracy and is akin to making and selling of photocopies of a book as well as duplicating a tape. According to Longe (2004) piracy has to do with the reproduction and distribution of software applications, same movies and audio CDs. This very act being committed using internet not only depletes nation's foreign reserve, it discourages creativity among the intellectual.

Stealing of computer hardware or removal of cellular phones and laptops from ships or offices is yet another type: these crimes are very common among our youths.

Crime of malice and destruction: This cyber crime involves criminals who are much more interested in abusing or vandalizing computers systems rather than profiting from them. The criminals create viruses, worms, logic bombs and Trojan horses to destroy the computer hardware and software.

Another serious and most common cyber crime is the cyber defamation: This arise where internet users use their computers to publish or paste defamatory articles about their friends or foes. They send e-mail containing defamatory and untrue information to so many people with the intention of destroying other persons' character or importance or image.

Other crimes committed in the cyber space include sending of spam mail, spreading of rumours, gossips, false information and viewing of pornographic or blue films.

Causes of Cyber Crimes

Many reasons have been advanced for the emergence and growth of computer crimes. One obvious reason is the magnitude of unemployment among Nigerian youths. As a result of idleness, many young people started to try their hands in everything including cyber crimes. In their desperation they spend many hours in cyber cafes everyday perfecting their evil deeds.

Unquenchable desires to get rich**:** Nigerians have become excessively materialistic especially the youth. They want to amass wealth at a very early stage of their lives. Their excessive quest for monetary gains through crimes has become the bane of many Nigerians at home and abroad. Many including some government leaders become so engrossed in money laundering and other cybercrimes that they are ever ready to reap where they never sowed.

There is hardly curiosity to learn: Many of the people who are today deep into computer offences never did that intentionally. They unknowingly in their interactions with computers and friends ran across them, continued with them, and perfected in them. Sometimes, without profiting from some of these crimes they settle for them and continue to reach out for more sophisticated ways of committing evils.

Malicious desire to destroy: Man has an innate desire to do good and evil. As a result those who are more prone to doing evil maliciously try to destroy by creating and spreading viruses to many computers. They sometimes damage and steal hardware and software for the sake of keeping people unhappy.

The advent of information communication technology**:** The presence of ICTS is equally the cause of the emergence and spread of cyber crimes. Internet has so constricted the world that whatever is happening in any country is simultaneously being observed and practised in Nigeria. This enhances intercultural diffusion. Nigerians have learnt to use email harvesters to get people's email addresses, thereby using them to commit different kinds of computer crimes.

The Effects of Cyber Crimes in Nigeria

The internet online business services, which are ordinarily supposed to be a blessing as they expose users to opportunities in various fields of life is fast becoming a source of worry and discomfort. This is due to enormous atrocities

being perpetrated through it. Cyber crime in any society is an ill wind that blows nobody any good. Its disastrous effects on Nigeria as a developing country are multifaceted and staggering. Corroborating this, Oyesanya (2009) observed that Internet criminal activities originating from Nigeria are fraught with financial and economic impact as international banks often delay Nigerian financial transactions until after due verifications.

Cyber crimes as practiced in Nigeria discourage creativity. Cyber criminals duplicate software and other like productions made by others and sell them without the creators' permission thus removing the creators' financial gain. The financial loss encountered by the creators kills creativity, would not enhance foreign exchange reserve and to bring praise to the creator's country. This is piracy which Longe (2004) described as the illegal reproduction and distribution of software applications, games, movies and audio CDs.

Moreover, these notorious activities of the cyber criminals have greatly destroyed the integrity of Nigerians. This has scared many foreign investors. They doubt the integrity of almost every Nigeria citizen. Foreign investors consider Nigeria as unattractive market due to her fraudulent activities (Oyesanya, 2006). This is very bad for a country like Nigeria.

Banks and other Financial Houses fear hackers from Nigeria as many of them had lost huge sums of money to them. Hackers and crackers are people who gain unauthorized access to computer either to steal money, information or for the joy and challenge of doing so. Nigeria has been rated as one of the most fraudulent countries in the world by many international organizations like the American National Fraud Information Center (2002) and the VeriSign (2003).

Cyber crime has deleterious effects on the flow of information into and out of Nigeria. Information from Nigeria is considered to have been falsified and therefore has to be reviewed and revalidated before use. The one coming into Nigeria is strictly doled out for fear of manipulation. This situation spells doom for the nation's information growth and utilization. Information growth and utilization exists where available information capturing and disseminating network systems are effectively and positively applied for sourcing and disseminating authenticated information to general public without any constraint. Here, there is freedom of information and the correctness of available information is assured. This information may be educational, vocational, social-personal, business transactions, general knowledge, etc. The attitudes of Nigerian "yahoo guys" or 419s (Internet utilization abusers) have so battered information from Nigeria that the international world accepts it only after serious efforts have been made to find out whether there are no hidden meanings attached to it. It will be bad if Nigeria loses information credibility. Cyber private companies around the world are beginning to take steps geared at blocking e-mails originating from Nigerian (Oyesanya, 2007). This is as a result of many cyber crimes being meted out by Nigerian computer users.

Recommendations

From what has been discussed in the preceding sections it follows that the growing rate of internet fraud presents a clear danger to the image and the economy of Nigeria. It therefore constitutes a serious threat to the achievement of her millennium development goals as well as her vision 20:20:20. To be able to eliminate this bottleneck in the progress of Nigeria, all hands must be on the deck. The government, individuals, internet private service providers and corporate bodies must rise to the challenges posed by this monster. In doing this every Nigerian must have to strip off every yoke of affinity, tribe or religion and be able to report any offender to the police for arrest and interrogation.

Corporate bodies, especially those involved in e-business ought to come together, pool resources and be able to protect their internet resources and web sites. They should equally explore all the possible avenues to safeguard their e-operations through appropriate mechanisms. They need to sponsor bills through their legislator-friends or representatives against cyber crimes for an enhanced business.

There is also the need to have some police men trained as cyber police. This is to enable them obtain relevant skills in handling computer criminals. Discussing the role of the police in eliminating cybercrimes, Ehimen and Bola (2006) suggested the creation of Central Computer Crime Response Wing to act as an agency to advise the state and other investigative

agencies to guide and co-ordinate computer crime investigation.

Moreover, the Nigerian legislatives should pass laws with harsh penalties for anybody caught in cyber crime of any sort. This, therefore, presupposes that Nigeria government and its regulatory authorities need urgently to make stringent laws and prescribe punishments due to the offenders. The prosecution ought to be precise without much legal encumbrances.

Conclusion

Cybercrime which is defined as unlawful act where the computer is a tool, a target or both is an ill-wind that blows nobody or society any good. It is a cankerworm that eats deep unto the socio-political and economic fabrics of any nation. Though its causative factors may be found in idleness and unemployment, the anxiety to learn and the joy of seeing others regret by the culprits cannot be left out. Cybercrime has pulled down many states and led individuals and business organizations to a situation where they exist but are not living; where they are beckoning on death to do its inevitable. Cybercrime has jolted the economy of many states like Nigeria and lays it open to international ridicule and shame.

The best a state can do is to be determined and resolve to fight it without any reservation. Governments, corporate bodies and individuals should get involved and committed. All the law enforcement agencies are to spread their dragnets and allow them catch culprits without fear or favour. It is there and then that the individuals, corporate bodies and governments that have been traumatized and bedridden economically by the power of cyber criminals can jump and pass, and sing songs of relief. Surely, the emergence and embrace of the internet culture in Nigeria has come with a lot of mixed feelings.

References

Adetoro, N. (2010). Internet Utilization an Abuse in Selected Cybercafes in Ogun state, *Nigeria. African Journal of Liberary, Archive and Informantion Science*. 20,(1), 19-27.

American National Fraud Information Center(2002).Nigerian Money Offer 4% of total Internet fraud.http://www.fraud.org/2002intstats.htm. Retrieved April, 5th 2012.

Earlyon Technologies Ltd. (2006). Meeting EFFC Anti-Crime Requirements with Earlyon Cafecentra. *Earlyon Cafecentra white Paper. 1-8 Retrieved in January 15th*.

Ehimen, O. R and Bola, A. (2010). Cyber Crime in Nigeria. *Business Intelligence Journal. 3, (1), 94-112.*

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

Eyitayo, O.T. (2008). *Internet Facilities and the status of Africa's Connectivity. Informantion and Management in the Digital Age: Concepts, Technologies, and African perspectives.* Edited by L.O. Aina, S.M. Mutula; M.A. Tiamiyu Ibadan: Third World Information Services Ltd. P.31

Ezeani, C.N. (2010). *Information Communication Technoogy: An Overview.* In Evarest C. Madu and Chinwe Nwogo Ezeani (Eds.) Modern Library and Information Science for Information Professionals in Africa. Pp.9-31 Ibadan: Text Links Publishers.

Kumar, V.S. (2010). *Cyber crime Prevention and Detection.* New Delhi: A.P. Police Academy.

Longe, O.B. and Chiemeke, S.C. (2004*). Cybercrime and Criminality in Nigeria- What roles can internet Access Points play?*

Oyesanya, F. (2007*). Nigerian Internet 419 on the loose.* Retrieved in February 2012. From Lunarpage.com

Verisign (2003).Countries involved in fraudulent activity, and other malicious internet traffic.http://www.verisign.com/corporate/briefing. Retrieved on 13th May,2012.

Williams, G. (2000). *Student Handbook for Information Communication Technology*, 4th ed. Cambridge: Pearson Publishing.