Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.980 – 991

RESEARCH ARTICLE

Combating the Menace of Cybercrime

Odumesi, John Olayemi
E-Learning Department
Civil Defence Academy, Abuja, Nigeria
olayemijohn@yahoo.com

Abstract- The contribution of internet to the development of the nation has been marred by cybercrime activities. Cybercrime is emerging as a very concrete threat, not only in Nigeria but the globe at large. This study is concern about the Nigeria approach in combating the menace of cybercrime. In order to ensure that this study achieves its aims and objectives, the methodology used for this study involves both primary and secondary sources of legal provisions relating to cybercrime law in Nigeria. Two theories of crime namely, space transition theory and crime opportunity theory were found to be relevant to this study. Five legislations namely, the Nigeria Criminal Code Act 1990, the Economic and Financial Crimes Commission Act 2004, the Advanced Fee Fraud and Other Fraud Related Offences Act 2006, the Money Laundering (Prohibition) Act 2011, and Evidence Act 2011, are the current means used in Nigeria to address cybercrime activities. The study establishes that, the state of legal protection against cybercrime in Nigeria is weak and inadequate to combat cybercrime. Based on the findings on the study, recommendations are made to the Nigeria government, the security and law enforcement agencies on how to combat the menace of cybercrime and ensuring cybersecurity.

Keywords- Nigeria, cybercrime, cybersecurity, legislations, cyberlaw

I. INTRODUCTION

Cybercrime is a global phenomenon and not belonging distinctively to Nigeria. Akano (2013) maintained that, cybercrime does not respect geographical boundary, fighting the menace can only be achieved through partnership with other cyber security organisations and institutions across the world.

Cybercrime has surpassed illicit drug trade as global top revenue earner for organised crimes. The cybercrime network has become a highly organised ecosystem with its own value chain including: researchers of stronger attack methods; hackers who compromise account data and make them available to dump vendors, Lemo (2013). According to him, the industrialisation of cyber fraud poses a great challenge to the cash-less society in Nigeria. He said the prevalence of fraud globally is contributory to the growing technophobia as users were apprehensive for the safety of their funds on electronic payment platforms.

The advent and growth of the internet has not only altered how people interact but has also added a new dimension to criminal activities in the society. Weber (2006) argued that, the computer and the internet provided an additional cloak of anonymity to the perpetrators of cybercrime and making illicit activities much more attractive.

A. Problem statement

Akinsehinde (2011) argued that, over 80 per cent of businesses with online presence in Nigeria are susceptible to cyber-attacks and the increasing spate of cyber-criminal activities was threatening the Nigeria economy. He argued that, web portals and web based applications of the Central Bank of Nigeria, Nigeria Stock Exchange, banks, pension fund administrators and switching/electronic payment companies had been found to be vulnerable to cyber-attacks due to inadequate security measures for safeguarding the platforms.

He lamented that, there are advanced countries with high Internet security measures, yet their systems were hacked. He recalled that the Hong Kong Stock Exchange and NZSDAQ servers were hacked via wed-facing applications. Based on his findings in Nigeria, most businesses including the Central Bank of Nigeria, Nigeria Stock Exchange and banks are vulnerable to hacking and the need to create awareness as we go into a cashless economy by adhering to international security standards.

Azazi (2011) set up a Committee on cybersecurity Legislation to access the Nigeria cyberspace. In the report submitted to the office of the National Security Adviser (NSA), the committee revealed the followings:

1. Nigeria lacks the structures to handle any cyber-attack emergency, with the increase in bomb attacks and growing threat of attacks through computer networks.
2. There is no comprehensive assessment of the preparedness of the country in the event of cyber-attacks.
3. There is no focal point for coordinating cybersecurity in Nigeria.
4. There are no structures to handle any emergency cases of cyber-attacks.
5. The current legal framework is grossly inadequate for cybersecurity in Nigeria and does not support a coordinated approach to developing a cybersecurity strategy.

The committee further revealed that, the challenges in developing a cybersecurity framework to include lack of awareness and jurisdiction overlaps among existing law enforcement agencies. Others are the absence of certification of critical national information infrastructure and the absence of systematic capacity and capability building for law enforcement agencies.

The committee recommended that the office of the National Security Adviser (NSA) should initiate the amendment of the National Security Agencies Act, Cap N74 LFN 2004 to create the Directorate of Cybersecurity; liaise with the Office of the Attorney General of the Federation and Minister of Justice and work with legislators to ensure the passage of the harmonised cybersecurity Bill.

Sorunke (2011) maintained that Nigeria at the cyberspace is under threats, with much vulnerability, many loopholes in our system and with issues bothering on our payment networks. He warned that, if urgent measures were not taken by businesses and government organisations deploying web-based platforms for their operations and with the increasing rate of cyber insecurity in Nigeria; companies might soon be faced with high incidence of hacking, leading to loss of data critical to a business life and revenue.

He maintained that, the high level of insecurity in the Nigeria's cyberspace might affect the cashless economy objective of the Central Bank of Nigeria. He noted that the wanton defacing of some government websites such as the Niger Delta Development Corporation (NDDC), Power Holding Company of Nigeria (PHCN), etc. by a group of hackers known as NaijaHacktivists; in practical terms inform how vulnerable most Nigerian organisations were in the cyberspace.

From the above, it is obvious that the Nigeria's cyberspace is porous and has no form of legal protection to regulate activities in Nigeria's cyberspace. Therefore, the study intends to look at the Nigeria approaches in combating the menace of cybercrime.

B. Objective of the study

The general objective is to highlight the nature of cybercrime and the threat they pose to the effective operations and service in the Nigeria cyberspace.

The specific objectives are as follows:

1. To highlight the reasons, implications and the approaches adopted by the Nigerian government in combating cybercrime and its criminal in the society.
2. To provide an aid in formulating appropriate legal and regulation framework for cyberlaw and ensuring cybersecurity in Nigeria.

C. Methodology

In order to ensure that this study achieves its aims and objectives, the methodology used for this study involves both primary and secondary sources of legal provisions in Nigeria. As regards primary sources, this study examines the various legal provisions relating to cybercrime law in Nigeria. The study also uses case review approach; that is, cases relating to cybercrime in Nigeria are reviewed.

With regards to secondary sources, a review of existing literature on cybercrime in Nigeria including text books, theses, journal articles, newspaper reports, conference papers, seminars and internet materials are considered and relied upon.

II. CYBERCRIME IN PERSPECTIVE – A REVIEW OF CYBERCRIME

Britz (2009) defines cybercrime as abuses and misuses of computer systems or computers connected to the Internet, which result in direct and/or concomitant losses and also criminal activity that has been facilitated via the Internet.

UN Office on Drugs and Crime (2005) defines cybercrime as conduct that entails the use of digital technologies in the commission of the offence; is directed at computing and communications technologies or involves the incidental use of computers with respect to the commission of other crimes.

Sociologically, Cohen and Felson (1979) maintained that, cybercrime is a crime of opportunity committed by a motivated offender against a suitable target under an unguarded condition. Cybercrime is not different from other types of crime (Emanuelsson-Korsell and Soderman, 2001).

Technologically, Brenner (2007) stated, it is the use of computer technology to commit crime. Because of the continuous breakthroughs in Internet technology, cybercrime can evolve into a new generation of criminal acts unseen and inexperienced (Wilson and Shun-Yung, 2009).

Cybercrime can be regarded as computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks (Thomas and Loader, 2000). As such, cybercrime involves crime committed through use of the computer systems. Therefore, computer crime is defined by the Department of Justice (1989) as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution.

This paper will adopt a working definition cybercrime in Nigeria from the sociological and technological aspects of cybercrime. Therefore, it is a crime involving the abuse or misuse of digital resources in a cyber environment on or through the internet, computer networks, computer systems and wireless communication systems.

A. Categories of cybercrime

Adamski (1998) classified computer crimes or cybercrimes as one of two categories:

1. Crimes geared specifically to the network and the related data-processing systems (For instance, offenses against computer and information security).

2. Crimes for which computer networks provide a new opportunity for the commission of traditional offenses (Such as fraud, industrial espionage, and child pornography).

The Council of Europe's Convention on Cybercrime (2001) covers cybercrime in four main categories:

1. Offenses against the confidentiality, integrity, and availability of computer data and systems.
2. Computer related offenses.
3. Content-related offenses (e.g. Child Pornography).
4. Offenses related to infringements of copyright and related rights. (Aldesco, 2002).

Wall (2001) has divided cybercrime into four categories:

1. Cyber trespass: crossing "boundaries" into other people's property and/or causing damage, e.g., hacking, defacement, and viruses.
2. Cyber deceptions and thefts: stealing (Money, property), such as credit card fraud or intellectual property violations (Piracy).
3. Cyber pornography: activities that breach laws on obscenity and indecency.
4. Cyber violence: bringing psychological harm to or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, such as stalking.

Smith, Grabosky, and Urbas (2004) classified cybercrime as that:

1. Involving the use of digital technologies in the commission of the offence,
2. Directed at computing and communication technologies themselves, or incidental to the commission of other crimes.

B. Typology of computer crime

The Department of Justice (1989) maintained that, there are three types of computer-related crimes:

1. A computer may be the object of a crime. This may involve theft of a computer software or hardware.
2. A computer may the subject of a crime. The computer in this category may be the subject for an attack. This category eencompasses all of the novel crimes that have arisen out of the technology explosion including the use of viruses, worms, Trojan horses, logic bombs, sniffers and distributed denial of service attacks.
3. A computer may be an instrument to commit traditional crime. Traditional crimes, including copyright infringement, mail and wire fraud, child pornography, identity theft, and copyright infringement, can be committed by using computers (Jacobson and Green, 2002).

Carter (1995) recognizes four types of computer crimes:

1. Computers as the target: This type of crime is committed when the action prevents the legitimate user from receiving the service (Taylor and Loper, 2003). These types of crimes include theft of marketing information, theft of intellectual property, and they may entail sabotage of personal data, intellectual property, or operating systems (Carter, 1995).
2. Computers as the instrumentality of the crime: Similar to the first typology, this category involves the use of computers as a means to commit traditional crimes (Bakewell, Koldaro, and Tjia, 2001). For example, a computer can be used to collect credit card information for fraudulent purchases.
3. The computer as incidental to the crime: This category of crime is committed when "a pattern or incident of criminality uses a computer simply for ease in maintaining the efficacy of criminal transactions" (Carter and Bannister, 2000). Crimes, such as money laundering and child pornography are examples of this type of crime.

4. Crimes associated with the prevalence of computers: This category of crime involves piracy issues, such as copyright violations of computer software and other misuse of electronic services, including telephone systems.

III. THEORETICAL FRAMEWORK

A. Space Transition Theory

Space transition theory is an explanation about the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and cyberspace (Jaishankar 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another.

The postulates of the theory are:

1. Persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime.
3. Criminal behaviour of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.
5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.
   (b) Associates of physical space are likely to unite to commit crime in cyberspace.
6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.
7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

The space transition theory provides an explanation for the criminal behaviour in the cyberspace. The theory is relevant to this study because it provides us insight understanding of the movement of persons and their characteristics from one space to another (e.g., from physical space to cyberspace and vice versa).

B. Crime Opportunity Theory

Felson and Clarke (1998) argued that opportunity is a cause of crime and a root cause of crime. They maintain that crime opportunities are at least as important as individual factors and are far more tangle and relevant to everyday life.

The theory argued that crimes transverse between location, time, target, direction, and method of committing the crime. The theory posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime (Felson and Clarke, 1998).

The principles of the theory are:

1. Opportunities play a role in causing all crime.
2. Crime opportunities are highly specific.
3. Crime opportunities are concentrated in time and space.
4. Crime opportunities depend on everyday movements of activity.
5. One crime produces opportunities for another.
6. Some products offer more tempting crime opportunities.
7. Social and technological changes produce new crime opportunities.

8. Crime can be prevented by reducing opportunities.
9. Reducing opportunities does not usually displace crime.
10. Focused opportunity reduction can provide wider declines in crime.

The crime opportunity theory provides an explanation on the opportunities technology changes produce and that crime opportunities are concentrated in time and space.

IV. NIGERIA APPROACH IN COMBATING CYBERCRIME

The development of cybercrime and cybersecurity bill legislations and policies began since 2004 in Nigeria. In 2011, the office of National Security Adviser, Federal Ministry of Communications Technology, Federal Ministry of Justice, and other strategic stakeholders re-harmonized a new Executive Bill which has been adopted by National Executive Council in 2013 and already passed to the National Assembly for legislative actions in 2014. The bill is expected to become a law as soon as possible. The bill is substantive and procedural in nature, with criminalisation of all undesirable activities occurring within Nigeria cyberspace, while seeking to create legal procedures for investigation, prosecution and conviction of cybercrime and criminality.

The Evidence (Act 2011) is a significant development in the effort of the government towards investigating and prosecuting cybercrime activities. With this Act, electronic evidences and documents are now admissible in Nigeria Courts. This is a major step in the right direction towards the prosecution of cybercrime activities in Nigerian courts.

The proposed Digital Piracy Bill of the Nigeria Copyright Commission is an important step towards protecting intellectual property and to address digital internet piracy of soft skills.

The Nigeria government also establish Computer Crime Protection Unit (CCPU) under the supervision of the Public Protection Department of the Federal Ministry of Justice. The Unit is to work with agencies such as Economic and Financial Crime Commission (EFCC), the telecoms and banking sector.

The harmonised drafted National Information and Communication Technology policy by the Federal Ministry of Communication Technology would help to reposition the nation's information technology sector, create the enabling environment for the rapid expansion of information and communication technology networks and for the transformation of Nigeria into a knowledge-based economy.

In addition, a national policy on Public Key Infrastructure (PKI) was launch by National Information Technology Development Agency (NITDA) with a view to implement a robust trusted certificate for online transactions and interactions on the internet as well as to reduce the incidences of cybercrime in the country.

However, there is no specific legislation on cybercrime in Nigeria. As a result, what constitutes cybercrime is not defined in any written law in Nigeria. This has been a major impediment against the successful eradication of the menace.

The current means used in Nigeria to fight the menace of cybercrime are related provisions in other penal legislations in Nigeria like the Nigeria Criminal Code Act 1990, the Economic and Financial Crimes Commission Act 2004, the Advanced Fee Fraud and Other Fraud Related Offences Act 2006, the Money Laundering (Prohibition) Act 2011, and Evidence Act 2011.

A. Nigeria Criminal Code Act 1990

This Act provides explanation on false pretence under Part 6, Chapter 38, Section 418:

"Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence."

Section 419:

"Any person who by any false 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."

Section 420:

"Any person who by any false pretence, and with intent to defraud, induces any person to execute, make, accept, endorse, alter, or destroy, the whole or any part of any valuable security, or to write, impress, or affix, any name or seal upon or to any paper or parchment in order that it may be afterwards made or converted into or used or dealt with as a valuable security, is"

Section 421:

"Any person who by means of any fraudulent trick or device 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 or to pay or deliver to any person any money or goods, or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour, and is liable to imprisonment for two years."

B. ***Economic and Financial Crime Commission (Establishment) Act 2004***

Under this Act, the functions and responsibilities of the Commission are stated in Part II, Section 6(b):

"The investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc."

Section 6(c):

"The co-ordination and enforcement of all economic and financial crimes laws and enforcement functions conferred on any other person or authority"

Section 6(e):

"The adoption of measures to eradicate the commission of economic and financial crimes"

Section 6(f):

"The adoption of measures which includes coordinated preventive and regulatory actions, introduction and maintenance of investigative and control techniques on the prevention of economic and financial related crimes"

The Commission has power under this Act in Part II, Section 7 to:

a. cause investigations to be conducted as to whether any person, corporate body or organization has committed any offence under this Act or other law relating to economic and financial crimes
b. cause investigations to be conducted into the properties of any person if it appears to the commission that the person's lifestyle and extent of the properties are not justified by his source of income;

Part IV, Section 14 to 18 stipulate offences which includes; offences relating to financial malpractices, offences relating to terrorism, offences relating to false information, retention of proceeds of a criminal conduct and offences in relation to economic and financial crimes and petitions.

The Commission had convicted over 500 persons out of 700 prosecutions since its formal take-off in 2003 (Lamorde, 2012).

C. ***Advanced Fee Fraud and Other Fraud Related Offences Act 2006***

Under this Act, offences relating to cybercrime were stated in Part 1, Section 1 (1) (2):

1. Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud
    a) obtains, from any other person, in Nigeria or in any other country for himself or any other person;
    b) induces any other person, in Nigeria or in any other country, to deliver to any person; or
    c) obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.
2. A person who by false pretence, and with the intent to defraud, induces any other person, in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.

Section 5 (1) (2):

1. Where a false pretence which constitutes an offence under this Act is contained in a document, it shall be sufficient in a charge of an attempt to commit an offence under this Act to prove that the document was received by the person to whom the false pretence was directed.
2. Notwithstanding anything to the contrary in any other law, every act or thing done or omitted to be done by a person to facilitate the commission by him of an offence under this Act shall constitute an attempt to commit the offence.

Section 6:

"A person who is in possession of a document containing a false pretence which constitutes an offence under this Act commits an offence of an attempt to commit an offence under this Act if he knows or ought to know, having regard to the circumstances of the case, the document contains the false pretence."

Section 7 (1):

1. A person who conducts or attempts to conduct a financial transaction which in fact involves the proceeds of a specified unlawful activity
    a. with the intent to promote the carrying on of a specified unlawful activity; or
    b. where the transaction is designed in whole or in part:
        (i) to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of a specified unlawful activity; or
        (ii) to avoid a lawful transaction under Nigerian law, commits an offence under this Act if he knows or ought to know, having regard to the circumstances of the case, that the property involved in the financial transaction represents the proceeds of some form of unlawful activity.

Section 8:
A person who -

a) conspires with, aids, abets, or counsels any other person to commit an offence; or
b) attempts to commit or is an accessory to an act or offence; or
c) incites, procures or induces any other person by any means whatsoever to commit an offence, under this Act, commits the offence and is liable on conviction to the same punishment as is prescribed for that offence under this Act.

D. ***Money Laundering (Prohibition) Act 2011***

The Act makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of a crime or illegal act and provides appropriate penalties. Under Part II, Section 15 (1) (a):
Any person who:

a. converts or transfers resources or properties derived directly from:
(i) illicit traffic in narcotic drugs and psychotropic substances, or
(ii) participation in an organized criminal group and racketeering, terrorism, terrorist financing, trafficking in human beings and migrants smuggling, tax evasion, sexual exploitation, illicit arms trafficking in stolen and other goods, bribery and corruption, counterfeiting currency, counterfeiting and piracy of products, environmental crimes, murder, grievous bodily injury, kidnapping, illegal restraints and hostage taking, robbery or theft, smuggling, extortion, forgery, piracy, insider trading and market manipulation and any other criminal act specified in this Act or any other legislation in Nigeria relating to money laundering, illegal bunkering, illegal mining, with the aim of either concealing or disguising the illicit origin of the resources or property or aiding any person involved to evade the illegal consequences of his action;

Section 18:
A person who:

(a) conspires with, aids, abets or counsels any other person to commit an offence;
(b) attempts to commit or is an accessory to an act or offence; or
(c) incites, procures or induces any other person by any means whatsoever to commit an offence, under this Act, commits an offence and is liable on conviction to the same punishment as is prescribed for that offence under this Act.

E. ***Evidence Act 2011***

This Act provides for the admissible of statements in document produced by computers in Nigeria. It contains extensive provisions on electronic computer generated evidence.

Admissibility of statement in document produced by computers is stated under Part V, Section 84 (1):
"In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question"

Section 84 (2): The conditions referred to in subsection (l) of this section are:

a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly lo store or process information for

the purposes of any activities regularly carried on over that period, whether for profit or not by anybody, whether corporate or not, or by any individual;

b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and
d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

The Act has only been applied to electioneering matters. The Nigeria Court of Appeal have applied Section 84 (1) and (2) of the Act to the case of:

1. Dr. Kubor V. Seriake Dickson in 2012
2. Akeredolu V. Mimiko in 2013

From the foregoing, there is no specific mention made of cybercrime in any of the Nigeria laws. Ehimen and Bola (2010) argued that, Nigeria is a place where computers can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime.

V. CONCLUSION

There is today increasingly dependency on computer systems and networks in Nigeria by government and citizens to provide crucial services. The findings of this study are that, addressing the menace of cybercrime in Nigeria is a necessary compliment to the great strides by government to transform Nigeria into an information and communication technology (ICT) driven economy. To do otherwise is to deliberately endanger the same infrastructure we have worked so hard and invested so much to build and absence of cybercrime enforcement constitutes real hurdle to launch full-fledged e-commerce in Nigeria.

VI. RECOMMENDATIONS

Based on the findings of this study, cybercrime is emerging as a very concrete threat in Nigeria and the existing legislations in Nigeria are inadequate to address its threats. On this note, the researcher suggests the following:

1. There is an urgent need for the speedy passage of the Cybercrime Bill 2013 presently on the floor of the National Assembly.
2. There is a need to protect all critical information infrastructures and secure computer systems and networks in Nigeria.
3. The establishment of national Computer Emergency Response Team (CERT) centre for the monitoring, detention and analysis of all activities within the Nigeria cyberspace and the globe at large.
4. The establishment of fully functional national digital forensic laboratory in the Office of the National Security Adviser (ONSA). This is to avail all law enforcement and security agencies a platform for detailed investigation of cybercrimes in Nigeria.
5. There is a need for a 24/7 emergence response website where victims can report all cases of internet fraud and cybercrime at large and know that, it will be given attention swiftly and in a transparent manner.

6. The government should determine their training needs in the area of cybercrime and explore bilateral, regional and multilateral cooperation mechanisms to meet those needs.
7. The government should heighten awareness of the dangers of cybercrime amongst the general public, including users in the education system, the law and security enforcement agencies, and the justice system on the need to prevent and combat cybercrime.

In addition to the recommendations of the reasearcher, Okeshola and Adeeta (2013) suggests the followings:

1. For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb cybercrime, they recommended that there is need for them to understand both the technology and the individuals who engaged in this act.
2. Cyber criminals caught are been prosecuted by government. They argued that cyber criminals assets should also be confisticated by the government and the imposition of longer prison terms for cyber criminals. This will serve as deterrence to those youths who want to indulge in such crime.

REFERENCES

1. Adamski A. (1998) Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm Retrieved on 15th December 2013
2. Advanced Fee Fraud and Other Fraud Related Offences Act 2006
3. Akano T (2013). Cyber crime: Nigeria redeems image. The Punch. http://www.punchng.com/business/technology/cyber-crime-nigeria-moves-to-redeem-image/ Retrieved on 10th January 2013.
4. Akinsehinde (2011): "80% of Nigerian businesses risk cyber-attacks" The Punch, October 11, 2011
5. Aldesco, A. L. (2002). The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime. http://digitalcommons.lmu.edu/elr/vol23/iss1/3 Retrieved on 5th November 2013
6. Azazi (2011): Cyber-attacks: "Nigeria lacks structures to handle emergencies" The Punch, December 29, 2011
7. Bakewell, E. J., Koldaro, M., and Tija, J. M. (2001). Computer crime. The American Criminal Law Review, 38, (3), 481-524.
8. Brenner, S. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. The Journal of Criminal law and Criminology, 97(2), 379-475.
9. Britz, M. T. (2009). Computer Forensics and Cyber Crime. New Jersey: Pearson Education.
10. Carter D (1995). Computer crime categories. FBI Law Enforcement Bulletin, 64, (7), 21.
11. Carter, D. and Bannister, A. J. (2000). Computer crime: A forecast of emerging trends. Paper presented at the Academy of Criminal Justice Sciences Annual Meeting, New Louisiana.
12. Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(August), 588-608.
13. Council of Europe. (2001). Convention on Cyber Crime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm Retrieved on 10th January 2014
14. Economic and Financial Crimes Commission Act 2004
15. Emanuelsson-Korsell, L. and Soderman, K. (2001). IT-related crime-Old crimes in a new guise, but new directions too. Journal of Scandinavian Studies in Criminology and Crime Prevention, 2 (1), 5-14.
16. Evidence Act 2011
17. Jaishankar K (2008). Space Transition Theory of cyber crimes. In Schmallager, F., &Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.
18. Jacobson, H. and Green, R. (2002). Computer crimes. American Criminal Law Review, 39, (273).
19. Lamorde, I. (2012). EFCC secures 500 convictions in 12yrs http://www.punchng.com/news/efcc-secures-500-convictions-in-12yrs/ Retrieved on 2nd February 2014
20. Lemo T (2013). Cyber crime: Nigeria redeems image. The Punch. http://www.punchng.com/business/technology/cyber-crime-nigeria-moves-to-redeem-image/ Retrieved on 10th January 2013.

21. Money Laundering (Prohibition) Act 2011
22. Nigeria Criminal Code Act 1990
23. Smith RG, Grabosky P, and Urbas G (2004). *Cyber Criminals on Trial*. Cambridge University Press: Cambridge.
24. Sorunke (2011): "80% of Nigerian businesses risk cyber-attacks" The Punch, October 11, 2011
25. Thomas, D. and Loader, B. D. (2000). Introduction. In D. Thomas & B. D. Loader (Eds), Cybercrime: Law enforcement, security, and surveillance in the information age (pp. 1-14). New York: Routledge
26. Taylor, R. W. and Loper, D. K. (2003). Computer crime. In C. R. Swanson, N. C. Chamelin, & L. Territo (Eds), Criminal Investigation (8th ed). New York: McGraw-Hill Companies, Inc.
27. UN Office on Drugs and Crime. (2005). The Eleventh United Nations Congress on Crime Prevention and Criminal Justice. http://www. unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf Retrieved on 12th August 2013
28. U.S. Department of Justice (1989). National Institute of Justice. Computer Crime*:* Criminal Justice Resource Manual. http://definitions.uslegal.com/c/computer-crime/ 02nd February 2014.
29. Wall DS (2001). Crime and the internet. London: Routledge.
30. Weber, J. (2006). The Cloak of Anonymity. Retrieved October 28, 2010, from http://business.timesonline.co.uk/tol/business/industry_sectors/media/article709214.Ece
31. Wilson, H. and Shun-Yung, K. W. (2009). Emerging cybercrime variants in the socio-technical space. http://ww2.valdosta.edu/~whuang/publications/huang%20article09.pdf 31st January, 2014

