PAK Publishing Group
Growing Knowledge for Future

Proceedings Book of ICETSR, 2014, Malaysia
Handbook on the Emerging Trends in Scientific Research
ISBN: 978-969-9347-16-0

Cybercrimes and Victimization: An Analysis of Economic – Cost Implications to Nigeria

Dagaci Aliyu Manbe
Department of Sociology, University of Abuja, Nigeria
Sule Magaji
Department of Economics, University of Abuja, Nigeria
Damagun Y. M.
Department of Accounting, University of Abuja, Nigeria

Abstract

Cybercrime has become a global contending problem and so is the plight of its victims. The growth of information technology and computer connectivity creates space for criminal to exploit security vulnerabilities in the cyber space. Unfortunately, several functionalities of modern day web browser are not vulnerability – proof, thus exposing the average internet user to cyber crime victimization. Systems that people rely upon, from bank to air defense radar, are accessible from cyber space and can be quickly taken over and knocked out without first defeating a country's traditional defenses. The increasing global technological dependency on the internet for administrative activities, information dissemination, commercial business and transactions across the globe, its associated challenges and risks has really come to stay in Nigeria. The seriousness of cyber crime problem in Nigeria can be better appreciated when we consider the fact that inspite of the several interventions made by Nigeria Government and non-governmental organizations in tackling cyber crime (white collar crimes) Nigeria has for four consecutives years (2006, 2007, 2008 and 2009) ranked third on the list of world cyber crime perpetrator countries. This paper seeks to explore the major causes, forms, rate of victimization, economic – cost to Nigerian nation with alternative strategies of reducing the menace.
Keywords: Cybercrime, Victimization, Socio-demographic characteristics, Economic – cost, Preventive measures.

1. Introduction

Scholars and commentators have argued that full-scale organized cyber crime is fast emerging (Lusthans, 2013). "Systems that people rely upon, from bank to air defense radar, are accessible from cyberspace and can be quickly taken over and knocked out without first defeating a country's traditional defenses" (Clarke & Knake, 2010, p. 31). The growth of information technology and computer connectivity creates space for criminals to exploit security vulnerabilities in the cyber space (Broadhurst, 2006; Kigerl, 2012). Unfortunately, several functionalities of the modern day web browsers are not vulnerability-proof (Agbefu, Hori & Sakurai, 2013), thus exposing the average internet user to cyber crime victimization. With mobile telephony access made pretty easier over the past half a decade in Nigeria through the offering of internet services by virtually all Global System for Mobile Communication (GSM) service providers in Nigeria, the internet has pervaded the lives of many adult Nigerians.

With the increasing dependence on the internet for work, business and pass-time, the internet with all its associated challenges and risks has really come to stay in Nigeria. However, not so many in Nigeria are aware that the internet super high-way has been invaded by criminals and deviants who lurk around desperately looking for targets. Oftentimes, the unguarded, naive and casual internet user fall prey to their antics. The problem of cyber crime victims is made worst by the seeming inability of law enforcement agents to effectively prosecute offenders. Clearly, law enforcement has not been able to keep up with technological advances to prevent cyber crime (Jaishankar, Pang & Hyde, 2008; Choi, 2006). Anti-hacking laws, because of their traditional approaches to crime containment, have been ineffective (Sharma, 2007). Various studies have explored the nature and extent of cyber crime and victimization (Bossier & Holt, 2010; Choi, 2008; Finn, 2004; Holt & Bossier, 2009; Haider & Jaishankar, 2010; Marcum, 2008; Ngo & Paternoster, 2011). Also there have been quite a number of Nigerian studies on cyber crime. One of the earlier studies by Longe and Chiemeke (2008) examined how access to the internet boosts criminality. Tade and Aliyu (2011) and Ojedokun and Eraye (2012), looked at the Nigerian university undergraduates involvement in internet crime and the benefits they believe that come from it. Other studies like Adeniran (2008) and' Aransiola and Asindemade (2011), also focus on cyber crime in Nigeria. Adeniran (2008) argues that the advent of the internet technology in Nigeria has led to the modernization of fraud among the youth in that cyber fraud seems to have become accepted as a means of living for the Nigerian youth. He argued that this is more so for those who are of college age (Adeniran, 2011).However, very few studies have been done on cyber crime victimization in Nigeria. This is the gap this study hopes to fill. The present study investigates the socio- demographic correlates of cyber crime victimization by seeking answer to the following question: What are the factors that can predispose one to cyber crime victimization in Nigeria?

2. Economic – Cost Implications of Cybercrime Victimization (N = 1354) in Nigeria

	Cyber crime victimization			
Variables	**Have been victim of cyber crime**	**Have not been victim of cyber crime**	**Total**	**X^2**
Age (Years)				**p< .069**
Younger respondents	226 (18.9)	967(81.1)	1193 (100.0)	
Older respondent	21 (13.0)	140 (87.0)	161 (100.0)	
Gender				p< .197
Male	158 (19.3)	659 (80.7)	817 (100.0)	
Female	89 (16.6)	448 (83.4)	537 (100.0)	
Marital Status				P<.005
Single	167 (16.5)	884 (83.5)	1011 (100.0)	
Ever married	80 (23.3)	263 (76.7)	343 (100.0)	
Level of Education				P<.342
Low level of education	9 (17.3)	43 (82.7)	52 (100.0)	
Medium level of education	151 (17.2)	727(82.8)	878 (100.0)	
High level of education	87 (20.5)	337 (79.5)	424 (100.0)	
Occupation				p< .000
Student/Apprentice	114 (15.1)	642 (84.9)	756 (100.0)	
Business/trading/Artisan	39 (17.3)	187(82.7)	226 (100.0)	
Civil/Public Servant	74 (24.7)	225 (75.3)	299 (100.0)	
Unemployed	20 (27.4)	53 (72.6)	73 (100.0)	
Religion				P<.040
Christian	169 (20.9)	641 (79.1)	810 (100.0)	
Muslim	60 (14.9)	343 (85.1)	403 (100.0)	
African Traditional Religion	4 (17.4)	19 (82.6)	23 (100.0)	
Others	14(11.9)	104(88.1)	118(100.0)	

Note. Younger respondents refer to those 15-34 years, while older respondents refer to those 35 years and above. Ever Married respondents refer to those who are married, divorced, separated or widowed. Low education refers to those that had less than seven years of schooling; medium education refers to those that had less than 16 years of schooling, while high education refers to those that had more than 16, years of schooling.

Table above indicates that 18.9% of younger respondents (15-34 years) have fallen victim of cyber crime as against 13.0% of older respondents (35 years and above). Younger respondents appear to be more vulnerable to cyber crime victimization than older respondents though this is not out rightly statistically significant (P< .069). This is hardly surprising as the younger respondents constitute the majority of the students' population/ internet-active group and therefore are more exposed to the risk of victimization than their counterparts. Table 1 also shows that 19.3% of male respondents and 16.6% of female respondents have been victims of cyber crime though this is not statistically significant (P< .197). Again, this could be attributed to the frequency of on-line activities by males. Males stay on-line more than females and sometimes may return late at night from cyber cafes.

Findings also indicate that 16.5% of single and 23.3% of ever married (married, widowed, separated and divorced) respondents had fallen victim of cyber crime. Statistically significant differences also exist among the two groups (P< .005). Ever married respondents appear to have been more victimized than those who are single. This is probably because they visit the cafes less frequently than single respondents and are therefore less likely to be aware of the tactics/tricks of hackers.

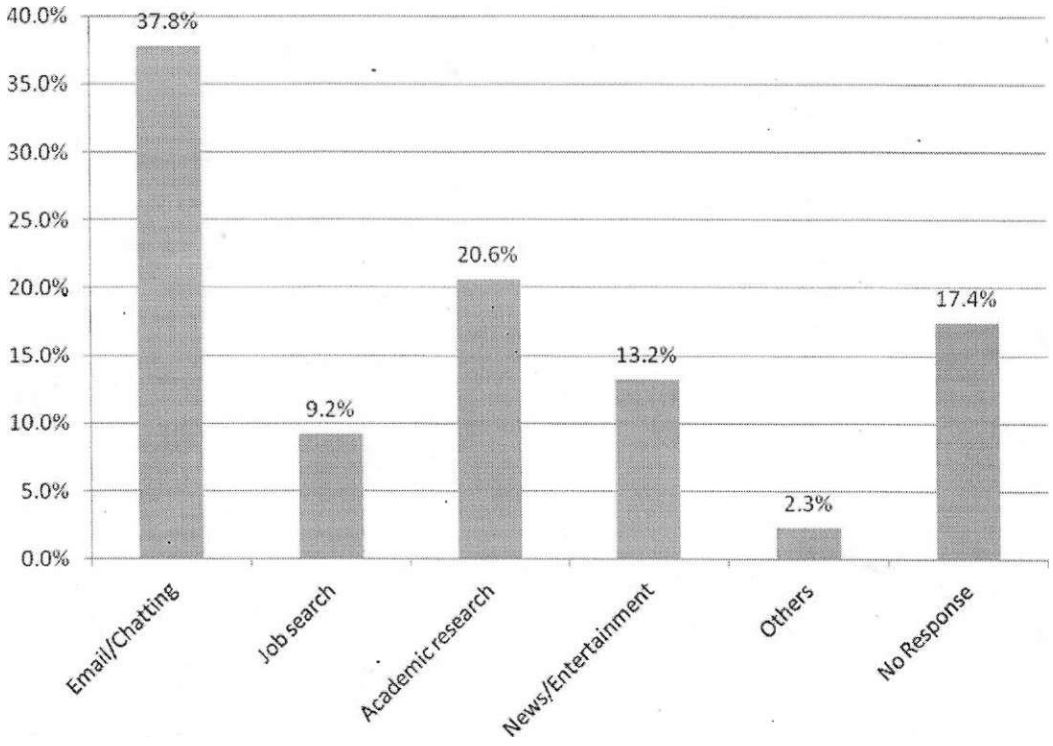
A look at the level of education of respondents shows that 17.3% of respondents with low level of education (less than seven years of schooling), 17.2% of those with medium level of education (less that 16 years of schooling) and 20.5% of those with high level of education (More than 15 years of schooling) had been victims of cyber crime. This finding was however not be statistically significant (P< .324). People with higher level of education are more prone to cyber crime victimization than those with low and medium education. This is perhaps so because people with higher level of education use internet facilities less frequently and may not be abreast with emerging cyber threats and hackers strategies.

Cyber crime victimization with respect to occupation indicates that 15.1% of students/apprentice, 17.3% of business people/traders/artisans, 24.7% of civil/public servants and 27.4% of unemployed respondents have fallen victim of cyber crime. Statistically significant difference exist between various occupations (P<.000). Unemployed persons are the most affected category of cyber crime victims. This is perhaps because this category of people are often hooked to the internet, desperately searching for money making opportunities. In their desperation, they are more likely to fall prey to cyber crime victimization.

For religion, 20.9% of Christians, 14.9% of Muslims, 17.4% of African Traditional Religion faithful and 11.9% of other religions like Hindu and Eckankar have fallen victim of cyber crime. The above table suggests that Christians are more likely to fall victim of cyber crime than adherents of other religions (P< .040). This may perhaps be a function of the "logic of numbers" since Christian users appear to be more in number. The study further investigated the activity mostly engaged in by respondents while on the internet. Findings show that 1, 37.8% pre-occupy themselves with email/chatting when on the internet, 9.2% use the internet for job search, 20.6% use it for academic research, 13.2% for news/entertainment and 2.3% for other activities which include "business" and "sourcing for clients" (see Figure 1). Since students constitute the majority of the internet usage population in Lagos metropolis one would have expected that their major internet activity will be academic research. However, the above finding suggests that students' major pre-occupation online is email/chatting. With the growth of social network sites like Face book, Twitter, Net-log, You-tube, Skype and so on, many students are entering chat rooms and making friends with both known and unknown persons thereby increasing their vulnerability to cyber crime victimization

Table 2 indicates that the independent variables are age, sex, marital status, level of education, occupation and religion, while the dependent variable is victimization. The result of the regression analysis shows that three variables: age, occupation and religion were statistically significant (p<.018, p<.002 and p<.044 respectively). The distribution shows that younger respondents are more likely to fall victim of cyber crime than older respondents. Also, unemployed people are more likely to fall victim of cyber crime than people of other occupation and Christians are more likely to fall victim of cyber crime than people of other religions. Therefore, age, occupation and religion are good predictors of cyber crime victimization. Unlike older respondents, younger respondents are more likely to take

online risk without calculating it. This is hardly surprising, given that young people's world" is a world of adventures. Similarly, unemployed respondents, in their desperation for online job opportunities may be trapped. Because of the relatively high level of youth unemployment in Nigeria, many young job seekers spend quality time on the internet searching for employment and business opportunities thereby exposing themselves to cyber crime victimization. Christians perhaps use the internet more than members of other religious groups and therefore are more exposed to online victimization than the rest of their counterparts.



3. The Socio-Economic Cost of Ctbercrimes on Nigeria Economy

Documentably, the incidence of cyber crime has resulted into some noticeable socio-economic changes in Nigeria. Specifically, the effects include: soled national image, stifled economic Development, Colossal loss of resource and lives, Threatened Privacy, Undermined National Sovereignty, Encouragement of other forms of crime, Misdirected law enforcement, on the one hand and job creation, poverty reduction, braced-up security, etc on the other.

Soiled National Image: Advance fee fraud has become synonymous to Nigeria. Nations of the world have lost interest in doing business with Nigerians. So many potential inventors have been so scared that they may never wish their enemies to, let alone dream of coming to invest in Nigeria. The following revelations of Hamzal-Seleh (a Saudi business Magnet), shortly after his rescue from an online aided kidnappers drives the point home. "They are wicked brutal and foolish. I was ready to invest, I was ready to invest other businessmen to come and invest in Nigeria" (Oji, 2011).

Characteristics, cyber crimes victimizes people all over the world hence it minimizes the chances of Nigerians doing business globally. Many online companies have employed software's that can re-flag or automatically reject online orders from Nigeria because of the rate of cyber fraud in the country (Hansen, 2002/2003). At the international Airports, Immigration officers will nearly skin Nigerians, waste their time and pelt them with embarrassing questions, the moment they reveal their identities. Recounting the pains of travelling with Nigeria passport, Adeboye (2008) says… "the moment they heared that I am a pastor that was when they decided that the search must be thorough…. At the end they apologized". This shows that the stench is too offensive to be wiped by religious accolades. Furthermore, Odey (2001) aptly captures his own ordeal thus:

> *I had been delayed for not less than two hours. As soon as my interrogators left….., the lady on the computer…. Tendered a very polite apology on their behalf. "Sir" she said to me. "Do*

not be offended. Your people are responsible for all this. We are not. They are terrible people and they have done terrible thinghs in this country. And we want to stop the *rot" (p 64)*

Stifled Economic Development: Online piracy and other cyber crimes; that render Nigeria cyber space too risky for buying and selling are busy suppressing, if not crushing creativity and online entrepreneurship. It is not uncommon to see Nigerian artiste roasting in penury after years of hard labour in the musical industry, while the pirates are getting richer. The sum of N11.2 billion is what Nigeria looses to software piracy every year (Ayatokun, 2006). Of course, that amount is big enough to manage Nigeria three orbit Satellites for five and half years. Infact, it is almost the annual budget of the National Space Research and Development Agency (NASRDA) (Adaramola, 2011). The "incredible volume of Spam emanating from Nigeria continues to be an issue of great concern to the nation and the world at large" because it over crowds the internet bandwith, reducing its speed of operation. For instance, most organizations including government parastatals cannot conduct online recruitments efficiently. Coupled with the issue of cyber-crimophobia that the international market has developed for Nigeria, we may continue to be limited to doing business, the crude way (manually).

Triggering other forms of crimes: Online pornography; can be crimogenic. The gospel of atypical sexuality as simonized by the pornographers has a far reaching impact on the personality of the viewers and by extension, the country. Studies have traced the root most rapes, drug use and child abuse to habitual pornographic interests.

Accumulative research…..demonstrate that pornography encourages sexual assault such as rape and child similarly children exposed to pornography at a very tender age are most liable to greater indulgence in deviant sexual practices particularly rape. The more they watch, the higher their chances of acting out…. (obiekwe, 2006 p.29).

More so, according to Molenkamp and Saffioti (2001) cybercrimes "fosters a voyeuristic attitude regarding sexuality". This continually moves individuals further away from the normal relational sex necessary for a health society. With the level of anonymity that is possible online, a man can easily engage his daughter unknowingly in cyber sex (Rittinghouse & Rensome, 2005). This is quite repugnant to natural cum social justice. With the type of things the leaders of tomorrow are "enjoying" today, courtesy of cyber porn, in future, such pornographic minds may see nothing wrong in legalizing rape as legislators. Already, we have the homosexual uprising making news in Nigeria dailies (Eze, 2011).

Colossal loss of Lives and Resources: In 2008 alone, one trillion was lost to computer crime generally. Similarly, in May 2011, Sony's play station came under attack and they lost up to $171 million (Voigt, 2011). Even businesses suffer great losses both tangible and intangible when attacked by hackers. Infact, the February 2000 DDoS that frustrated online transactions across the globe did cost up to $1 billion. The malware called "love bug" designed by a 23 year old philipino hacker wasted $10 billion worth of assests world wide in may 2000. Even the inventor was amazed that the worm could be that devastating.

In U.S victims of credit-card theft may be liable for the initial $50 of fraudulent charges but financial institutions bear the brunt. However the cost of victimization may include goodwill hence organizations don't find it funny sharing their experience (Goodman, 2002/2003). Many organizational victims of industrial or economic espionage have lost their sensitive information (non-material assets). Whereas convicted offenders have lost heavily due to lawsuit and resulting damage awards and eroded reputation (Haag, 2002:76). Regrettably, Nigeria has lost job opportunities by not having foreign investment due to fear of crime.

A part from consuming money and times that would have been used for other things through addicted scamming, it also consumes lives. Some victims go to the extent of committing suicide or murder. Tyler clement, a victim of cyber bullying had to jump down the bridge to escape the embarrassment of watching the video of him in a homosexual display, sent online by some bullies in his new school (Kawalski et al, 2008). Similarly, a Nigeria diploma was murder in Zech Republic by retired defrauded Nigeria scammers (Ogunsaya 2006).

Threatened privacy: With the trend of things, privacy is increasingly becoming endangered. Hackers can scan all massages traveling in a network, using a packet sniffer, all in attempt to capture some private information. There was a case in Wisconsis where a person uploaded the nude picture of his ex-girl friend and her new lover, into the cyberspace. The victims became alarmed when they received strange calls from people as far as Denmark commenting on the show of shame (Grabosky,

2101; Awake, July 2011). When the cyber spies makes nonsense out of privacy, the concept of safety becomes a hoax. For in every functional security there is a spice of obscurity.

Undermined National Sovereignty: By lending weight to transborder and other organized crimes, cyber crimes undermines the sovereignty of Nigeria and any other nation for that matter (Siegel, 2007:475). Several police and military systems across the globe including the so called supper powers have been humbled by hackers. For instance in 2000, Ikenna Iffih-a 20 years old Nigeria was convicted for hacking into the U.S army's and NASA'S computer among other private targets (Ogunsaya, 2006; Bashir, 2011). The worst is that most of the attacks go undetected. According to Goodman (2002/2003). Out of 38,000 attacks perpetrated against the U.S Department of Defence, between 1992 and 1995, only 4% of the successful attacks were detected. Yet the CNN reports an increase in the "asymmetric attacks" in which a small group do disproportionate damage on governments and large companies. A typical example is that painful-sweet revelations of the wikileaks that has punctured U.S's foreign policy. Often times, spies do give away state secrets or security information for a peanut. (Voigt, 2011). The case of Nigeria will be unimaginable considering the level of our technology. If the green trees are falling what will happen to the dry ones?

Misguided Law Enforcement: It is quite easy for an innocent man (a victim of identity theft) to be jailed for a crime he never contemplated, in life. Criminals try as much as possible to sway investigations to the people they have captured their personal information. (Arase & Obaedo, 2007).

Positive effects: Cyber crime has taken many families out of poverty, brought prestige to the "young millionaires, created job for some unemployed youths and beefed up the activities of the security agents in Nigeria and elsewhere. Considering the damage done to our economy by colonial masters, one may come to appreciate the fact that the children of those colonial thieves are now reaping what their forefathers sowed. Yes, it's more like a payback time for deliberately taking advantage of our fore parent's simplicity and ignorance. At least, they now know that we are not monkeys. Anatomical analysis of the spam letters reveals that corrupt and greedy Euro-Americans do connive with local thieves to milk Nigeria dry (Olusesi, 2008; Goodman 2002/2003).

However, when juxtaposed with the disservice cybercriminals has done to Nigeria, the aforementioned benefits become so infinitesimal. Of a truth there is no evidence to prove that fraudsters are mindful of the family members of Lord Lugard and his cohorts. If that is the case, why have Nigerians constantly scammed Americans, Czech Republicans and even their fellow Africans?. If there is anything to prove, to the world, it is that the diffusion theory of development is not a fable. We can prove a point by making contributions by way of inventions. When stigmatized as a "rogue nation" our economy suffers at the long run.

One home truth is that no one (including the cybercriminals) is immune from the effects of crime. Thus, cyber crime is a respecter of no persons, especially at the long run. If banks are attacked our money goes, if the ISP got over whelmed by DDOS, we all share in the frustration. Should our business environment be rendered too unsafe for transactions, the international business community will avoid us like lepers as the rate of unemployment gets monstrous. If nothing is done now, posterity will watch our children unborn fall into the pit we are digging today (Waziri, 2009).

4. The Way Forward

Cyber crime problem has become a global problem and so is the plight of its victims. Cyber criminals are intelligent people who understand the psychology of various, age, sex and economic occupational groups. In setting their strategies, they manipulate the minds and massage the egos of the most vulnerable group of young adults who are so impressionable. This scenario is exacerbated by the undue emphasis on wealth and material possession by the Nigerian society where the end seems to justify the means.

Rather than resort to the "fire brigade" approach to crime control that has become the norm rather the exception in Nigeria, the government should dedicate more energy and resources in addressing the social conditions that give rise to cyber crime. The various efforts by law enforcement agencies to combat the menace of cyber crime will only be successful and sustainable if the real victims and targets are made less suitable for on-line victimization.

Anti-cyber crime campaigns should be taken to post-primary schools and institutions of higher learning. The virtues of honesty, hard work and integrity should be taught our youths. Every effort should be made to practically demonstrate to the youth of this generation and the upcoming ones that

there is dignity in labor and that work is gain not pain. Also more recreational facilities should be provided in schools and cities across Nigeria. They should be properly secured from touts and street urchins and made accessible to adult Nigerians and accompanied minors free of charge. The Nigerian society needs to redefine where it stands on the issue of wealth acquisition. Rather than celebrate wealth per se, she should celebrate service and dignity. This is one way of saving internet active Nigerians from the pains of cyber crime victimization.

References

Adaramola, Z. (2011). Nigeria to launch two satellites into orbit in July. In daily trust, Friday, June 24, 2011. pp:11.

Adeniran, A. (2011). Cafe culture and heresy of yahooboyism in Nigeria. In K. Jaishankar, (Ed.), Cyber criminology: Exploring internet crimes and criminal behavior. Boca Raton, FL, USA: CRC Press. pp: 3-12.

Adeniran, A. I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. International Journal of Cyber Criminology, 2(2): 368—381.

Adeola, A. (2010). History of internet in Nigeria. In Ada, S. (ed) Introduction to mass communication. (Accessed on 03/10/2011). Available from www.introductiontomasscommunications2.Blogsport.com/2010/05/history-of-internet-in-Nigeria.html.

Adesina A.A. (2011). Interview granted to fact file crew on capital fm, October 2011.

Adler, F., Mueller, G.O.W, Laufer, W.S. (2007). Criminology and the criminal justice system. 6th Edn., U.S: Mc-Graw Hill.

Agbefu, R. E., Hon, Y., & Sakurai, K. (2013). Domain information blacklisting method for the detection of malicious'webpages. International Journal of Cyber Security and Digital Forensic, 2(2): 36 -47.

Arase, S.E. and Obaedo, A. (2007). Hi-tech (Computer and cyber) crimes. In Arase, S.E. and Iwuofor, (eds) Policing Nigeria in the 21st century. Ibadan: Spectrum Books E. pp: 299-307.

Ayantokun, O. (2006). Fighting cybercrime in Nigeria. Available from www.tribune.com/ng/08062016/infosys2.html.

Babalola, A. (2011). EFCC an organ of reformation. Interview to ZT, 6(1). March, 2011.

Bashir, M. (2011). NSA: Cyber terrorism days are numbered in daily trust, Friday June 24, 2011. pp: 3.

Bohm, R.M and Haley, K.N. (2007). Introduction to criminal justice. 3rd Edn., Califonia: Glencoe/Mc Graw Hill.

Bontrager, S. (2011). Richard cloward and lloyed ohlin (1960) and modern criminology. (Accessed on 16/12/2012). Available from www.criminology.fsu.edu/crimthery.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber crime policing. An International Journal of Police Strategies and Management, 29(2): 408 — 433.

Chapman, C. (2009). The history of internet in nutshell. (Accessed on 03/10/2011). Available from www.sixrevisions.com/resources/the-history.

Clarke, R., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. New York: Harper Collins Publishers.

Clinton, H. (2009). The future of Nigeria is up to Nigerians. A speech at a town hall meeting with NGOs. August 19, 2009 in Abuja. Published in ZT, 4(3): 54.

Cloud and Ohlin, (1960). Deferential opportunity. As interpreted in. Availabe from www.http://megaessays.com.

Cloward, R. (1959). Illegitimate means, anomie and deviant behaviour. America Sociological Review, 24(2): 164-174.

Dambazau, A.B. (2007). Criminology and criminal justice. 2nd Edn., Ibadan: Spectrum Books.

Dion, M. (2010). Advance fee fraud letters as machiavellian//narcissistic narratives. In Available from www.cybercrimejournal.com.

Edozien, C.J. (2009). We need protection to tackle corruption. Interview Granted to ZT, 4(3): 43.

EFCC, (2006). Advance fee fraud and other related offences act, 2006.

Emeagwali, P. (1997). Can Nigeria leapfrog into the information ages? (Accessed on 7/4/2011). Available from http://Emeagwali.com/speaches/igbo/7.html.

Finn, J. (2004). A survey of online harassment at a university campus. Journal of Interpersonal Violence, 19: 468-83.

Gabriel, C. (2010). History of internet in Nigeria… Same as in Adeola 2010 above.

Goodman, M. (2002/2003). Making computer crime count. In victor, J.L. and Naughton, J (eds) Annual Editions. Criminal justice. Connecticut: McGraw Hill/Dushkin.

Grabosky, P. (2010). 9 types of cybercrime. (Accesed on 7/6/2011). Available from www.hku.hk/cybercrime.htm.

Haag, et al., (2002). Computing concepts. 1st Edn., New York: McGraw-Hill.

Hague, W. (2011). The London conference on cyberspace. THISDAY, 16(6021): 7. Tuesday, October 18th 2011.

Hansen, B. (2003/2004). Cybercrime: Should penalties be tougher? In victir, J.L. and anughton, J. (eds) Annual Editions: Criminal Justice. USA: McGraw Hill and Dushkin. pp: 19-27.

Jaishakar, K. (2007). Establishing a theory of cyber crimes. (Editorial) International Journal Of Cyber Criminology, 1(2). July 2007. (Accessed on 31/8/2011). Available from www.cybercrimejournal.com.

Jedlicka, L.S, (2004). Computers in our world. Boston: Thomson.

Kent, P. (1999). The complete idiots guide to the internet. 6th Edn., Indianpolis: Que.

Longe, O.B and Chiemeke, S.C. (2008). Cyber crime and criminality in Nigeria-what roles are internet Access points playing? Availbale from www.eurojournal.com/ejss-6-4-12.pdf.

Maya, E. (2010). Cyber terrorism hits Nigeria. Available from www.abujacity.com.

Mayeda, A. (2005). You aint seen nothing yet. (Accessed on 27/6/11). Available from http://emeagwali/com/speaches/future/internet/index.html.

Mbasekei, M.O. (2008). Cybercrimes: Effects on youth devlpt. A paper presented at clean foundations' youth against crimes quarterly interactive forum in Bola Ige Millennium Secondary School Ajegunle, Lagos 1st Sept. 2008. (Accessed on 14/6/2011). Available from http://i.genuis.org/member/profile.php./id/1138/post1007.

Molenkap and Saffioti, (2001). The cyber sexual addiction. journal of Human Development, Spring 2001, 22(1): 5-7.

Ngo, F. T., & Paternoster, R. (2011). Cyber crime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5: 773 -793.

Njoku, E.T. (2011). Globalization and terrorism in Nigeria. Foreign Policy Journal. (Accessed on 24/10/2011). Available from http://www.foreignpolicyjournal.com.

Nkanga, E. (2011). Non-passage of cyber crime Bill Decried. (Accessed on 31/08/2011). Available from www.thisdaylive.com.

NPC, (1998). 1991 population census of the federal republic of Nigeria: Analytical Report at the National level Abuja.

Numbai Police, (2011). Cybercrime awareness. Available from www.cybercellnumbai.com.

Nwankwo, I.S. (2011). Nigeria law: Attacks in information systems: How safe is the Nigeria cyberspace? International Legal Strategists Group. (Accessed on 14/6/2011). Availble from www.facebook.com/note-php? Note-id=496656445826-52k.

Obiekwe, O.T. (2006). The impact of pornography on Nigeria Youths in Gwagwalada area Council of Abuja. (Unpublished B.Sc Project, Department of Sociology University of Abuja, Abuja).

Odekunle, F. (2010). Corruption: I support life imprisonment and special court. Our Milestone, 1(1): 74.

Odey, J.O. (2001). The anti-corruption crusade: The Saga of a crippled giant Enugu: Snap Press.

Ogbunwezeh, E.F. (2006). EFCC and cyber crimes: The true lessons. (Accessed on 14/6/2011). Available from http//www.nigeriavillagesquare.com.

Ojedokun, U. A., & Eraye M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. International Journal of Cyber Criminology, 6(2): 1001-1013.

Oji, C. (2011). Scan: Police rescue Saudi Bizman from kidnappers daily sun, Thursday October 20th 2011. (Accessed on 21/10/2011). Available from www.sunnewsonline.com.

Olakami, J. & Co. (2011). Evidence act 2011: Synoptic guide. 1st Edn., Abuja: Lawlords.

Olusesi, M. (2008). Cyber crime in Nigeria: A Sociological Analysis. (Accessed on 14/6/2011). Available from http://profgave.blogspot.com.

Oni, (2009). Nigeria. (Accessed on 03/10/2011). Available from http://opennet.Net/research/profiles/Nigeria.

Osuji, K.C. (2005). Cyberlaws: Its application and enforcement. (Unpublished LL.B Project, Faculty of Law University of Abuja, Abuja).

Oyesanya, F. (2004). Nigeria: Heaven for terrorist internet communication. (Accessed on 7/10/2011). Available from www.nigeriavillagesquare.com/acticles/femi-oyesanya/nigeria-heaven-for-terrorist-internet-communication?

Oyesanya, F. (2007). Nigeria internet 419 on the loose. (Accessed on 14/6/2011). Available from www.dawodu.com/yesanya.1htm.

Peace, (2010). Common wealth internet governance forum. Available from www.commonwealthconnectsprogramme.org.

Ribadu, N. (2007). A welcome address presented at the West African sub-regional meeting on advance fee fraud jointly organized with INTERPOL at the EFCC Training and Research Institute (TRI) Karu, Abuja. Current Trends in Advanced Fee Fraud in West Africa, Retrieved on 15th August 2013. Available from www.efccnigeria.org/index. php?option=com_docman&task= doc_ download&gid=9

Rittinghouse, J.W. and Ransome, J.F. (2005). IM: Instant messaging security. USA: Elsevier Digital press.

Sagay, I. (2010). EFCC has given us hope. An Interview Granted to Our Milestone, I(1): 48.

Sharma, R. (2007). Peeping into a hacker's mind. Can criminological theories explain hacking? Social Science Research Network. (Accessed on 15'h August 2013). Available from http: / / ssrn. com/abstract= 1000446.

Shelly, G.B., Cashman, T.J., Waggoner, G.A. (1996). Using computers: A gateway to information: World wide web edition. Canada: Boyd and Fraser Publishing Co.

Siegel, L.J. (2007). Criminology: Theories patterns and typologies. 9th Edn., U.S.A: Thomson Wadsworth.

Tade O., & Aliyu, I. (2011). Social organization of internee fraud among university undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2): 860—875.

Ubani, D. (2011). Dan Ubani, Abia State commissioner for information says Abia State University rape video, a ruse. In Available from www.nesz.onlinenigeria.com.

Uzor, B. (2011). New evidence act paves way for electronic evidence in courts. Available from www.businessdayonline.com.

Voigt, K. (2011). Analysis: The hidden cost of cybercime. (Accessed on 7/6/2011). Availble from www.edition.cnn.com.

Waccs, (2010). The 1st West African cybercrime summit (WACCS 2010): The communique. Published in www.waccs.web.officeline.com.

Watch Tower, (2011). What should i know about social networking? Part 1. Awake July 2011. pp: 24.

Waziri, (2008). Anti-graft war: Expect revolution. Zero Tolerance, 3(2): 28.

Waziri, F. (2011). Towards increasing capital flow to Africa: EFCC's reforms and way forward. Paper Presented at UN Conference on Least Developed Countries, Istanbul Turkey. Published in our Milestone, 2(1): 34.