Cybercrime among University Undergraduates: Implication for Counseling

Anyanwu J. I & Obiyo N.O.
Department of Educational Foundations
University of Nigeria, Nsukka

Abstract

This study investigated the prevalence of cyber crime in the south eastern part of Nigeria, the reasons for the crime and preventive measures. The study adopted an Ex-Post Facto design and used 300 respondents from cyber cafes in the higher institutions in the South Eastern Zone of Nigeria. The instrument for data collection was a four- point scale questionnaire. The findings reveal that all 12 types of cyber crime listed exist in the South eastern states of Nigeria namely, Imo, Abia, Ebonyi, Anambra and Enugu states. The reasons for engaging in cyber crime include poverty, unemployment and frustration, among others. The preventive measures are basically informational and can be given by counselors through group activities like seminars, workshops and enlightenment campaigns to support the efforts of the government.

Key Words: Cybercrime, Counseling, Behavioural, Disorder, Undergraduates, ICT.

Introduction

Worldwide, information and communication Technology (ICT) is being acclaimed as an important phenomenon for sustainable development because of its positive impact on socio-economic development and education. The Nigerian National Policy on Information Technology stated that sustainability, promotion and competitiveness of the nation hinge on this sector (FRN2001) and a major aspect of this sector is the internet.

The internet has the capacity to influence education and national

development (Menchik 2004, Ayeni 2000, Ofoegbu 2007) and this has motivated individuals, institutions and organizations to establish cybercafés where people can readily access information from the internet. Opportunities of this nature abound in universities and other higher institutions in Nigeria in consonance with the goals of tertiary education which among others include: to acquire both physical and intellectual skills which will enable individuals to be self- reliant and useful members of the society (NPE, 2004).

Greater percentages of the internet users are the youths (Ofoegbu 2007) and there is conflicting reports on ICT competencies and usage by gender with majority in favour of boys (Faulkner 2002, Field 2010, Ude, 2010). However, some people use these competencies negatively and abuse this application of knowledge and information diversity, leading to criminality or cybercrime.

Cybercrime according to Duggal (2011) is any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes. Expatiating further, Nagpal in Pati (2011) stated that unlawful acts whereby the computer is used either as a tool or target or both constitute cybercrime. As a target, criminals can physically damage or steal the computer system, internet time and even information contained in the electronic form, gain unauthorized access to computer system and computer networks among others.

Specific computer crimes according to Atili (2011) include financial fraud, theft of proprietary information, system penetration from the outside, unauthorized control/access over computer system, possession of unauthorized information, on-line gambling and transmission of viruses among others. Spam, obscene or offensive content/ pornography (basically child pornography) and harassment through e-mail equally constitute cybercrime (Denise 1998).

Contributing Pati (2011) stated that these crimes listed may be committed against the individual, people's property, organization and the society.

Report from Odapu (2008), show that e-mail scams emanating from Nigeria, constituted 1.1% of the 2007 complaints received in Internet Crime Complaint Centre (IC3) in the United States alone. Besides, the amount lost by individuals reporting fraud-type monetary loss in 2007 puts Nigerian letter fraud at 6.4% amounting to $1922.99million.

In terms of financial crimes, reports from the Central Bank of Nigeria (CBN) indicate that the banking sector lost N7.3 billion to cyber financial crimes in 2007. In February 2008, Spanish Police arrested 10 Nigerian internet fraudsters for allegedly fleecing internet users of over $28,000 by making them believe they had won a lottery game.

Cybercrime used to be regarded as mainly a developed world problem due to the fact that they adopted the computers and internet earlier. With the rapid adoption of computers in Nigeria, cybercrime also known as "Yahoo, Yahoo" has assumed an alarming dimension among the youths (Atili, 2011). Contributing, Pati (2011) stated that the cyber criminals include children and adolescents between the age group of 6 – 18 years drawn into cyber crime mainly due to the urge to know and explore things, excel amongst peers or due to harassment by friends. This validates Erikson's position in his theory of psychosocial development that children between the ages of 6-12 devote their energies to self-improvement and to conquer people and things; they adjust to the tool world and strive to master whatever they do. Success in this venture culminates in industry or inferiority complex when they fail.

Some of these cyber criminals may have emotional behavioural disorder (EBD). People with EBD are those (students/Youths) whose behaviours do not conform to the accepted standards and rules. The characteristics may manifest within the family group with early symptoms of lying, stealing, disobedience, verbal or physical aggression towards other family members (Obiyo, 2006). The adolescent may become involved in the activities of an adolescent gang, where antisocial acts including cybercrime can be learnt.

Cybercrime is a nonlocal crime; it can occur in jurisdictions separated by vast distances and a cyber criminal can remain 'faceless' for long. In spite of the constitution of the Independent Corrupt Practices Commission (ICPC) and the Economic Financial Crimes Commission (EFCC) who are charged with the duty of eliminating the menace, and successes achieved, cybercrime is still raging on. Zulu (2008) declared that public-private partnership is essential in addressing the increasing complexities of cybercrime as no one party can solve the problem alone. This is where personal/social counseling services given to students in institutions by guidance counselors to help them acquire interpersonal social relationship skills through assertive

training and cognitive restructuring becomes necessary to nip potential cyber criminals in the bud since cybercrime is perpetrated by youths. Cognitive restructuring is a process of helping individuals acquire problem solving/decision making skills that will enable them to overcome peer pressure and be assertive when necessary. It equally equips people with rational thinking capabilities that help them expunge mundane ideas and beliefs previously acquired.

The purpose of the study therefore was to identify the prevalent cybercrimes in the South Eastern part of Nigeria, causes, prevention strategies and the influence of gender on cybercrime.

Research Questions

The study was guided by three research questions:
1. What are the prevalent cyber crimes among young people and students?
2. What are the reasons for getting involved in cybercrimes by the youths?
3. What are the cyber crime prevention strategies?

Hypothesis

One null hypothesis was formulated and tested at 0.05 level of significance:

Ho1: there is no significant difference in the mean ratings of prevalence of cyber crime based on gender.

Methodology

Design: The researchers adopted an ex-post facto design for the study.

Area of Study: The study was done in the South East geopolitical zone of Nigeria made up of five states namely; Anambra, Ebonyi, Enugu, Imo and Abia.

Population for the study: All the male and female students in all the nine Federal and State Universities in the South Eastern Zone of Nigeria totalling 30,816 (16,672 males and 14,104 females) comprised the population of the study. (Academic Planning Units of the Universities, 2009).The choice of students was based on the fact that they use the internet frequently both for academic and non academic purposes.

Sample for the study: Multistage sampling technique was adopted. Firstly, simple random sampling technique was used in selecting three State and two Federal Universities. From these universities, faculties of Agriculture and Engineering were randomly selected. Subsequently, sixty respondents (15 males and 15 females from each faculty) were randomly selected from each of the

Universities to make up the 300 respondents for the study.

Instrument for data collection: The instrument used for data collection was Cybercrime Questionnaire (CQ). It is a four point rating scale developed by the researchers to investigate the prevalence, socio economic factors of cybercrimes in Nigeria and preventive measures to help nip the crime in the bud. The scales are Strongly Agree (SA) - four points, Agree (A) - three points, Disagree (D)- two points and Strongly Disagree (SD) -one point. Three experts from Special Education, Guidance and Counselling and Measurement and Evaluation validated the instrument. The instrument has two sections- A and B. Section A dealt on the biographic data of the respondents, while Section B was on the prevalence of cybercrime, the causes and methods of prevention with a reliability coefficient of .87.

Data collection and analysis technique: The questionnaires were distributed using the direct delivery method. The completed questionnaires were retrieved on the spot. Data collected was analysed using mean and standard deviation for the research questions. The decision rule of 2.5 was obtained by computing the arithmetic average of the rating values used in the scale. The null hypothesis was analysed using t-test statistic to test for gender difference at 0.05 level of significance.

Results

The result revealed that the 12 cybercrimes listed are prevalent among the youths in the South Eastern States of Nigeria with internet time theft, polluting youths through indecent exposure, financial crimes, online gambling, forgery and transmitting virus ranked highest. The youths are motivated into cyber crime by unemployment, peer influence as a result of youth gang activities and poverty in the home. The biographic data of cybercriminals indicate that youths between 16 to 20 years, unemployed, school drop outs and those from broken homes are the major culprits. To prevent cybercrime, counsellors should organize seminars and workshops to teach youths the legal means of financial independence through skill acquisition and entrepreneurship instead of the 'get rich quick' mentality, teach them how to be assertive in order to resist peer pressure. Students, school staff and parents should be enlightened on the consequences of cybercrime and self disclosure in terms of uploading photographs or credit card/ATM validation on-line. The cybercafé operators have to monitor the sites accessed by their

patronisers. These are presented in the tables below.

What are the prevalent cyber crimes in South Eastern Nigeria? Ho1: there is no significant difference in the mean ratings of prevalence of cybercrime based on gender. See Table 1.

Table 1: Mean responses and t-test analysis on the prevalent cybercrimes in the South Eastern Nigeria and gender difference.

S/N	Cybercrimes	X1	SD	X2	SD	X3	SD	t-cal	Rmk
	Crime against individuals and their property								
1	Harassment via e-mail (incessant and sometimes threatening e-mails)	2.92	1.00	2.96	1.02	2.82	.98	1.33	n-sig
2	Cyber- stalking-posting mails in cites frequented by victims.	3.04	.93	3.05	.96	3.01	.88	.43	n-sig
3	Dissemination of obscene materials	2.98	.91	2.98	.82	2.99	1.02	-.12	"
4	Defamation/Blackmail-exposure to hatred and rejection by others.	2.94	.99	2.82	1.03	3.13	.87	-3.2	"
5	Unauthorized control/ access over computer system.	2.99	.99	2.96	1.03	3.04	.92	-.70	"
6	Indecent exposure to obscene sites	3.09	.96	3.11	.98	3.04	.91	.77	"
7	E-mail spoofing(showing another address instead of the origin of the mail)	2.97	1.10	2.91	1.14	3.08	1.02	-1.5	"
8	Cheating and fraud	3.07	1.05	3.01	1.07	3.17	.99	-1.6	"
9	Computer vandalism-physical damage or theft of computer system	2.92	.98	2.88	.98	2.98	.96	-.97	"
10	Transmitting virus	3.08	1.06	2.94	1.10	3.31	.94	-3.3	"
11	Forgery of admission and recruitment letters	3.10	.98	3.01	1.05	3.26	.84	-2.5	"
12	Intellectual property crimes(plagiarism/copy write infringement	2.96	1.01	2.89	1.05	3.10	.91	-2.1	"
13	Internet time thefts-using the internet without	3.27	1.68	3.28	4.56	3.25	.84	.11	"

S/N		X1	SD	X2	SD	X3	SD	t-cal	Rmk
	paying.								
B	**Crimes against organizations**								
14	Possession of unauthorized information	2.89	1.02	2.82	1.01	3.02	1.05	-1.7	"
15	Cyber terrorism against government and organizations	2.92	.97	2.88	.94	2.97	1.037	-.89	"
C	**Crimes against society at large**								
16	Pornography (basically child pornography)	3.10	1.05	2.96	1.08	3.34	.92	-3.7	"
17	Polluting the youths through indecent exposure	3.23	1.00	3.07	1.10	3.52	.72	-4.9	"
18	Trafficking on drugs, human beings etc	2.93	1.03	2.82	1.09	3.14	.90	-3.3	"
19	Financial crimes-credit card, ATM theft	3.17	.93	3.06	1.03	3.38	.70	-3.7	"
20	Sale of illegal articles like arms, drugs etc	2.96	.99	2.80	1.06	3.24	.78	-4.7	"
21	Online gambling	3.11	1.02	2.98	1.06	3.32	.91	-3.4	"

Table t=1.96, t-cal = t- calculated, X1= prevalent crimes, X2 = mean responses of the females , X3= mean responses of the males, Rmk= remark,. Number of respondents; females =256, males =144, df =398.

Table 1 shows that all the crimes are prevalent in the south eastern part of Nigeria, with internet time theft, polluting youths through indecent exposure, financial crimes, online gambling, forgery and transmitting virus, ranking highest. There is however, no significant difference in the prevalence of cybercrime based on gender.

What are the reasons for getting involved in cybercrimes by the youths? See Table 2.

Table 2: Mean responses on the reasons for getting involved in cybercrimes

S/N	Causes of Cybercrime	X	S D	Rmk
1	Poverty in the home	3.02	1.08	Agree
2	Curiosity to explore opportunities in the internet	2.87	.93	"
3	Ignorance of the consequences of the crime	2.79	1.04	"
4	Youth mass unemployment	3.20	.95	"
5	Peer influence as a result of joining a gang	3.19	1.07	"

Table 2 shows that peer influence as a result of joining a gang and poverty ranked highest amongst the causative factors of cybercrime.
What are the cybercrime prevention strategies? See Table 3

Table 3: Mean responses on strategies for preventing cybercrime

S/N	Items	X	SD	Rmk
	Strategies for preventing cybercrime			
1	Avoiding disclosing any information about self on the internet.	3.29	1.15	Agree
2	Avoid sending any photograph online particularly to strangers and chat friends	3.30	.88	"
3	Always use latest and up dated antivirus software to guard against virus attacks	3.21	.83	"
4	Never send or validate your credit card or ATM card number in any site that is not secured to guard against fraud.	3,58	.70	"
5	Criminals should be reported to crime control agencies immediately	3.49	.73	"
6	Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children	3.52	.69	"
7	Website owners should watch traffic and check any irregularity on the site.	3.54	.74	"
8	Enlightenment programme in the secondary schools by guidance counsellors to warn students, school staff and parents on the consequences of cybercrime	3.46	.76	"
9	Parents should detect and handle any sign of Emotional Behaviour problems in their children early to prevent cyber crime	3.74	1.87	"
10	Cyber cafe owners should monitor the sites their customers visit	3.37	.87	"
11	Cognitive restructuring of the youths on the need to make money in a clean and legal manner	3.28	.95	"

Table 3 shows that all the items are effective for preventing cybercrime with parents detecting and handling emotional behavioural problem in their children early ranking highest.

Discussion
Results from the study revealed that all the cybercrimes are prevalent in the south eastern part of Nigeria, with internet time theft, polluting

youths through indecent exposure, financial crimes, online gambling, forgery and transmitting virus, ranking highest. This finding lends credence to Odapu's (2008) report that Nigerian letter fraud – Email scams, constituted 1.1% of the 2007 top IC3 complaints received in the US alone. Besides, the amount lost by individuals reporting fraud-type monetary loss in 2007 puts Nigerian letter fraud at 6.4% amounting to 1,922.99 million US dollars. The same report also revealed that Nigeria has the highest number of cyber crime incidents in Africa and is responsible for an estimated eight percent of global cyber crimes.

On reasons for engaging in cyber crime it was found out that unemployment, peer influence as a result of joining a gang and poverty ranked highest amongst the causative factors of cybercrime. It also confirms that youths aged 16-20 years, unemployed, school drop outs and those from broken homes are the major criminals.

This finding is in line with Patti's (2011) submission that frustration due to being sacked or unhappiness with ones employers which may be economically based lead people into cyber crime. The involvement of youths 6-12 years may be due to inquisitiveness or desire to explore things and peer influence which is the developmental stage they are in

according to Eriksons' psychosocial theory of personality development. The study equally revealed that all the items are effective for preventing cybercrime with parents detecting and handling emotional behavioural problem in their children early ranking highest. All the strategies listed are basically informational which is a vital aspect of counselling service. Information is given to students, parents, teachers and even the general public on vital and current issues such as cyber crime through group counselling activities such as seminars, workshops and through the mass media. There is however, no significant gender difference in the prevalence of cyber crime in South Eastern Nigeria. This means that both males and females are prone to cyber criminalities.

Implication for counselling
Cybercrime is real and executed by youths found in secondary and tertiary institutions of learning. Crime of any type is dangerous especially if it is prevalent among youths because its time lag will be long, its dissemination fast and dimension easily multipliable. There is urgent need for School Guidance Counselors and special education teachers to step up personal/social counselling services in secondary schools to arrest the activities of youth gangs in schools, detect and

handle emotional behavioural problems of students promptly to avoid a carry-over to tertiary institutions where they are perfected. Counselors, especially academic staff in higher institutions owe it as a duty to step up enlightenment programmes such as vocational awareness including entrepreneur-ship opportunities, sources of students aid-in-grants and scholarship schemes that will benefit the indigent students in these institutions.

Conclusion

Cybercrime is still raging on in the South Eastern State of Nigeria with Internet time theft, polluting youths through indecent exposure, financial crimes, online gambling, forgery and transmitting virus topping the list. Youths are motivated into cyber crime by unemployment, peer influence due to youth gang activities and poverty in the homes. Unemployed youths, school drop outs and those from broken homes between 16 to 20 years the major cybercrime culprits.

The capacity of human mind is unfathomable and though it has not been quite possible to eliminate cyber crime completely from the cyber space, it is possible to check them. Seeing that cybercrime is basically perpetrated by youths, the services of guidance counselors in schools will help in checking the menace through cognitive restructuring like; organizing seminars and workshops to teach youths the legal means of financial independence through skill acquisition and entrepreneurship instead of the 'get rich quick' mentality and enlightenment programmes to warn students, school staff and parents on the consequences of cybercrime. Besides, Parents should detect emotional behavioural disturbance and handle it early enough with the help of the guidance counsellors and special education teachers. The cybercafé operators have to monitor the sites accessed by their patronisers who in turn should be enlightened on the consequences of self disclosure in terms of uploading photographs or credit card/ATM validation on-line.

Recommendation

It is therefore recommended that:

1. Guidance counsellors especially in secondary schools be empowered with the logistical and financial requirements to carry out the enlightenment programmes that will enable youths develop self confidence, be aware of both sources of students' financial aid schemes and vocational opportunities in the society with emphasis on self reliance through entrepreneurship.

2. Parents and cybercafé operators should censor the cyber activities of their children and customers respectively.

3. The crime watch agencies in Nigeria should not relent in dealing with those cyber criminals already in the society.

References

Atili, A (2011) Wanted! Law for tackling cyber crime. *The Nation;* e-Business August 25th, p. 41.

Ayeni, B. (2000). *Information Technology and Higher Education in Nigeria*. Paper Presented at the First National Conference of the Fulbright Alumni Association of Nigeria (FAAN). University of Ibadan, Nigeria, August7-10.

Denis ,M. A cybercrime. (2009). *Encyclopædia Britannica 2009 Student and Home Edition.* Chicago: Encyclopædia Britannica.

Duggal, P (2011). *Cybercrime*. Retrieved from Narvi.org 11th August, 2011.

Erikson, E. H (1982). *The life cycle completed*. New York; Norton.

Faulkner, W. (2002). *Women, Gender in/and ICT: Evidence and Reflections from the UK*. Retrieved on July 20, 2010 from

http://www.ress.ed.ac.uk/sigis/publ ic/displaydoc/full/Do2-part3.

Fedral Republic of Nigeria (2001). *Nigeria National Policy on Information Technology* (IT). Retrieved on July 13, 2011 from http://www.nitda. gov/docs/ policy/ngitpolicy.pdf

Federal Republic of Nigeria (2004). *National Policy on Education* (4th edition), Lagos: NERDC Press.

Obiyo, N. O. (2006). Effects of self application strategy on socio psychological behaviors of emotionally behaviorally disordered (EBD) pupils. *Unpublished Ph.D thesis of University of Nigeria, Nsukka.*

Odapu, S. M. (2008) Nigeria: Cyber Crime - Time to Stop County's Dominance *Daily Trust 6 September.*

Ofoegbu,T. O.*(2007).* Internet as a Source of Knowledge Generation for Students in higher Institutions in Nigeria. *Review of Education: Institute of Education Journal, University of Nigeria, Nsukka 18(1), 120-125.*

Parker, Donn B. (2009)"*Computer Security*." Microsoft® Encarta [DVD]. Redmond, WA: Microsoft Corporation.

Patti, P (2011) *Cyber crime*. Retrieved 2nd August from Naavi.org.

Zulu,B. (2008) Microsoft Combats Cybercrime in *Nigeria Business Center* Oct, 25.