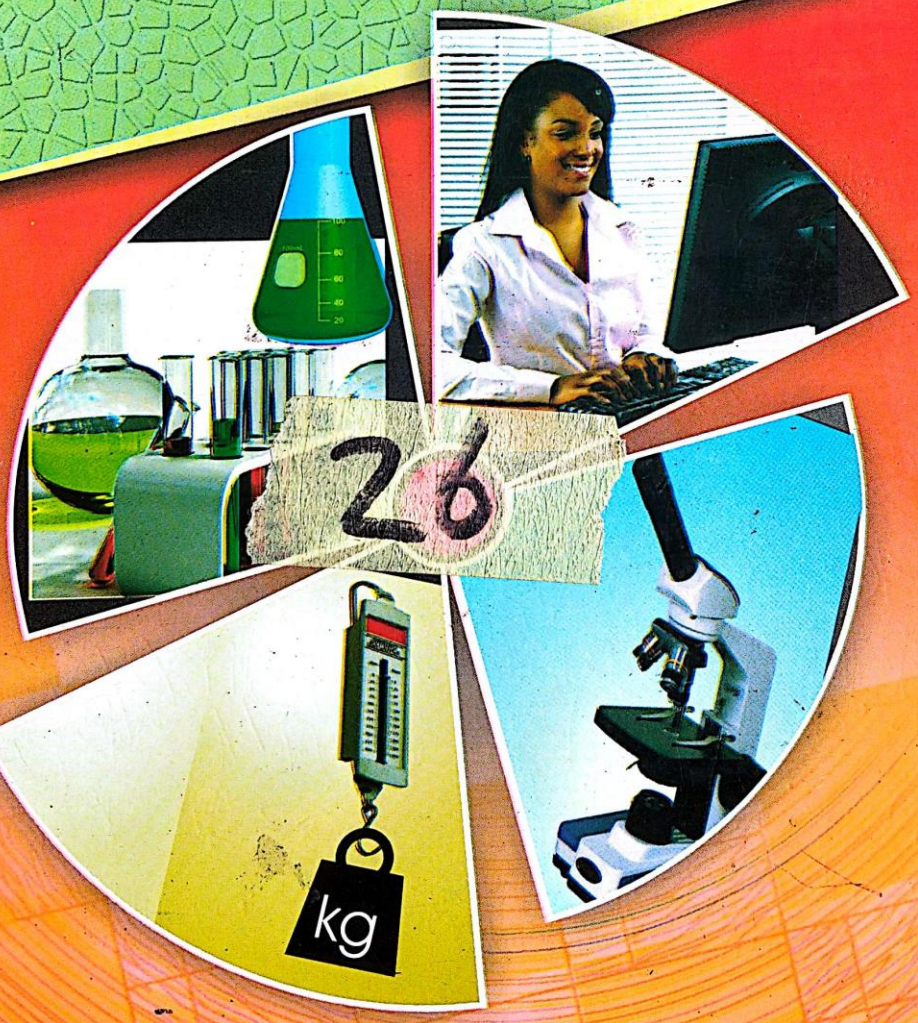
# JOURNAL OF SCIENCE EDUCATION

VOL 12 NO. 1, 2015




SCHOOL OF SCIENCES
NWAFOR ORIZU COLLEGE OF EDUCATION
NSUGBE, ANAMBRA STATE

Ikemelu, C.R.

# JOURNAL OF SCIENCE EDUCATION

Vol. 12, No. 1, 2015

School of Sciences
Nwafor Orizu College of Education
Nsugbe, Anambra State, Nigeria.



✓ 197-209

# An Investigation into the Nature, Causes and Effects of Cyber Crime on World Economy: Implication for Computer Education

By
**Chinelo. R. Ikemelu**
Computer Science Dept.
Nwafor Orizu College of Education, Nsugbe

**Abstract**
*The study investigated the nature, causes, and effects of cybercrime on the world economy: Implication for computer Education. Descriptive Survey designs were adopted and carried out at Nwafor Orizu College of Education Nsugbe. Three hundred and thirty-five (335) students formed the population of the study that was randomly selected from population of six hundred (600) students in the institution. The questionnaire that elicited data on the study was developed by the researcher, duly validated. The reliability of the instrument was tested using Pearson Products movement correlation co-efficient of 0.77 after the pilot study. In the analysis of data, mean and standard deviation were used. The data analysis revealed that hacking, cyber theft, spamming, economics and financial fraud, phishing are the nature of cyber crime committed on the network. This may cause by unemployment, poverty rate, corruption, proliferation of Cybercafés, etc. It was found that effects of cyber crime have given room for many side-effects in the society and entire world economy such as, high costs of security, cost of sales or lower productivity, financial fraud, increasing costs to design resources and technology to combat cyber crime, property loss etc. It was recommended among others that government should make provisions for intensive training of forensic and law enforcement agencies on ICT, so that they can track down the cyber criminals no matter how intelligent and cunning they may be.*

## Introduction

The term "Cyber" is a prefix used to describe an idea as part of the computer and Information age, and "Crime" can be described as any activity that contravenes legal procedure mostly performed by individuals

with a criminal motive (Halder & Jaishankar, 2011). According to Shinder (2002), cyber crime is defined as any criminal offenses committed using the internet or another computer network as a component of the crime. Cybercrimes are offences that are committed against individual or group of individuals with a criminal motive to internationally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones. Such crimes may threaten nation's security and financial health (Akogwu, 2012).

Furthermore, cybercrime is broadly described as criminal or unethical activity in which computers or computer networks are tools, targets, place of criminal activity which includes everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable an illicit activity, (Shinder, 2002). According to Agba (2002), Cyber crime may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may also cause e-media and every system to collapse within a fraction of seconds.

Anderson and Ross (2012) affirmed a comprehensive definition when they stated that "cyber-crime" is given a criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

This includes anything from downloading an illegal music file, stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

As the world is going globalize, educational institutions, organizations such as financial institutions, companies and small business enterprises are

rely on computers and internet-based networking for information exchange. Acording to Fafinski, (2014), there are nearly 2 billion internet users and over 5 billion mobile phones connections worldwide. Every day, 294 billion emails and 5 billion phones messages are exchanged. Most people around the world now depend on consistent access and reliability of this communication channels. As more subscriptions or connection increases to the network there is also an escalation of cyber crime. Cyber crime and digital attack incidents have increased around the world as a result of this connection to the network (Longe et al., 2013).

Information technology revolution associated with the internet has brought two positive functions; firstly, it has contributed positive values to the world (Brenner, 2007). While on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world. The internet online business services, which ordinarily suppose to be a blessing as it exposes one to a lot of opportunities in various field of life is becoming a source of discomfort and atrocity (Akogwu, 2012).

**Geometric Report on Cybercrime**

Cybercrime has become a recalcitrant problem in the foreign countries especially in the United States. According to Center for Strategic and International Studies (2014) found that the United States has notified 3,000 companies in 2014 that they had been hacked, with retailers leading as a favorite target for hackers. According to crime-research.org, as early as 2003 the United States was already leading the world in percentage of cyber attacks at 35.4 percent, followed by South Korea at 12.8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cyber crime. As a result, many hackers and other cyber criminals can flourish in countries with few Internet crime laws while attacking richer countries through their computer.

In Nigeria, perpetrators of this crime who are usually referred to as "yahoo yahoo boys", who are taking advantage of e-commerce system available on the internet to defraud victims who are mostly foreigners thousands and millions of dollars. They fraudulently represent themselves

as having a particular good to sell or that they are involved in a loan scheme project. They may pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have been duped or fallen victims. But these could not only be the techniques used by these cyber criminals.

In Nigerian higher institution also, cyber crimes are perform by students and lecturers. But in most instances the students. Several students in the institution of higher learning engage in cyber crime with the aim of emerging as the best student in an examination, or as a profit making venture since the tools for hacking in our modern world has become affordable by many (Balkin et al., 2006). Recently, The Edo State Police Command has arrested a 31 year old man, for allegedly hacking into the West African Examination Council (WAEC) website. The suspect was said to have opened a website where he posted fake questions and answers of Senior School Certificate Examination (SSCE) for candidates on agreed fees (Vanguard, 2014. Pg 12). Nigeria itself is beset by high rate of poverty- people living below the breadline, high unemployment and corruption. These people are willing to do anything, legal or otherwise, in order to make a living.

It is obvious that internet has been the easiest and fastest means of information transmission. However, since there is no clear legislation in Nigeria about cybercrime, these criminals are free from punishment after perpetration of the act. Their increased activities on the network escalate on daily bases and this leads to malfunction of the network in the organization and the entire world economy.

**Statement of the Problem**

The contribution of internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives. There is a sense of dissatisfaction and general feeling when criminals use computer technology to attack government, institution and organization and individual file or crucial information. This problem has an adverse effect on our economy and the entire world at large, such problems includes.

Lost of funds, Lost of credit card to the hands of cyber criminals which may

be used to cause havoc on the network, Identity theft, Denial of service attack (DOS) which can stop the entire network from working, Loss of Revenue to company which can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization, e.t.c.

The problem of this study is therefore to investigate into the nature, causes and effects of cyber crime on world economy: Implication for computer Education.

**Purpose of the Study**

The general purpose of the study is to investigate the nature, effects and causes of cybercrime on the world economy. Specifically, the study is sought to

1 Investigate the nature of cyber crime committed on the network.
2 Determine the causes of cyber crime.
3 X-ray the effects of cyber crime on world economy and make recommendations based on the findings.

**Research Questions**

Five research questions guided the study:

1 What are the natures of cyber crime committed on the network?
2 What are the causes of cyber crime on the world economy?
3 What are the impacts of cyber crime on world economy?
4 To what extent does cyber crime affects world economy?
5 What are the panaceas to cyber crime?

**Method**

The research design adopted was a descriptive survey. The study investigated the nature, cause and effects of cyber crime on the world economy. According to Akuezuilo and Agu (2003),descriptive research survey describes and interprets what is; it seeks to find out the conditions or the relationship that exist ,opinion that are held, processes that are going on, effects that are evident or trends that are developing. It is also used when the whole population of the study are being used.

The study was carried out at Nwafor Orizu College of Education, Nsugbe. The population of the study comprised all students of Nwafor Orizu College of Education Nsugbe. These population was drawn from the six (6) schools in the institution. Random sampling technique was used for the selection of three hundred and thirty- five (335) students using balloting without replacement from the three randomly selected 6 from the schools of the institution. Two experienced IT lecturers and two experts on measurement and evaluations, of Federal University of Technology Owerri (FUTO), duly validated the instrument. Their comments were used for the final draft of the instrument.

To establish the reliability of the researcher instrument, the researcher collected and tested data using the test-retest reliability method. The scores of data collected were correlated using Pearson Product movement Correlation. The coefficient was 0.77. The instrument used for the study was a structured questionnaire on cyber crime. The questionnaire was distributed by the researcher and research assistant and was collected back promptly.

The mean standard deviation was used to answer research questions. The mean scores of 2.5 and above was accepted as cut-off point for the level of agreement, while any item with mean scores below 2.5 was considered not influential as perceived by the respondents and then was rejected.

## Results

**Research Question 1:** What are the natures of cyber crime committed on the network?

**Table 1**

**Mean ratings and standard deviation of the students on products natures of cyber crime committed on the network.**

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 1 | Hacking | 3.42 | 0.85 | Accepted |
| 2 | Cyber-Theft | 2.93 | 1.07 | Accepted |
| 3 | Viruses and Worms | 2.01 | 1.07 | Rejected |
| 4 | Spamming | 2.67 | 1.07 | Accepted |
| 5 | Economic and financial fraud | 3.12 | 1.18 | Accepted |

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 6 | Phishing | 3.13 | 0.98 | Accepted |
| 7 | Cyber harassment | 2.19 | 0.8 | Rejected |
| 8 | Cyber laundering | 3.10 | 0.81 | Accepted |
| 9 | Website cloning | 2.28 | 0.64 | Rejected |
| 10 | Next of kin scam | 1.55 | 0.8 | Rejected |

The result from table 1 above showed that the items number 1,2 ,4,5, 6 and 8 yielded a mean scores above 2.5, thus were accepted by the respondents as the natures or types of cyber crime committed on the network. While item 3, 7, 9 and 10 have their mean scores below 2.5, thus was rejected by the respondents.

**Research Question 2:** What are the causes of cyber crime on the world economy?

**Table 2**

**Mean ratings and standard deviation of the students on the causes of crime on the world**

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 11 | Unemployment | 3.13 | 1.16 | Accepted |
| 12 | Poverty Rate | 2.90 | 1.15 | Accepted |
| 13 | Corruption | 3.18 | 1.15 | Accepted |
| 14 | Lack of Standards and National Central Control | 3.76 | 0.73 | Accepted |
| 15 | Lack of infrastructure | 1.52 | 0.72 | Rejected |
| 16 | Lack of National Functional Databases | 1.24 | 0.73 | Rejected |
| 17 | Proliferation of Cybercafés | 2.52 | 0.68 | Accepted |
| 18 | Porous Nature of the Internet | 2.54 | 1.25 | Accepted |
| 19 | Excitement to succeed, get-rich syndrome, vengeance and sometimes sabotage | 2.57 | 0.95 | Accepted |

Results of table 2 above showed that items 11, 12, 13,14,17,18 and 19 were all accepted with mean scores above 2.5 as the decisions rule.

**Research question 3:** What Are the Impact of cyber crime on world economy?

**Table 3**

**Mean and standard deviation of the Impact of cybercrime on world economy.**

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 20 | Economic and financial loss | 2.60 | 1.11 | Accepted |
| 21 | Loss of reputation | 3.07 | 1.00 | Accepted |
| 22 | Reduced productivity | 3.18 | 1.15 | Accepted |
| 23 | Intellectual property losses | 2.90 | 0.69 | Accepted |
| 24 | Reputational Damage | 2.34 | 0.99 | Accepted |
| 25 | Increased Cost of Security | 3.10 | 0.91 | Accepted |
| 26 | Impersonating an Antivirus | 2.39 | 0.67 | Accepted |
| 27 | Cost of sales or lower productivity and a decision to avoid the internet for some activities. | 3.00 | 1.3 | Accepted |

Table 3, above showed that all the items received mean scores above the decision rule of 2.5 and were accepted by the respondents as the possible Impact of cyber crime on world economy.

**Research question 4:** To what extent does cyber crime affects world economy?

**Table 4**

**Mean ratings and standard deviation of the cybercrime affects world economy.**

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 28 | Hackers may attempt to take over company servers to steal information that may be detriment to the company | 2.78 | 0.89 | Accepted |
| 29 | Cyber criminals are expert in designing special codes which they normally use for fraudulent act. | 2.66 | 1.14 | Accepted |
| 30 | Criminals on the network can create attractive messages to run across the banking websites and use it for stealing money | 3.12 | 1.18 | Accepted |

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 31 | Cyber criminals can easily access login details and fraudulent transaction to steal peoples' money. | 3.84 | 0.54 | Accepted |
| 32 | ATM services are also prone to fraudulent activities by cyber criminals using various tricks to intercept confidential data in the card. | 3.18 | 1.15 | Accepted |
| 33 | Economic and financial threats are on the increasing rate through cyber crime. | 3.75 | 0.78 | Accepted |
| 34 | Frauds on cyber such mediums facilitate the attacker for illegal activities such as money laundering | 2.85 | 1.19 | Accepted |
| 35 | High costs of security for cyber protection. | 2.61 | 1.02 | Accepted |
| 36 | There are costs in identifying risks, building new and safer operating procedures. | 2.16 | 0.8 | Rejected |

From the results of the analysis in table 4 above showed that items 29,30,31,32,33,34,35 and 36 were designated accepted by the respondents. while items 37 and 38 were rejected.

**Research Question 5: what are the panaceas to cyber crime?**

**Table 5**

**Mean and standard deviation of the panaceas to cyber crime**

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 37 | Adoption of encrypting deployment strategy in technology to avoid interception of messages | 2.50 | 1.01 | Accepted |
| 38 | Installation of firewall for the protection of computer systems | 2.52 | 1.08 | Accepted |
| 39 | Users should be cautions and very careful in down loading to avoid virus. | 2.79 | 0.99 | Accepted |

| S/N | ITEM | Mean ($\bar{x}$) | Std (SD). | Decision |
|---|---|---|---|---|
| 40 | Blacklist unsolicited emails should be avoided | 2.21 | 0.99 | Rejected |
| 41 | Do not share sensitive information with people you don't know in the cyber. | 3.12 | 1.18 | Accepted |
| 42 | Individuals should report all suspected cases of cyber harassment to the law enforcement agency. | 2.19 | 0.8 | Rejected |
| 43 | There should be more centralized co-ordination at regional and interregional levels, to streamline the fight against cybercrime. | 2.52 | 1.08 | Accepted |

Result of Table 5 above showed that items number 37, 38, 39, 41and 43 yielded a mean score above the decision rule of 2.5 and were accepted by the respondents as the remedy to combats cybercrime. While items 40 and 42 were rejected by the respondents as not the major solution to the cybercrime.

**Discussion of Findings**

The study found that hacking, cyber-theft, spamming, economic and financial fraud, phishing and cyber laundering are the types of cyber crime committed on the network. However, majority of the respondents disagreed that viruses and worms, cyber harassment, website cloning, and next of kin scam are types of cyber crime. It is in line with Anah et al (2012), who identified eight types of cyber crime via; Cyber Terrorism, Identity Theft, Drug Trafficking deals, Malware, Cyber Stalking, Spam, Logic Bombs, and Password Sniffing.

It was found that unemployment, poverty rate, corruption, lack of standards and national central control, porous nature of the internet and excitement to succeed, get-rich syndrome, vengeance and sometimes sabotage are the causes of cyber crime on the world economy. They rejected the view that lack of infrastructure, lack of National functional databases and proliferation of Cybercafés cause cyber crime on the world economy.

The findings is in support with Anah et al (2012), who found that

cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system, urbanization, quest for wealth. The research also indicated those items 20-27 were all accepted as the impact of cyber crime on the world economy. Halder & Jaishankar (2011) asserted that cyber crimes may threaten a nation's security and financial health. It was also found that cyber crime have really gone far in affecting world economy negatively. The findings indicated that items 41 and 43 were all accepted as panacea to cyber crime, in the sense that if well adopted, will actually help in solving the problems of fraud in the cyber.

This was buttressed by Mbasekei (2008), who suggested that Telecommunication Regulatory Agencies (TRA) should enhance security on internet service providers' server in other to detect and trace cybercrimes. Also creation of job opportunities for the teeming unemployed youths would go a long way in minimizing the menace of cyber crime.

## Conclusion

The Study has revealed that cyber crime can take many forms such as hacking, cyber-theft, spamming, economic and financial fraud, phishing and cyber laundering. The causes of cyber crime include unemployment, poverty rate, corruption, lack of standards and national central control, porous nature of the internet and excitement to succeed, get-rich syndrome, vengeance and sometimes sabotage.

Cyber crimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. This type of crimes may threaten a nation's security and financial health. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. Some of the ways of combating such crimes include taking reasonable steps to protect ones property by ensuring that firms protect their IT infrastructure like Networks and computer systems; government should assure that cyber crime laws are formulated and strictly adhered to and individuals should observe simple rules by ensuring antivirus protection on their computer systems.

**Recommendations**

Base on the findings, the following recommendation were made:

1. The entire citizens should be educated on the need to maintain and update their systems.
2. The Government should ensure that laws concerning cyber crime are formulated and strictly adhered to.
3. Individuals should observe simple rules, proper anti-malware protection on their computer systems, individuals should also be encouraged to avoid pirated software, never to share their Personal Identification Number (PIN), bank account, email access code to unknown persons.
4. Telecommunication Regulatory Agencies (TRA) should enhance security on internet service providers' server in other to detect and trace cybercrimes.
5. Formal training can be augmented by establishing a cyber security curriculum
in the education system.
6. Government should make provision for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals no matter how intelligent and cunning they may be.

**References**

Adebusuyi, A. (2008) The Internet and Emergence of Yahoo Boys sub-Culture in World. *International Journal of Cyber-Criminology, 0794-2891, Vol.2 (2)* 368-381, July-December

Agba,P.C. (2002), International Communication Principles, Concepts and Issues. In Okunna, C.S. (ed) *Techniques of Mass Communication: A Multi-dimensional Approach.* Enugu: New Generation Books.

Anah Bijik Hassan, Funmi David Lass, & Julius Makinde (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology.*

Akogwu, S. (2012), An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria *(Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria.*

Akuezuilo & Agu (2013) *Research and Statistics in Education and Social Sciences.* Awka: Nuelcenti Publishers and Academic press ltd.

Anderson, Ross (2012). *Measuring the cost of cybercrime, 11th Workshop on the Economics of Information Security* Retrieved, June 7th,2012 .http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., and Zarsky, T. (2006). *Cybercrime: Digital Cops in a Networked Environment.* New York: New York University Press.

Brenner, S. (2007). *Law in an Era of Smart Technology.* Oxford: Oxford University Press.

Ehimen, O.R. and Bola, A, (2010). Cybercrime in World. *Business Intelligence. Journal, January 2010,* Vol.3.No.1. pp. 300-320

Grabosky, P. (2006). *Electronic Crime.* New Jersey: Prentice Hall

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global Publishers Ltd.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2013). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact, 9(3),* pp. 155-165.