IJAAR PUBLISHING® DOI: 10.46654

Scholarly Journal of Social Sciences Research | ISSN: **2955-0785**
Vol. 1, Issue 1 (June, 2022) | www.ijaar.org/sjssr

CYBERCRIME: PREDICTIVE IMPACT ON E-COMMERCE IN NIGERIA

BY

Nwachukwu Ugbomah
Department of Intelligence and Security Studies
Novena University, Ogume
Ugbomahn@gmail.com

Nduka Omede
Department of Business Administration
Novena University, Ogume
Omesco63@gmail.com

And

Obi Christopher Ugochukwu
Department of Intelligence and Security Studies
Novena University, Ogume
xtopterobichris@yahoo.com

ABSTRACT

The influx of criminal elements into the cyber space has been identified as a major problem of internet businesses in the contemporary business world. This study examined the predictive impact of cybercrimes on commence in Nigeria. To achieve this objective, two hypotheses were formulated to establish whether or not there is a significant relationship existing between the two intervening variables i.e. cybercrime and its predictive impact on E-business in Nigeria. Survey research design was adopted and data were obtained from structured questionnaire which was analyzed using Pearson's product-moment coefficient of correlation. The result of the analysis revealed that there is a significant relationship existing between the two variables. Based on these findings, it was therefore concluded that the success of e-commerce depends largely on resolving cybercrime challenges which is now a worldwide phenomenon and to restore customers' confidence in the usage and application of e-commerce requires cohesive and proactively coordinated approach of cyber security system that is backed by appropriate legal framework. The study recommended among others, that the law enforcement agencies should be equipped with the necessary and relevant technological innovations and knowledge so as to catch up with the increasing sophistication and knowledge of cybercriminals.

Keywords: ***Cybercrime, E-commerce, Technological, Innovations Cohesive, Sophistications.***

Introduction

The globe is witnessing a paradigm shift in commerce. Commerce is no longer restricted only to the physical market place, advanced technologies have made electronic and mobile commerce to become very pronounced, popular and attractive.

Turben, et. al. (2008), describe electronic commerce as the application of computer networks including the internet and web for buying, selling, transferring, exchanging products, services or information. According to Akintola, et. al. (2011), e-commerce can be broken down into merchandise (selling goods, services, electronically moving items through distributive channels) and e-finance (online financial services and transfer-debit card, smart card etc.).

Electronic commerce has opened window of opportunities for business organization to improve their market share by not only delivery their products but services faster and cheaper (Abbas, et. al., 2021). Beyond expanding consumer range, it allows customers to shop at their convenient.

The pandemic has promoted the growth of e-commerce websites (UNCTAD, 2021). Electronic commerce has now become a very convenient platform to make purchases with the covid 19 pandemic. The covid 19 pandemic has rendered physical contact risky as people increasingly accept social distancing, isolation and avoiding of public spaces to stay safe and alive. The habit and life style will possibly endure which will further promote e-commerce positively.

There is however growing concern about the use and application of electronic commerce worldwide. The absence of physical contact and surveillance exposes electronic transactions to increase chances of fraud and crimes. Companies and individual consumers are at risk of losing vital information and money to fraudsters.

The rapid growth in digital technology has brought unimaginable risks such as cybercrime. Cybercrime is undoubtedly a contemporary problem not only in Nigeria but the world at large. Internet based platforms which have provided an array of opportunities for individuals and organizations are now potential source of risk.

Statement of the Problem

The use and application of electronic commerce has brought about phenomenal and profound changes for organizations, consumers and society at large. Namehkaren (2013) noted the e-commerce is now a priority for many business organizations as it ensures customers not only having a whole range of products to choose from but also immediate delivery of products. Companies and individual customers are excited with the growth of electronic commerce and are equally worried about the threat posed by cyber criminals. The internet revolution has ushered not only new patterns of crimes but also criminal victimization across the globe (Ndubueze, 2019). It is believed that no individual is totally immune to cyber-attacks from determined and organized community of cyber criminals (Srinivasan,2017). According to Ehime & Bola (2010), the reports on Nigeria cybercrime situation is worrisome and presently damaging the dignity and reputation of the country as a sovereign nation. This research, therefore, is a thorough investigation of the predictive impact of cybercrime on electronic commerce in Nigeria.

Objective of Study

The objective of study is to examine cybercrime and predictive impact on e-commerce in Nigeria. The specific objectives are:

- Find out the underlying causes of cybercrime in Nigeria.
- Ascertain user's perception of e-commerce protection and security
- Identify the predictive impact of cybercrime on e-commerce in Nigeria

Research questions

What are the causes of cybercrime in Nigeria?
Do users of e-commerce feel protected and secured?
What are predictive impacts of cybercrime on e-commerce?

Hypothesis

1. There is no significant relationship existing between cybercrime revealing personal information and e-commerce transactions.
2. There is no significant relationship existing between cybercrime and threats to e-commerce.

Conceptual Clarification

Kumar (2004) defined cybercrime as an unlawful act wherein the computer is a tool or target or both. It simply implies that cybercrime is committed using computer or against computer. Ekemezie & Ngene (2004), consider cybercrimes as computer crimes committed against a computer or telecommunication or the use of computer or telecommunication to accomplish illegal acts. Cybercrimes are illegal activities conducted in cyberspace with clear intent of defrauding either organization or individuals or even putting the computer out of effective order. They are computer mediated activities that are illegal and committed through global networks (Thomas & Loader, 2003). Cybercrimes are harmful activities that are information, global and networked (Wall, 2007). Ehiman & Bola (2010) conceive cybercrime as criminal activities involving information communication infrastructure. The criminal acts involve illegal or unauthorized access, illegal intersection that involves technical means of non-public transmission of computer data to and from or within a computer system and data interference that includes unauthorized damage, deletion, deterioration, alteration, suppression of computer data.

Bremen (2010), posits the variants of cybercrimes that exist are simply a reflection of crimes in the physical space that migrated to the cyberspace. Wall (2001) categorized cybercrime into four types. Which are:

- Cyber trespass- Cyber trespass is the crossing into other people's property online with the intent of causing damage. Examples are hawking, defacement and viruses attack.
- Cyber deception/theft- Cyber deception and theft entails the stealing of money or property online. Examples are phishing e-mails, credit card fraud or violation of intellectual property
- Cyber pornography- it entails the violation of obscenity and decency laws online. Example child pornography.
- Cyber violence- It simply refers to acts of causing psychological harm or instigating physical harm against others online that violate human rights laws. Good examples of this are online hate speech, cyber stalking, etc.

E-commerce is a revolution in business practices (Ohidujjaman, et al., 2013). It is an emerging concept that describes the process of buying and selling or exchange of products,

services and information via computer network including internet (Anupam, 2011). E-commerce means doing business by electronic means (Turban, et al., 1999). It is where business transaction takes place via telecommunication network, particularly the internet. Jamsheer (2019) describe e-commerce as the utilization of telecommunication network to automate business relations and workflow. It involves the buying and selling of products, services and information via computer networks that includes the internet (Timmers, 2000). Bristol (2001) asserts that e-commerce entails the conduction of trade in products and amenities under the assistance of telecommunication and telecommunications centered instruments.

With the advent of the internet, the term e-commerce includes:

- Electronic trading of physical goods and intangible such as information
- All the steps involved in trade such as online marketing, ordinary payment and support for delivery.
- The electronic provision of services such as after sales support or online legal advice.
- Electronic support for collaboration between companies such as collaborative online design, engineers or virtual business consultancy team (Zwass, 2001).

E-commerce has increasingly been a necessary component of business strategy and a strong catalyst for economic development (Hssan, 2010). E-commerce offers a level playing ground for large business as well as small and medium scale enterprises to operate in the global market place (Muhammad, 2013).

The threat in cyberspace is advancing faster than imagined. Ensuring cyber security requires coordinated effort from citizens and the information segment of a country. Cyber security is the body of technology, processes and practices designed to protect network, companies, program and data from attack, damage or authorized access (Ajini, 2017). The goals of cyber security are to accomplish the under listed objectives. Which are:

- To assist individuals, reduce the chances of vulnerability of the information and communication technology(ICT)system network
- To nurture and develop in individuals and institutions a culture of cyber security.
- To ensure collaborative effort of the public, private and international institutions in securing the cyberspace.
- Availability
- To further the understanding of current trends in cybercrimes and effective solution to it.
- Integrity, which will include authenticity and non-repudiation.
- Confidentiality (Ajini,2017).

Theoretical Framework

Risk Society

The theoretical framework adopted for this research is risk society. This research is anchored on risk society as propounded by German sociologist Ulrich Beck. The argument of Ulrich Beck is that society is gradually moving away from traditional and industrial society towards a new modern risk society which is individual, global and self-confrontational (Smith,et.al.1995).

The emerging nature of modern society is that risk tends to multiply with increasing level of complexities of society system of production, consumption, governance and technological control (Wada, et. al. 2012). Modernity is presently characterized by the production and

distribution of risk occasioned by increasing complex techno-scientific system. Jackson, et. al. (2016) asserted that in late modern society, risk is increasing due to technology and science rather by being aborted by technology progress. We are no longer in a world that is less prone to risk but a world of risk, with magnitude of risk so great that it transcends both time and place.

Giddens (1990), distinguish between external risks and manufacture risks. External risks are perceived to be produced by non-human forces (natural disasters). Manufactured risk is the result of modernization process itself resulting from high level of human activities through human agencies. Such risks come from pollution, newly discovered illness and crimes
Longe& Longe (2005), noted that risk society is a society in which the central political conflict is not a class struggles over distribution of resources but instead on non –class based struggles over the distribution of technological risk. As noted by Beck (1992), social production of wealth is accomplished by social production of risk. Technological innovation and advancement comes with unintended risks that portends severe consequences for society
Internet revolution has ushered in digital market, where sellers and customers are satisfied with their business transactions. It has resulted in operational efficiency as well as improving financial performances. E-commerce transaction is a complex system that involves the use of technology and human interaction. E-commerce, like all technological innovation is open to risk, particularly the threat of cyber-crime which we must acknowledge so as to systematical come up with solutions to prevent and minimize it occurrence and threat in the society.

Research Design
Descriptive survey was considered appropriate for this research. Descriptive survey is adopted as it allows researcher the opportunity to observe and describe the phenomenon of investigation in its unaltered state (Barwanlear, 1995).

Area of Study
The area of study is Delta State.

Population of Study
The population of study consists of owners and managers of small and middle enterprises in Delta State. Researcher adopted simple proportion in determining the number of owners and managers of small and middle enterprise in Asaba, Warri and Sapele. The population stands at 2800.

Sample Size and Sampling Technique
In order to obtain an appropriate sample from the target population, the Taro Yamane was adopted.

Taro Yamane
=

$$n = {}^{n}/_{1+N\,(e)^{2}}$$

Where n = sample size sought
e = level of significance

N=2800
=0.0025x2800=7
1+7=8

Hence $^{2800}/_{8=}$ 350.

Sampling Procedure

The simple random method was adopted in picking the sample size from the target population. Simple random method was adopted because of the common characteristics of study population and the fact that every member of the population had equal chance of being selected.

Instrumentation

The instrument that was used for this study is the questionnaire. Self-developed and validated questionnaire that is titled cybercrime and e-commerce in Nigeria and patterned on four point Likert scale was used. The four point Likert scale with response as strongly agree, agree, disagree and strongly disagree.

The questionnaire had two sections which are section A and section B. Section A dealt with persona data of respondents while section B was on subject of investigation.

Validity and Reliability

The validity of research instrument was ascertained through the standard practice of consultation with experts in criminology and cyber security. Their input was taken into consideration in the final questionnaire.

The reliability of the instrument is the consistency with which the instrument measures what it is supposed to measure. This was carried out with the test –retest method. Questionnaire was re-administered to the same group of respondents after one-week period. The test-retest correlation was above 0.05 level of significance.

Data Analysis

Data collected from the field was analyzed with the use of frequency, simple percentage and regression coefficient for the validation or invalidation of constructed hypotheses.

The study was descriptive survey that examined respondent's views and perceptions. Frequency tables, simple percentage and regression were adopted for the testing of hypothesis.

Table 1: Distribution of Respondents by Gender

Option	**Number**	**Percentage (%)**
Male	360	78
Female	100	22
Total	**460**	**100**

Field survey, 2022

Table 1 shows that 360(78%) are male and 100(22%) are female.

Table 2: Age Distribution of Respondent

Option	**Frequency**	**Percentages (%)**
21 – 30	260	57
31 – 40	100	22
41 – 50	60	13
51 – 60	40	8
Total	**460**	**100**

Field survey, 2022.

Table 2 shows that 260(57%) are within the 21 – 30 age group, 100(22%) are within 31 – 40 age group and 60(13%) are within the 41 – 50 age group. 40(8%) respondents are within 51 – 60 age group.

Table 3: Marital status of Respondents

Option	**Number**	**Percentages (%)**
Married	350	76.1
Single	85	18.5
Separated	25	5.4
Total	**460**	**100**

Field survey, 2022

Table 3, shows 350(76.1%) are married, 85(18.5%) are single and 25(5.4%) are separated.

Table 4: Educational Questionnaire of Respondents

Educational attainment	**Number of Frequency**	**Percentages (%)**
School certificate	260	56.5
OND/NCE	100	22
Degree	70	15
Postgraduate	30	6.5
Total	**460**	**100**

Field survey, 2022.

Table 4, shows 260(56.5%) are school certificate holders, 100(22%) are NCE/OND holder, 70(15%) are degree holders and 30(6.5%) are postgraduate degree holders. All respondents are literate and can attend to issues of inquiry.

SECTION B

Table 5: Respondents perception on causes of cybercrime

		SCALE				
S/N	**Item statement**	**SA**	**A**	**D**	**SD**	**Total**
6.	Unemployment/Poverty is contributing factor for prevalence of cybercrime	250	150	50	10	460
		54%	23%	11%	2%	100%
7.	Peer influence account for youth involvement in cybercrime	260	150	40	10	460
		56%	33%	9%	2%	100%
8.	Anonymity in cyberspace fuel cybercrime	300	100	50	10	460
		65%	22%	11%	2%	100%
9.	Weak government polices/uncertainty of punishment account for prevalence of cybercrime	250	150	40	20	460
		54%	32%	9%	4%	100%

Field Survey, 2022

Research question one is on causes of cybercrime in Nigeria. The reason is to ascertain the underlying causes of cyber criminality in Nigeria.

Item 6 which is if unemployment/poverty is contribution factor for cybercrime shows that 250 (54%) strongly agreed, 150(22%) agreed. 50(11%) disagree and 10(2%) strongly disagreed.

Item 7, examined if peer influence account for youth involvement in cybercrime. 260(56%) strongly agreed, 150(33%) agreed, 40(9%) disagreed and 10(2%) strongly disagreed.

Response to item 8 shows that 300(65%) strongly agreed, 150(22%) agreed, 50(11%) disagree and 10(2%) strongly disagreed that anonymity in cyberspace fuels cybercrime.

On item 9, weak government policy/uncertainty of punishment account for prevalence or cybercrime, 250(54%) strongly agreed, 150(33%) agreed 40(9%) disagreed and 20(4%) strongly disagreed.

Table 6: Perception of Respondents on security and protection of e-commerce transactions

		SCALE				
S/N	**Item statement**	**SA**	**A**	**D**	**SD**	**Total**
10.	Cannot ascertain if websites are secured	250	100	50	10	460
		54%	22%	11%	2%	100%
11.	Personal information can be revealed with e-commerce transaction	290	120	32	18	460
		68%	26%	37%	4%	100%
12.	Reuse of personal information for unrelated purposes can result with e-commerce.	260	120	50	30	460
		56.5%	26%	11%	6.5%	100%
13.	Do not have latest information on techniques and tactics of cyber security	260	150	70	30	460
		56.5%	22%	15%	8%	100%

Field survey, 2022.

Table 6 is a perception on security and protection of e-commerce transaction. The reason is to find out if e-commerce transaction is secured and protected. Item 10, on cannot ascertain if websites are secured shows that 250 (54%) strongly agreed, 100(22%) agreed, 50(11%) disagreed and 10(2%) strongly disagreed.

Response to item 11, which is if personal information can be compromised with e-commerce transaction shows that 290(68%) strongly agreed, 120(26%) agreed, 32(4%) disagreed and 18(4%) strongly disagreed.

Item 12, on reuse of personal information for unrelated purposes can result with e-commerce shows that 260(56.5%) strongly disagreed, 120(26%) disagreed, 50(11%) disagreed and 30(6.5%) disagreed.

Item 13, on not having latest information on techniques and tactics on cyber security shows that 260 (56.5%) strongly agreed, 100(22%) agreed, 70(15%) disagreed and 30(6.5%) strongly disagreed.

Table 7: Perception of Respondents on cybercrime on e-commerce

		SCALE				
S/N	**Item statement**	**SA**	**A**	**D**	**SD**	**Total**
14.	Do not trust e-commerce because of prevalence of cybercrime	300	100	40	20	460
		65%	22%	9%	4%	100%
15.	Do not trust internet to work properly to protect transaction in e-commerce	260	120	50	20	46o
		56.5%	26%	11%	6.5%	100%
16.	Cybercrime is detrimental to e-commerce transaction	280	120	40	20	460
		61%	26%	9%	4%	100%
17.	Cybercrime is a threat to everyone in e-commerce	295	125	30	10	460
		64%	27%	7%	2%	100%

Field survey, 2022.

Table 7 is a respondent perception on impact of cybercrime on e-commerce. The reason is to find out is the impact of cybercrime on e-commerce in Nigeria.

Item 14, dwell on do not trust e-commerce because of prevalence in cybercrime shows that 300(65%) strongly agreed, 100(22%) agreed, 40(9%) disagreed and 20(4%) strongly disagreed.

Item 15, do not trust internet to work properly to protect transaction in e-commerce shows 260(56.5%) strongly agreed, 120(26%) agreed, 50(11%) disagreed and 30(6.5%) strongly disagreed.

Response to item 16, cybercrime is detrimental to e-commerce transaction shows 280(61%) strongly agreed, 120(26%) agreed, 40(9%) disagreed and 20(4%) strongly disagreed.

Item 17, cybercrime is a threat to everyone in e-commerce shows 295(64%) strongly agreed, 125(27%) agreed, 30(7%) disagreed and 10(2%) strongly disagreed.

Hypotheses

1. There is no significant relationship existing between revealing personal information and e-commerce transaction.

2. There is no significant relationship existing between cybercrime and e-commerce threat.

Test of Hypotheses

To ascertain the validity and reliability of the research outcome, the hypotheses are tested using the Pearson's product-moment coefficient of correlation.

Test of Hypothesis one

There is no significant relationship existing between revealing personal information and e-commerce transaction.

Data Analysis table

Table 8: Response on the effect of cybercrime, personal information and e-commerce transaction.

Response	**Number**	**Percentage (%)**
SA	290	63
A	120	26
D	32	7
SD	18	4
Total	**460**	**100**

Source: table 5

Table 9: Contingency table

X	**Y**	**X^2**	**Y^2**	**XY**
4	290	16	84100	1160
3	120	9	14400	360
2	32	4	1024	64
1	18	1	324	18
10	**460**	**30**	**99848**	**1602**

Source: Researchers' computation, 2022.

$$r = \frac{n\sum xy - (\sum y)^2}{\sqrt{[\sum x^2 - (\sum x)^2][n\sum y^2) - (\sum y)^2]}}$$

$$\frac{4(1602) - 10(460)}{\sqrt{[4(30) - 10 \times 10][4 \times 99848 - 460 \times 460]}}$$

$$\frac{6408 - 4600}{\sqrt{[120 - 100][4 \times 99848 - 211600]}}$$

$$\frac{1808}{\sqrt{20(399392 - 211600)}}$$

$$\frac{1808}{\sqrt{3755840}}$$

$$\frac{1808}{\sqrt{1937}}$$

$$r = 0.93$$

$$t = r\frac{\sqrt{n-2}}{\sqrt{1-r^2}}$$

$$t = 0.93 \times \frac{\sqrt{4-2}}{\sqrt{1-(0.93)^2}}$$
$$t = 0.93 \times \frac{\sqrt{2}}{\sqrt{1-0.86}}$$
$$t = 0.93 \times \frac{\sqrt{2}}{\sqrt{0.14}}$$
$$t = 0.93 \times \frac{1.41}{0.37}$$
$$t = 0.93 \times 3.81$$
$$t = 3.54$$
$$TableValue = 3.182$$

Decision

From the above calculated value 3.54, when compared with table value t = 3.182, at 5% level of significance, the null hypothesis is rejected, while the alternative hypothesis is accepted and conclude that there is a significant relationship existing between revealing personal information and e-commerce transactions.

Test of hypothesis two

Ho_2: There is no significant relationship existing between cybercrime and threat to e-commerce transactions.

Table 10: Response on the effect of cybercrime e-commerce transaction

Response	**Number**	**Percentage (%)**
SA	295	64
A	125	27
D	30	7
SD	10	2
Total	**460**	**100**

Source: Table 6

Table 11: Contingency table

X	**Y**	**X^2**	**Y^2**	**XY**
4	295	16	87025	1180
3	125	9	15625	375
2	30	4	900	60
1	10	1	100	10
10	**460**	**30**	**103650**	**1625**

Source: Researchers' computation, 2022.

$$r = \frac{n\sum xy - (\sum y)(\sum y)}{\sqrt{[\sum x^2 - (\sum x)^2][n\sum y^2) - (\sum y)^2]}}$$

$$\frac{4(16025) - 10(460)}{\sqrt{[4 \times 30 - 10 \times 10][4 \times 103650 - 460 \times 460]}}$$

$$\frac{6500 - 4600}{\sqrt{[120 - 100][414600 - 211600]}}$$

$$\frac{1900}{\sqrt{20 \times 203000}}$$

$$\frac{1900}{\sqrt{4060000}}$$

$$\frac{1900}{2014}$$

$$r = 0.94$$

$$t = r\frac{\sqrt{n-2}}{\sqrt{1-r^2}}$$

$$t = 0.94 \times \frac{\sqrt{4-2}}{\sqrt{1-0.88}}$$

$$t = 0.94 \times \frac{\sqrt{2}}{\sqrt{0.12}}$$

$$t = 0.94 \left[\frac{1.41}{0.34}\right]$$

$$t = 0.94 \times 4.14$$

$$t = 3.89$$

$$Table\ Value = 3.182$$

Decision

From the above calculated value 3.89, when compared with table value t = 3.182, at 5% level of significance, the null hypothesis is rejected while alternative hypothesis is accepted and concluded that there is a significant relationship existing between cybercrime and threats to e-commerce transactions.

CONCLUSION

Electronic commerce has extended quickly across the globe and it is expected to increase significantly with covid 19 experiences. Covid 19 which has rendered physical contact risky has further promoted e-commerce positively. With the adoption of e-commerce, individuals and organization will save time, be more cost effective and improve business transactions generally. The success of e-commerce depends largely on resolving cybercrime challenge which is now a worldwide problem. To ensure customer's confidence in the use and application of e-commerce requires a cohesive and coordinated approach of cyber security system that is backed by appropriate legal framework.

RECOMMENDATIONS

The prospect of reducing the impact of cybercrime on e-commerce will be bright if the following recommendations are adhered to by appropriate stakeholders. The recommendations are:

- The government should ensure strict laws and enforcement are in place as weak penalties will not act as deterrent.
- Firms should endeavor to secure their information and network.
- Law enforcement agencies should be exposed to latest technological training so as to catch up with the increasing sophistication and knowledge of cybercriminals
- E-commerce users should be educated and enlightened that self-protection is the first line of defense in fraud cases.
- Government must address the challenge of unemployment and poverty, which is the underlying cause of crime in virtually all societies.

References

Ajayi, A., Aderounmu, A. & Soriyam, H. (2008). Improving the respond time of online buyer in Nigeria. The way forward. *Journal of Internet Banking and Comerce*,13(1),1-10.

Akintola, K., Akinyele, R. & Agbonifo, C. (2011). Appraising Nigeria readiness for e-commerce towards achieving vision 2020. Http://www.aspapress.com/volume/vo/aissuez/11RAAS92.

Beck, U. (1992). *Risk society: towards a new modernity*. London: Sage publication.

Bristol, A. (2001). The impact of electronic commerce on tax revenue of the Caribbean community. Regional tax policy Administration unit, George Town Guyana, SA.

.Efenioglu, A., Yip, V. & Murray, W. (2004). *E –commerce in development. Issues and influences.* San Francisco: University of San Francisco.

Giddens, A. (1990). *Consequence of modernity*. Cambridge: Polity Press.

Jackson, T., Jack, K. & Robert, W. (2016). Cybercrime and the challenges of socio-economic development in Nigeria. *JORIND14*(2).

Longe, O & Longe, F. (2005). The Nigeria web content. Combating the pornographic malaise using web filter. *Journal of Information TechnologyImpact*.5(2),12-25.

Longe, O.& Chiemeke, S. (2008). Cybercrime and criminality in Nigeria. What roles are internet access points playing. *Journal of Social Sciences* ,6 (4).

Ndubueze, P. (2017). Cyberterrorism and national security in digital Nigeria. In P. Adejoh & Adisa, W.(ed.). Terrorism and counter terrorism war in Nigeria: Essays in honour of lieutenant General Tukur Buratai. Lagos: University of Lagos Press.

Srinivasan, R. (2017). Hobby hackers to billion-dollar industry: The evolution of ransomware. Computer Fraud and Security, (11), 7-9.

Sumanjit ,D. & Tapaswini, N. (2013). Impact of cybercrime, Issues and challenges. *International Journal of Engineering Sciences and Emerging technologies.* Vol 16(2),142-153.

Sumanjit& Tapaswini, N. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Science and Emerging Technologies* Vol.6 (2),142-153.

Thomas, D. & Loader, B. (2000). Introduction. In Thomas, D. & Loader, B.(ed) *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Turban, E., King, D., Mckay, T., Marshall,F., Ice, T. & Vichleu, D.(2008). *Electronic commerce: A managerial perspective*. New Jersey: Pearson.

UNCTAD (2015). *Information economy report. Unlocking the potential of e-commerce for developing countries*. New York: United States.

UNCTAD (2015). Information economy report2005. Unlocking the potential of e-commerce for developing countries. Unite Nations Publications.

Uwakwe, U. (2016). Prospect and challenges of e-commerce in Nigeria. Hltp://wwwpunchonline.u.ng.com.

Wada, F. & Oduleji, G.(2012). Electronic banking and cybercrime in Nigeria. A theoretical policy perspective on causation. *African Journal of Computer and ICT*.43(3),69-82.

.