ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

Cybercrime and its Implications on the Economy of Nigeria

Stephanie Fitswemila Philip
Advance Fee Fraud Section, Makurdi Zonal Directorate
Economic and Financial Crimes Commission, Nigeria

Abstract:- One of the tenets of globalization is the advancement of Information and Communication Technology (ICT) mainly achieved through computer interconnectivity enabled by the internet in a presumed market place known as cyber space where both buyers, sellers and users in the form of individuals, corporate bodies and government meet. These interconnectivity brought about economic opportunities and inclusion. One of the areas so developed is the e-commerce sector where communication and interactions in the form of transaction is hinged on instant exchange of information, goods and services but, as friendly as these interactions are, they are not without their consequences- Cybercrime is one which often comes with huge financial loss and economic impact. Nigeria in its quest to liberalize trade and digitalize its transactions adopted the use of emerging technologies and services to drive the change but the tools and methods used to enhance the transactions are oftentimes misused by cybercriminals to their benefit thereby causing huge financial losses for the victims and invariably impact negatively on the economy. This research reviewed some existing literature on the subject of cybercrime, and its manifestations within the financial sector while relying on the Social Learning Theory as the reason for the prevalence of cybercrime among youths. Data was drawn and questionnaires administered. Analysis was done using CHI square in the Statistical Package for Social Sciences (SPSS). The study, therefore, concluded that there is a significant relationship between Cybercrime and the Nigerian economy and that Cybercrime had impacted negatively on the growth and development of the digital economy, in particular, and the Nigerian economy at large. Finally, the study offers solutions on how the Internet can engage the various Internet-based platforms, particularly calling on institutions responsible for combating this crime to put every effort required to end this menace.

Keywords:- *Cybercrime, Financial Crime, Digital Economy, E-Commerce.*

I. INTRODUCTION

The Nigerian economy has suffered over the years as a result of several factors which include insufficient policies or lopsided implementation of the policies. These challenges are further compounded by insecurity arising from insurgency and related vices which greatly hampered economic activities across the country. More to these, the 21st Century witnessed advancement in Information and Communication Technology, which has become a major catalyst for interaction within the socio-economic activities of all sectors, and especially in the area of commerce but these benefits, however, came with challenges of computer-based crime, also known as Cybercrime.

Cybercrimes take place in the sphere of the interconnectivity between the computer hardware and the Internet within cyberspace usually perpetrated by having unauthorized access to computers, networks and other data stored in systems. This have consequences as huge amounts of money, sensitive data and intellectual property are stolen through cyber-espionage, identity theft and hacking operations on lucrative targets. Cybercrime has become a disturbing and growing menace globally.

Efforts made at curtailing cybercrimes have not been maximally successful. Even the government is lagging in its understanding of the nature of the crime because of its constantly evolving as well as how to eliminate it. The issue of anonymity that usually shroud the identity of the perpetrators remain a concern. Gathering electronic evidence across jurisdictions far from source has not only proven to be challenging but has often resulted in loss of evidence. Victims (individuals and organizations) who have been swindled of their money or denied access to sensitive data often resign to fate for fear or reputational damage instead of reporting to the authorities. Therefore, the extent of impact made by cybercrimes on the economy is not fully known. The implication is that the setbacks caused by cybercrimes in relation to other forms of organized crimes remain uncertain but a holistic framework for tackling this menace is being improved.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

This study seeks to add to what other researchers (Akogwu, 2012, Olusola, et al 2013, Ene & Jack, 2016) have done. The objectives of this study, therefore, include among others:

- Uncovering public perception on the need for digital-based economy that can adequately cater for 21st Century needs; and
- Determining the implications of cybercrimes on the growth and development of the Nigerian digital economy.

II. LITERATURE REVIEW

With the Internet, life has become dependent on computers and the interaction comes with some level of complexity, irrespective of motive. (Wilsem, 2011) The nature of cybercrime is complex, often manifesting in various dimensions across regions but access to data is usually unauthorized. These kinds of crimes have a severe impact on the socio-cultural lives of people and the economics of the society because societies function maximally through exchange of information.

Globally, Cybercrime affect governments at all levels, organizations and individuals and has continued to occupy global agenda. The threat is not slowing down and the impact increasing by the day. i.e McAfee and the Center for Strategic and International Studies (CSIS) estimates that, cybercrime costs the global economy $600 billion a year – up from a 2014 study which put the figure at $445billion, representing 0.8 percent of global GDP". It is currently estimated to reach $23 Trillion in 2027. (Majwil et al, 2023) The evolution of technology with increased speed and number of internet users has contributed to weakening cyber security.

The motive centers around stealing or diversion of finances directly or indirectly. *Verizon* (2016) Data Breach Investigations revealed that 95% of web attacks are financially motivated and statistics abound to verify this assertion. i.e, The Central Bank of Nigeria (CBN) reported $649 Million to cyber-attacks in six months as a result of phishing and scams across Nigeria in 2017, this figure is significantly up by 174% from $550 Million in 2016 (Business Day, 2018) This was re-emphasized by the Federal Bureau of Investigation (FBI) where its report disclosed that, "the country (Nigeria) ranks third in Electronic Crimes globally surpassed only by the United States of America and the United Kingdom while 91.6 Nigerian residents have access to the Internet".(*Cable News Online*, 2021)

The development of Nigeria's digital economy is equally threatened by growing criminal activities in the Cyberspace as cybercrime shakes trust in the very foundations of digital commerce. Smart technology of the modern age which interconnected devices, adaptive systems and other digital technologies relied on to transform the financial sector are also threatened by cybercrime as trust in such systems are being eroded (Hakmeh, 2017). Despite the aforementioned, there is no sufficient awareness about the nature, manifestation and impact of Cybercrime among the large population of Information and Communication Technology consumers in Nigeria today (Olusola et al, 2013). Lack of awareness on the modus operandi of cyber criminals among computer and internet users including organization and the general public has compounded some of these difficulties.

A. The Concept of Cybercrime

All crimes perpetrated by the aid of computers and its accessories are considered as cybercrimes but scholars have argued that cybercrime is better understood when the word is slit. Saini, Rao and Panda (2021:202), defined, "The term 'Cyber' is a prefix used to describe an idea as part of the computer and Information age while 'Crime' refers to any activity that is contrary to legal procedure, which is carried out by individuals with the aim of causing damage to the victims."

Article 7 of the *Council of Europe Cybercrime Convention* sees cybercrimes as *computer-related fraud* hence defined it as;

"intentional…and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible."

The above definition sees cyber from the perspective of the act of criminality. Halder & Jaishankar (2011:23) see it as, "Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim" but Kamini (2011) defines Cybercrimes as crimes committed on the internet or unlawful acts using the computer as either a tool (e.g. identity theft, phishing scams, spams) or a targeted victim (e.g. unauthorized access to computers networks) etcetera. Mc Connel (2000) lists four characteristics of the computer; it's easy to learn; does not require huge resources to cause huge damage; it defies physical jurisdiction and illegal act is often not clear. The computer, being the centerpiece of cybercrimes, is either the tool or the target of computer based crimes. On the basis of these, the relatively easier way in which these crimes may be committed, they have become a major security challenge to law enforcement agencies in particular and the public in general.

Cybercrime methods vary but as technology advances, new methods of crime emerge and again, the more sophisticated the tools, the more sophisticated the techniques of fraud. (Sandywell, 2009) Ribadu (2017), "the most prevalent forms of Cybercrimes in Nigeria are cloning of websites, false representations, internet purchase and other e–commerce kinds of fraud." However, financial fraud, identity theft, and fraudulent electronic mails popularly known as yahoo-yahoo, Business Email Compromise (BEC), romance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

and dating scams are other forms of cybercrimes prevalent in Nigeria. (NFIU, 2023)

The revolution and continued development of Information Technology is a two-edged sword which is both positive and negative. Communication as well as sharing of ideas from one location of the world to another are faster and easier while transactions are carried out in a flash. Oyewole and Obeta (2002) observe that "the Internet is the interconnection of computers across the world thereby creating unlimited opportunities for mankind" while Okeshola & Adeta (2013:100)said, "the Internet has created a geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. Considering these limitless advantages of the internet, one can easily subscribe to the fact that it is an important tool for national development in a developing country like Nigeria."

Despite the blessings, it also threatens the order of the society through crime (Okeshola & Adeta, 2013). Sceptics are critical of online information originating from Nigeria hence, it is safe to say that the evolution of cybercrimes in Nigeria is becoming a major bane of the benefit of Information Technology to the growth of the economy. Although cybercrimes are carried out by people of all ages, younger people are mostly the perpetrators in Nigeria because it accessible and affordable to many.

The motive for Cybercrimes may be anything, money is mostly the problem; banks and other commercial businesses who deals with money regularly are therefore normally the favorite target of Cybercriminals as *Verizon 2016,* has pointed out, money is the motivation in 95% of cases. In recent times Point of Sale (POS) agents, who serve as Mobile Banks, have increasingly become targets of fraud. In addition to institutions, individuals who are money gatekeepers in their organization like accountants, auditors remain the target of Cybercriminals. In the last decade, the rise of FinTechs and Blockchains as third-party financial providers have further compounded the woes of Banks and specifically online transactions.

B. Cybercrimes and digital economy

Globally, the adoption of cashless policies have accelerated e-fraud with huge consequences. *Business Standard,* 2023 reported $48 Billion losses to merchants in 2023. The situation is not different in Nigeria, to reduce over reliance on cash transactions and to mitigate the problems that comes with a cash trapped economy such ransom payment, election rigging, high cost of handling and processing, bribery, the CBN introduced the electronic payment system which include use of cards, ATMs and POS transactions to facilitate transactions. (Yaqub, et al 2023) The policy is intended to bring about development and modernization in payment system in Nigeria, to drive inclusion and cut cost of banking as well (Ene, Abba and Fatokun, 2019)

E-commerce has been revolutionized by the internet more than anything. Businesses with strong investments in ICT have wider reach of buyers and subscribers than those without the use of ICT. This sub sector thrives on the efficiency of e-payment- an electronic means of making payment for goods and services procured online. (Adeoti, 2013)

Totonchi and Kakamanshadi (2012:2) defined e-commerce as, "the exchange of goods and services between four groups over the internet. This can happen business to consumers, businesses to businesses, intra consumers and consumer to consumer". This process reduces cost, is prompt and instant in the case of payment which methods are usually automated. E-commerce is a facilitator of the digital economy. As *Vanguard, 2021* noted, "E-commerce-based businesses are leading drivers of growth and diversification of Nigeria's economy. The sector is boosting the economy by increasing productivity, encouraging innovation, bettering knowledge management, educating customers and driving finer shopping experiences". The report added that, "The current e-commerce spending in Nigeria is estimated at $12 billion, and is projected to reach an impressive $75 billion in revenues per annum by 2025, according to the International Trade Administration".

The introduction of new technologies to fast track transactions became a turning point for cyber fraudsters who discovered that they could explore all channels of electronic banking for fraud. The adoption of cashless policy triggered the adoption of digital products including wallets and applications with limited or no Know Your Customer (KYC) procedure which is often used to perpetrate fraudulent transactions thereby triggering financial losses especially in the area of e-commerce.

Furthermore, the Covid 19 and Naira re-design policies of the CBN further pushed Nigerian society into an abrupt enforcement of the cashless policy. (Monye, 2024) The resultant effect is what the Chief Risk Officer of Nigerian Inter-Bank Settlement System (NIBSS) reported by *Vanguard*, 2023 said, that "For fraud trends over the last five years, in 2019, we're looking at about N3 billion and currently 2023, we are looking at about N9.5 billion to date. Fraud losses have increased dramatically over the last five years." By the end of 2023, this figure stands at N12.2 Billion. While the channel for the global is through digital wallets, for Nigeria, the NIBBS identify betting platform as the primary channel used in siphoning these, usually cashed out through wallet accounts and POS agents as the conduit where cash is finally drained out of the financial system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

C. Effect of Cybercrime on Nigerian Economy

The financial sector is one of the pillars of the Nigerian economy which intricately weaves the various institutions, both public and private and the markets in a complex interaction under the regulatory watch of the Central Bank of Nigeria. Among other functions of this sector is for the institutions to provide services hinged on technological tools and devoid of risk that is geared towards enhancing efficient service delivery to the overall socio-economic growth. However, Cyber criminals depend on the disruptive nature of these tools to boycott both the regulations and their legal application to disrupt economic activities on a micro and macro level thereby undermining economic growth. Cybercrimes have continued to have an impact on critical sectors of the Nigerian economy.

Cybercriminals have long targeted financial institutions and merchants who deal with voluminous transitions which come with huge financial losses, bad image and competitive disadvantage with competitors. It is said that banks spend thrice as much on cyber security in comparison to non-financial institutions. With the adoption of cryptocurrency in Nigeria, the report on crypto related fraud has only added color to the existing dimension of financial fraud giving rise to money laundering as cyber criminals now prefer using cryptocurrencies, hiding under the anonymity of the wallet addresses to move proceeds of crime with ease across jurisdictions without being noticed.(Emmanuel & Santos, 2019) And it is a consensus among regulators of banks around the world that Cybercrimes pose great risks to global financial stability. It is believed that protection offered by law enforcement, huge budgets around the world, access to talents constitute some of the serious sources of cybercrimes. (Najaf, Mostafiz and Najaf, 2021)

Cybercrimes have severe impacts on society. Ene & Jack (2016:43) said that the effect "ranges from its ability to aid corruption, money laundering, military espionage, and terrorism and on the overall, undermining technological and socio-economic development of any country." Furthermore, Kamini (2011:242) argues that, "a nation with high incidence of crime cannot grow or develop; hence cybercrime leaves negative social and economic consequences." These consequences, according to Ene & Jack (2016:46), "are manifest in all spheres of the nation's socio-economic life and due to the stigma of corruption associated with the country, foreign investors are taking steps geared at blocking emails originating from the country and financial instruments are accepted with extreme caution."

This has of course made international financial institutions to invest in anti-fraud compliance policies and standards designed for the prevention, authentication of transactions, and defense of frauds, while exploring perceived loopholes in the financial network in order to stop these frauds. The *CBN Guidelines on Operations of Electronic Payment Channels and other Regulations* and other guidelines meant to direct and provide operational basis for payment systems seems to have less effect on protection of data as new fraud records continue to break previous records. The efforts of law enforcement have not changed the trend either.

D. Theoretical Framework

The Social Learning Theory explains diverse criminal behaviors. Proponents like Akers believe that people learn deviant behaviors through association and exposure with individuals and peers who are involved in crime. Aker (2009) argues that this "exposure to deviant behavior provided individuals with definitions that are seen as either approving of or neutralizing the behavior... rationalizations for criminals when committing a crime. Differential reinforcement refers to the rewards that are associated with a particular criminal behavior."(p.) One can then deduce that criminal behavior is learnt by mimicking the actions of other persons over time either by listening or watching.

This Theory has explained the development of Cybercrime and also enumerated salient issues in the commission of other Cybercrimes. Basically, the theory helps us to understand that the rationalization and skill to commit crime is often learnt and re-enforced through association with others. The proliferation of cybercrime through a network of syndicates spread across jurisdictions, learning the trade sometimes set up like formal education such as the operation of *"Yahoo Academy"* where other youths with similar demography are taught the art of deception through computer tricks and manipulation is a testament to this Theory. (*EFCC, 2024*)

III. METHODOLOGY

Survey, which studies large and small populations, is adopted as the research design for this study. Samples are selected from the population and studied in order to find the relative incidence, distribution and interrelation of sociological and psychological variables. Members of the general public, workers in financial institutions, business owners, students, and security agents make up the population of this study. The population figure from the study was 100 respondents. The study is conducted in Makurdi, Benue State, Nigeria. Makurdi is located in the Middle Belt along the Benue River, lying between latitudes 7.7411N and longitudes 8.5121E. Makurdi metro area has an estimated population of 407,000. Sampling method was applied to selecting units of analysis from a larger population and Random Sampling is used to obtain the portion of the target population while Taro Yamane's method n = N/1+N (e) 2 is used for analysis.

The Statistical Package for Social Science (SPSS) software is used in analyzing the data in this study. Data collected is analyzed using frequencies and percentages which enabled the study to present true data characteristics and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

findings with a great deal of accuracy. Data Interpretation and analysis is also used to describe items in tables.

IV. FINDINGS AND DISCUSSION

The analysis of data is based on the number of questionnaire distributed and the responses received from respondents.

Table 1. Age Grade of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 20 years	15	15.0	15.0	15.0
	21-30 years	15	15.0	15.0	30.0
	31-40 years	30	30.0	30.0	60.0
	41yrs and above	40	40.0	40.0	100.0
	Total	100	100.0	100.0	

Source: field survey, November, 2019

15 respondents which represent 15.0 percent of the population are below 20yrs. 15 respondents which represent 15.0 percent of the population are between 21-30yrs. 30 respondents which represent 30.0 percent of the population are between 31-40yrs; While 40 respondents which represent 40.0 percent of the population are 41 years and above. This shows a fair representation of sample.

Table 2. Cybercrime has Effect on the Growth and Development Nigerian Economy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	45	45.0	45.0	45.0
	Agree	20	20.0	20.0	65.0
	Disagreed	25	25.0	25.0	90.0
	Strongly disagreed	10	10.0	10.0	100.0
	Total	100	100.0	100.0	

Source: field survey, November, 2019

Table 2 above shows the responses of respondents that cybercrime has an effect on the growth and development of the Nigerian economy.

Forty-Five (45) respondents, which represent 45.0 percent of the population, strongly agreed while 20 respondents, which represent 20.0 percent of the population, agreed that Cybercrime has an effect on the Nigerian economic growth and development. Twenty-Five (25), respondents which represent 25.0 percent of the population, strongly disagreed that Cybercrime has an effect on the Nigerian economic growth and development while the remaining 10 respondents, which represents 10.0 percent of the population, disagreed that Cybercrime has an effect on the growth and development of the economy. This implies that Cybercrime has an effect on the Nigerian economic growth and development.

Table Two above makes the percentage distribution to the statement that Cybercrime has an effect on the Nigerian economic growth and development. Increase in Cybercrime has a negative effect on the economic growth and development of Nigeria. This is arrived at based on the number and percentage of respondents who supported it. 45 respondents, who represent 45% of the population, strongly agreed and another 20% agreed. Only 25% of the population disagreed that Cybercrime has an effect on the Nigerian economic growth and development. From the foregoing, it can be seen that Cybercrimes have negative impact on the socio-economic development of any country.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

Table 3. There are Implications of Cybercrime on the Nigerian Economy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	53	53.0	53.0	53.0
	Agree	17	17.0	17.0	70.0
	Disagree	20	20.0	20.0	90.0
	Strongly disagree	10	10.0	10.0	100.0
	Total	100	100.0	100.0	

Source: field survey, November, 2019

Fifty-Three (53) respondents, which represent 53.0 percent of the population and 17 respondents, which represent 17.0 percent of the population, strongly agreed and agreed respectively that there are implications of Cybercrime on the Nigerian economy. Twenty (20) respondents, which represent 20.0 percent of the population, disagreed. Consequently, ten (10) respondents, which represent 10.0 percent of the population, strongly disagreed that there are implications of Cybercrime on the Nigerian economy. This implies that there are implications of Cybercrime on the Nigerian economy. This is because the responses from most of the respondents are in the affirmative.

The widely held perception of the public is that Cybercrimes have consequences on the economy of Nigeria. This can increase skepticism in e-commerce, especially when larger sums of monies are to be shipped through online platforms across locations. The fear of losing funds, uncertainty about the trustworthiness of certain payment platforms, quality of products among other factors are contributing to the grounding of the growth and development of the digital economy in the country.

V. CONCLUSION AND RECOMMENDATIONS

It is evident from this study that cybercrime is wreaking havoc on the economy of Nigeria. There is also increasing negative perception of e-transactions, which is a consequence of Cybercrime. These among other things are championing the hindrances to the growth and development of the digital economy in particular and the Nigerian economy at large. The study concludes by alerting the public to be aware of the alarming rate and the extent of damage of Cybercrime on the economy. The Law Enforcement institutions such as the Police, EFCC and ICPC, who investigate this crime, should continue to bridge knowledge gap towards uncovering its nature and dimensions and as well deploy every known and affordable technology in fighting the crime. Furthermore, Governments at all levels should support unemployed youths who are the majority of perpetrators of cybercrime by channeling their energies towards profitable technological engagements and providing an environment where micro businesses can thrive in the Nigerian economy.

REFERENCES

[1]. Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology. *Second Asia International Conference on Modeling and Simulation. Beijing: AICMS. pp 77-82*

[2]. Adeoti. O. O. (2013). Challenges to the efficient use of point of sale (POS) Terminals in Nigeria. *African Journal of Business Management. pp 2801-2806*

[3]. Akers, R. L. (2009). Social learning Theory in Encyclopedia of Criminological Theory. *Sage Publication Inc. pp 22-30.*

[4]. Akogwu, S. (2012). An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria. Available at iResearch.com

[5]. Business Standard, 2023. *E-commerce losses due to online fraud to exceed $48 billion globally.* Available at https://www.business-standard.com/article/current-affairs/e-commerce-losses-due-to-online-fraud-to-exceed-48-billion-globally

[6]. Business Day, 2022. *Nigeria recorded a 174% increase in cybercrimes in six months, here's why you should be bothered*. Available at https://businessday.ng/news/article/nigeria-recorded-a-174-increase-in-cybercrimes-in-six-months-heres-why-you-should-be-bothered/

[7]. Cable News Online, 2021. *Nigeria ranked 16th in FBI global Cybercrimes report.* March 18, 2021. https://www.thecable.ng/nigeria-ranked-16th-in-fbi-global-cybercrime-victims-report

[8]. Centre for Strategic and International Studies. 2018. Economic Impact of Cybercrime at $600 Billion and Counting - No Slowing Down. February 21, 2018

[9]. Central Bank of Nigeria, 2020. Guidelines on the operations of electronic payment channels in Nigeria.

[10]. *Daily Trust, (2018).* "The Menace of Internet, Mobile Phone and Scammers." December, 2018.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1539

[11]. EFCC, 2025. EFCC arrest 14 Suspected Internet Fraudsters in a "Yahoo Academy" in Makurdi. [Online] Accessed from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9776-efcc-arrests-14-suspected-internet-fraudsters-in-a-yahoo-academy-in-makurdi

[12]. Ene R. W., & Jack T. B. C. (2016). 'Cybercrime and the Challenges of Socio-Economic Development in Nigeria.' *JORIND 14(2) December, 2016. ISSN 1596*-8303.

[13]. Ene E. E., Abba G. O, and Fatokun, G.F. (2019). The Impact of Electronic Banking on Financial inclusion in Nigeria. *American Journal of Industrial and Business Management, 2019. pp 1409-1422*

[14]. Hakmeh, J. (2017). *Cybercrime and the Digital Economy in the GCC Countries.* Chatham House. pp 1-20

[15]. Halder, D. and Jaishankar, K. (2011). 'Cybercrime and the Victimization of Women: Laws, Rights, and Regulation. *Hershey, PA, USA: IGI Global. ISBN 978-160960830-9. pp*

[16]. Kamini, D. (2011): Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences* (*2011) Vol 3, No 1, pp 240-259.*

[17]. Mc Connell (2000), Cyber Crime and Punishment. Archaic Law Threaten.

[18]. Mijwil M.M, Filali, Y, Unogwu O.J. and Bala, I. (2023). Exploring the top five emerging threats in cyber security. *Mesopotamian Journal of Cyber Security*. *Vol 2023. pp 57-63*

[19]. Monye, E. (2024). Why Nigeria's controversial naira redesign policy hasn't met its objectives. *Carnegie Endowment for International Peace*. *January, 2024. pp 2-4.*

[20]. Najaf, K., Mostafiz K, & Najaf R. (2021). Fintech firms and banks sustainability: Why Cyber security risk matters? *International Journal of Financial Engineering VOL. 08, N0. 02 pp 1-2*

[21]. Nigeria Financial Intelligence Unit, (2023). Money Laundering Typologies through Fraud in Nigeria. *pp 1-20*

[22]. Oyewole, A.S. and Obeta, A. (2002). An Introduction to Cyber Crime. [Online] Available at http//www.crime-research.org/articules/cyber-crime.

[23]. Okeshola B. F & Adeta A. K. (2013): The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research. Vol. 3 No. 9; September 2013.*

[24]. Ribadu, N. (2007), Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna. July 2007 (unpublished)

[25]. Saini, H., Rao, Y. S., & T. C. Panda (2012). Cyber-Crimes and their Impacts: A Review *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622. Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209*

[26]. Totonchi, J. and Kakamanshadi G. (2012). Relationship between globalization and e-Commerce. *International Journal of e-Commerce, e-Management and e-Learning. Vol. 2. N0. 2012. pp 1-5*

[27]. Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science*. *pp 45-51.*

[28]. Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8(2), pp 115-127*

[29]. *Vanguard (2023).* Banks lose N9.5bn to e-fraud in 2023. [Online] Available at https://www.vanguardngr.com/2023/08/banks-lose-n9-5bn-to-e-fraud-in-2023/

[30]. *Vanguard, (2021).* Social Media: Facilitating e-commerce for the digital economy. [Online] Available at https://www.premiumtimesng.com/opinion/477293-social-media-facilitating-e-commerce-for-the-digital-economy

[31]. Verizon, (2016). Verizon's 2016 Data Breach Investigations Report finds Cybercriminals are exploiting Human Nature. [Online] Available at https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human

[32]. Yaqub J. O, Bello H. T, Adenuga I. A and Ogundipe M. O. (2013). The Cashless Policy in Nigeria: Prospects and Challenges. *International Journal of Humanities and Social Sciences*. *Vol. 3. N0. 3. February, 2013. pp 200-211*