The Socio-ethical and Economic Implications of Cybercrime in Nigeria: A Narrative Study

Nneamaka Philomena Ojukwu PhD
Department of Religion and Human Relations
Nnamdi Azikiwe University Awka
np.ojukwu@unizik.edu.ng 08067966338
&
Casimir N Osigwe
Department of Religion and Human Relations
Nnamdi Azikiwe University Awka
cn.osigwe@unizik.edu.ng 08039463270

Abstract

The use of computers and the internet has brought a visible revolutionary change in our modern society. People make use of computers and the internet for different reasons and purposes. However, the reason for the invention of the computer and internet services is to make life easier and more comfortable but unfortunately, those with negative mindsets have deviated from the purpose thus the emergence of cybercriminals. This paper analyses the economic and socio-ethical implications of cybercrime in Nigeria. The paper uses both qualitative and quantitative methods of data collection from secondary source publications for the work. It has been discovered that cybercriminals have destroyed a lot of organizations as well as some private individuals by illegally trespassing into their databases. Similarly, the greater percentage of the people involved in cyber crimes in Nigeria are the youth. The major causes of this malady are identified to be youth unemployment, the quest for wealth, lack of strong criminal laws as well poor parenting among others. This scenario has damaged the image of Nigeria before the international community and has scared a lot of foreign investors from coming to invest in Nigeria. This paper therefore narrates and suggests different ways through which this malady can be controlled.

Keywords: Socio-ethical, economy, cybercrime, Nigeria, narrative and study.

Introduction

Cybercrime is a global issue that is not peculiar to Nigerians alone. It is a criminal act that is directly involved the use of computers and internet networks for its execution. However, as the internet is becoming popular every day, organizations such as banks, churches, schools, government agencies and even private individuals are relying heavily on it and other information technology to engage in communication and conduct their business activities. In line with this thought, Ekeji (2013) avers that most organizations, institutions, agencies and governments today depend on computer networks to carry out both simple and complex business operations, engage in technological advances, perform interdependent financial transactions and also disseminate classified information. This simply confirms that a visible revolutionary change has emerged in communication and socio-economic transactions via the Internet. Information and communication technology (ICT) systems are used virtually in all works of life.

Furthermore, as these developments allow for enormous gain, productivity, efficiency and communication, they also create loopholes which may destroy an organization. It is these loopholes when inadequately managed that create an avenue for cybercrime. Investigating the same subject matter, Okeshola (2013) opines that the term cybercrime can be used to describe any dubious activity which involves the use of a computer or internet network. Similarly, Herman et al (2012) view cybercrime as a criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or online data or sabotage of equipment and data. Still on this, Omodumbi et al (2016) writes that cybercrime is a term used for such crime such as fraud, theft, blackmail, forgery and embezzlement in which computers or networks are used. The Council of Europe Convention on Cybercrime (2001) agrees that any criminal offence committed against or with the help of a computer network is identified as cybercrime. Wall (2005) stresses that cybercrime is committed online and is often not clearly linked to any geographical location. In support of this view, Gjata (2007) maintains that the emergence of new technology has increased the number of perpetrators that take advantage of these resources to use them illegally for their own gain. Cybercrime can never be possible without the use of computers and the internet and for the cyber world to be adequately protected from abuse, there is an urgent need for information security, ethical education and other awareness programmes.

Types of Cybercrime

It is very difficult to find out all the types of cybercrime because every day new dimensions of cybercrime are invented. Omodunbi et al (2016) state that as the internet grows to become more accessible and more services become reliant on it for their daily operations so does the threat landscape. The cases of cybercrime are increasing at the same rate the internet service is spreading. Hamid et al (2014) identify two major categories of cybercrime which they termed active and passive computer crimes. They state that an active computer crime occurs when someone obtains access to a secured computer environment or telecommunication device without authorization (hacking) while passive computer crime occurs when someone uses a computer to both support and advance illegal activity.

However, in Nigeria, cybercriminals change their modus operandi regularly and as such there are many types of cybercrime of which we are going to cite a few.

- **Identify theft**: This involves the retrieval of vital information about someone to get access to his personal information site so as to perform unlawful transactions on his or her behalf without his or her knowledge and permission. Reyns (2013) asserts that identity theft can be seen as the deceitful act or fraudulent intentional unauthorized use of a person's identifying information for an unlawful or criminal purpose without their consent. Similarly, Wall (2013) educates that it is an online fraud that encompasses the cloning or duplication of someone's digital information or online account with the intention of committing identity fraud against an individual or organization. Hamid et al (2014) say that it is an act of obtaining sensitive information about another person without his or her knowledge and using this information to commit theft or fraud. For Nweibineli and Aguoshim (2021), it is an act of using trickery to gain a dishonest advantage over or steal someone's personal information to perform an unlawful transaction on someone's behalf without the person's knowledge. It has been observed that the internet has given cybercriminals the opportunity to obtain such information from vulnerable companies' databases. It has also enabled the victims to believe that they are disclosing sensitive personnel information to a legitimate business. Sometimes, it comes as a response to an e-mail asking to update billing or membership information. Sometimes it takes the form of an application to a fraudulent internet job posting.

  Besides, identity theft is not peculiar to private individuals alone. Sometimes companies, banks, religious organizations and some other big organizations are victimized. Reyns and Hamson (2016) explain that big organizations also experience data breaches involving customer or consumer data being leaked or stolen, thereby leading to the occurrence of identity theft using information gained from these breaches.

- **Financial fraud**: This type of cybercrime is common in Nigeria. Billions of naira are lost annually by consumers who have their credit cards and calling card numbers stolen from online databases. At times the criminals steal the PINs of the users and, with their cards, use them to withdraw all the money in their victims' accounts. Fafinski (2008) maintains that financial crime includes Internet banking, credit and debit card fraud and money laundering. Similarly, Ekeji (2013) agrees that in Nigeria people design web link forms requesting users to fill in their basic information including unique details like PINs and use that to commit crimes. Sometimes, they engage their prey in a telephone conversation claiming to be staff or an account officer from their victim's bank so as to get the needed information from the victim. The use of ATMs and credit cards, which were meant to provide convenience and comfort for their users, has become a means of stealing people's money by cybercriminals.
- **Illegal e-Lotteries**: Most Nigerians especially youths are being duped by cyber criminals through this means. Due to the highly visible gap between the rich and the poor in Nigeria, the youths who want to become millionaires overnight always fall prey to those criminals who always set traps for them through their illegal e-lotteries. According to Fasuyi (2015), most Nigerian youths are eager to travel abroad and those scammers are aware of this and they respond by creating online visa lotteries to rip off unsuspecting youths. It is worth noting that even American and Canadian visa lotteries have been used to defraud many Nigerians, especially the youth. He explains further that the quest to get rich quickly by most Nigerians is often exploited by online criminals who send all kinds of tempting messages of an existing lottery bonanza (though fictitious) where participants can win all sorts of items and money ranging from cars, houses, electronics, laptops, to mention but a few.
- **Hacking**: This is about illegal access, defacing, hijacking and eavesdropping. Hamid et al (2014) state that hacking is the unauthorized access and subsequent use of other people's computer systems. It is one of the most analysed and debated forms of cybercriminal activity that is also very common in Nigeria. Individuals, organisations and companies have suffered a lot at the hand of these criminals through hacking.
- **Internet Pornography:** Internet pornography has been a disturbing trend, especially among youths. According to Fasuyi (2015), it involves using the internet to download and transmit pornographic pictures, videos, writing etc. He stresses that it is an avenue used for luring unsuspected children to paedophilic activities and the distribution of child pornography. Still on this, Brenner and Goodman(2002) opine that pornography and other offences against morality include child pornography and other offences against minors, stalking, harassment, hate speech etc. Mohammed et al (2012) concur that this category of cybercrime covers a range of conduct that has objectively ascertainable sexual elements including paedophilic activity such as grooming a child for sexual activity.

Causes of cybercrime

A lot of factors have been considered by so many scholars as the major causes of cybercrime in Nigeria. Hassan et al (2012 cited in Omodunbi et al 2016) identify the following as the major causes of cybercrime in Nigeria.

- **Unemployment**: The alarming rate of youth unemployment in Nigeria is quite disheartening and it has pushed many Nigerian youths to embrace any means of livelihood whether acceptable or not. Omodunbi et al (2O16) report that over 20 million graduates in Nigeria are not gainfully employed. Ibrahim (2020) writes that the youth unemployment rate is currently about 47% and some of the unemployed youths as a matter of survival engage in some criminal activities. Ajufo (2013) notes that the unemployed youths have decided to take matters into their hands by engaging in unwholesome acts, increasing militancy, violent crimes, kidnapping, restiveness and political instability. The number of unemployed youths keeps increasing annually as the universities and other institutions of higher learning are graduating their students who are qualified. The rate at which jobs are provided does not commensurate with the number of the labour force in the country. Besides, the Nigerian government does not encourage private-sector business cum entrepreneurship.

- **Quest for wealth**: It will not be out of place for one to say that youths nowadays are not ready to start small hence they strive to keep up with their rich counterparts by engaging in cybercrimes and other criminal activities. Moreover, the ostentatious display and celebration of wealth in Nigeria have pushed some of those young people into going to an extreme. Even religious bodies are not exempted as many keep celebrating anyone who donates huge amounts of money without caring how the money was made. Ekeji (2013) avers that there is a large gap between the rich and the average and as such many strive to keep up using the quickest means possible. In line with this thought Atta-Asamoah (2009) concurs that in a region suffering from serious poverty with a rising youth unemployment rate and endemic corruption, the flamboyant display of wealth by cybercriminals has become a lure to the poor and unemployed youths desperate to share in the wealth.
- **Lack of strong criminal laws**: The Nigerian criminal laws do not address cybercrime directly and adequately; and without an existing strong and defined law to govern the cyber activities in Nigeria, the menace of cybercrime will not be checked. Sulieman (2019) submits that Nigeria’s lack of strong cybercrime laws is the reason most youths venture into “yahoo yahoo”. Ekeji (2013) writing on this issue says that weak/fragile laws regarding cyber criminals exist in Nigeria, unlike the real world where criminals such as armed robbers are treated with maximum penalties. Osuntuyi et al (2021) in support of this view say that Nigerian laws are effective against crimes perpetrated in the physical world but not in the digital space due to a lack of technology to combat cybercrime. It is this unfortunate situation of not being well equipped with sophisticated hardware to track the virtual forensic criminal that aggravates cybercrime.
- **Desire for revenge**: Most of these cyber criminals otherwise known as “Yahoo boys and girls” are of the opinion that their mission is to revenge what the Europeans that colonized Africans did to their forefathers. Some are of the opinion that colonial masters stole a lot from Africans during their African enterprise and as such must pay for their crimes. Suleman (2019 cited in Osuntunyi et al, 2021) echoes this point when he says that Yahoo boys believed that the colonial masters had brutally enslaved their great grandfathers; thus, in return, they wanted to collect their entitlement, while others have flawed confidence that they have wanted to retrieve the money that European people borrowed from their great grandfathers.
- **Poor parenting**: Parents are the first teachers to inculcate good morals and values in their children. When parents fail in their duties in the upbringing of children /wards the result is always catastrophic. Anozie and Amelo (2013) aver that effective parenting is hard work and all involved in trying to mould the moral character of a child. Obi (2013) affirms that some parents have neglected their duty at the expense of wealth and other material factors, and the abused house helpers have taken over the precious role of parenting. It is obvious that sometimes these parents who are always occupied with their jobs may not know the whereabouts of their children. These children grow up to be a menace to society.

Socio- ethical and economic Implications of Cybercrime

The use of modern technology is quickly expanding in developing countries and Nigeria is embracing the innovation seriously. As the economy is increasing its reliance on the internet, it is as well exposed to all the threats posed by cybercriminals. Hemraj et al (2012) observe that internet-based cybercrime has become a huge menace threatening the socio-economic and technological advancement of Nigeria. Maitanmi et al (2013) equally observe that cybercrime obstructs socio-economic growth in Nigeria. It frightens both local and foreign investments owing to the lack of trust. Omodunbi (2016) testifies that the Nigerian economy, including the enormous amount of e-business, is greatly threatened by the rapid increase in e-crimes. Similarly, Uzochukwu et al. (2019) opine that cybercrime has painted a crimophobia image of the country before the international community which has scared both foreign and local investors away and limited their interest to invest in the country.

Furthermore, Jackson and Ene (2016) succinctly give some potentially negative impacts cybercrime has on the socio-economic development of Nigeria as follows

- Widespread cybercrime has tarnished the image of Nigeria before the international community thereby making the country unsafe for foreign investors.
- Cybercrime has negatively impacted the confidence Nigerians have in the digital economy thus inhabiting digital growth.
- Cyber-attacks against business and organisations has the ability to damage the reputation of an organisation and result in a loss of customers and revenue.
- The need to develop measures to combat and respond to cyber-attacks imposes significant costs on businesses and organisations.
- Financial losses accrued by consumers and businesses resulting from the theft of information and money or extortion impedes economic growth.
- Nigeria’s critical infrastructure may be targeted by cyber-attacks and this can lead to immediate and long-term economic losses.
- Cybercrime has the potential to fuel other criminal activities and increases the cost of time and resources for law enforcement agencies.
- It can lead to the loss of business assets and cost to government agencies and businesses in re-establishing credit histories, accounts and identities.
- Loss of personal financial resources and the subsequent emotional damage. Nigeria has been enlisted among the nations where cybercrimes are widespread and it poses a serious threat to the socio-economic development of Nigeria. Besides, cybercrime is gradually turning our society into a morally bankrupt society. Morality which is the bedrock of every progressive society is gradually being swept under the carpet. Moral values such as hard work, honesty and industriousness are no longer virtues to emulate. The quick money-making syndrome is now the order of the day. The idolization of wealth and materialism is a big challenge and it has eaten deep into our system. In line with this, Ndubueze (2013) explains that the traditional value orientation that prices a good name over silver and gold seems to be fast declining. He stresses that virtues of handwork, integrity, and self-reliance are fast being displaced by what he termed “hot cash” “grab-all” and “hit and run” syndrome.
- A greater percentage of Nigerian youths want to hit it big without minding the consequences of whatever that is involved. Adeniran (2011) observes that our society is exposed to youth who have been disillusioned and have not been taught the good virtue of genuine hard work. Such youth have had no trouble immersing themselves in

the internet phenomenon of "Yahoo boyism". Some of these Yahoo boys and girls, who have no regard for human persons, involve themselves in some ritual killings and also employ the use of some extraordinary powers to carry out their activities. Osuntuyi et al (2021) agree that Yahoo boys/ girls make use of spiritual ingredients that can help them to successfully scam their victims by hypnotizing them even though their victims might be aware of the precedence of cybercrime. It has become obvious that today one's personal qualities and virtues no longer count; the wisdom, nobility and majesty of simplicity, frugality and modesty have seemingly become of the past.

Conclusion and recommendations

No human society has achieved a completely crime-free society; rather what every society strives to achieve is to reduce the rate at which certain crimes are committed. However, for any society to develop, it must create an uncomfortable system and environment for criminals. The issue of cyber security must be addressed seriously as it is affecting the image of the country in the outside world. Nigeria's government should create stronger laws for cybercrime and be able to enforce such laws.

Besides, there is a serious need for job creation in Nigeria, but this should not be the role of the government alone. The private sector should equally assist in creating jobs for the young graduate. More so, creating vocational skills and entrepreneurial programmes should help to reduce the percentage of unemployed youth in Nigeria. Furthermore, all faith-based organizations should help in resetting the minds of the youth through their preaching. They should be at the forefront of preaching the values of peace, honesty and hard work. Ministers of religion should preach against the unhealthy quest for quick money that is now the order of the day, and the celebration of the rich with questionable character should be condemned. Also, parents should play their roles well by starting early in life to inculcate in their children the importance of those good moral values. They can as well create time to interact with their children to know when they start deviating from those values inculcated in them.

References

Adeniran, A. I. (2011) Cafe Culture and Heresy of Yahooboyism in Nigeria, Jaishankar, K(eds) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* London CRC Press pg3-12

Ajufo,B.I.(2013) Challenges of Youth Unemployment in Nigeria: Effective Career Guidance as a panacea African Review,7(1)pg307-321

Anozie,C. and Amelo, H.(2013) Morality as the Kpim of Social Order in Ukagba, E.U Obi, D.O and Nwankwor,J.l.J.(eds) *The Kpim of Social Order* American Xubris

Atta-Asamoah, A.(2009) The Impulsive Upsurge of Yahoo-Yahoo in the 21st Century in Nigeria: Islamic Perspective. *African Journal of Criminology and Justice Studies 12(1)pp91-104*

Brenner,S.W and Goodman,M.F(2002) Cybercrime: The need to Harmonize National Panel and Procedural Laws Retrieved from *http://www.isrcl.org/paper/brenner.pdf*

Convention on Cybercrime, a unique instrument for international co-operation Budapest Council of Europe Retrieved from *http//convention.coe.mt / treaty /EN/ projects. htm*

Ekeji, C. (2013) Cyber Crime in Nigeria Retrieved from *https// www.academia.edu*

Fafinski,S.(2008) UK Cybercrime report Retrieved from http: //www.garlik.com

Gjata,S.(2007) Cybercrime Retrieved from http://mason.gmu.edu/ogjata/index.html

Hamid,T. etal (2014) https//www.reseachgate.net/publications/280488863

Hassan, A. B. etal(2012) Cybercrime in Nigeria: Causes, Effect and the Way Out, ARPN Journal of Science and Technology, Vol. 2(7) 626-631

Hemraji, S. etal(2012) Cyber Crime and their Impacts: *A Reviewed International Journal of Engineering Research and Application (IJERA) vol 2 (2) pp202-209*

Jackson, T.C.B and Ene, R. W(2016) Cybercrime and Challenges of Socio -Economic Development in Nigeria *JORIND 14(2) 2016*

Maitanmi,O.(2013) Impact of Cybercrime on Nigeria Economy. The International Journal of Engineering and Science (IJES) Vol 2(4) 45-51

Ndubueze,P.N (2013) Generation Y and online victimization in Nigeria: How Vulnerable are younger respondents? A paper presented at the second International Conference of the south Asian Society of Criminology and Victim ology (SASCV) January 11-13,2013 at Kanyakumari Tamil Nadu India

Nwabineli, T.C. and Aguboshim, F.C.(2021) Strategies for Identity Theft Prevention and Countermeasures in Nigeria: A Narrative Study, *International Journal of Advance in Engineering Management (IJAEM) V3 (1) Jan-Feb 2021 pp:826-832*

Obi, D.O (2013) Family Values and Social Order in African Contemporary Context in Ukagba E.U Obi, D.O and Nwankwor,J.l.J.(eds) *The Kpim of Social Order* American Xubris

Omodunbi, B.A. etal (2016) Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology V1(1)

Osuntunyi, P.M etal (2021) Youths and Cyber Insecurity in Nigeria: The role of Religion in Mitigating against the Yahoo Yahoo Phenomenon.

Reyns, B.W (2013) Online routines and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct Contact Offense. Journal of Research in Crime and Deliquency 50(2) 216-238

Reyns, B.W and Henson, B. (2016) The Thief with a Thousand Face and the Victim with none: identifying Determinants for online Identity Theft Victimization with routine Theory. *International Journal of Offender Therapy and Comparative Criminology Vol 60(10) 1129-1139 http://doi.org/1177/0306624× 15572861*

Suleiman, A. O(2019) The lmpulsive Upsurge of Yahoo-Yahoo in the 21st Century in Nigeria: Islamic Perspective. *African Journal of Criminology Justice Studies AJCJS12(1) 99- 104*

Uzochukwu, C. etal(2019) An Exploratory Study of Cybercrime in the Contemporary Nigeria Value System. European Journal of Social Science Studies vol 4(3),131-141

Wall,D. S(2005) The Internet as a Conduit for Criminal Activity in Pattavina,A. (ed) Information Technology and the Criminal Justice System. Saga Publication USA

Wall,D.S.(2013) Policing Identity Crimes: Policing and Society https/doi.org/10.1080/10439463.2013, 780224