HOW CYBERCRIME IN NIGERIA

Olakunle Mercy Risikat, Chiamaka
S1 Law Study Program
Faculty of Law and Business
Abia State University
Uturu, Nigeria
e-mail: olakunlemercyrisikat@gmail.com

ABSTRACT: *Advances in global telecommunication infrastructure, including computers, mobile phones, and the Internet, have brought about major transformation in world communication. In Nigeria, the young and the old now have access to the world from their homes, offices, cyber cafes and so on. Lately, internet or web-enabled phones and other devices like iPods, and Blackberry, have made internet access easier and faster. However, one of the fall outs of this unlimited access is the issue of cybercrime. Consequently, cybercrime, known as "Yahoo Yahoo" or "Yahoo Plus", is a source of major concern to the country. Nigeria's rising cybercrime profile may not come as a surprise, considering the high level of poverty and high unemployment rate in the country. What is surprising, however, is the fact that Nigerians are wallowing in poverty despite the huge human and material resources available in the country. With the aid of the human security approach, this paper aims to (i) establish a nexus between poverty and cybercrime in Nigeria; (ii) examine the efforts of the Nigerian government in forestalling cybercrime; and (iii) suggest measures that could be put in place to help in curbing cybercrime as well as bringing about poverty alleviation. The paper suggests that the government must put viable policies and programmes on poverty reduction and eradication in place. However, these policies and programmes need to be judiciously backed by actions*

Keywords : Cybercrime; Poverty; Nigeria

INTRODUCTION

The advent of computers and the internet has opened a vast array of possibilities for the young and the old in the international community to have access to the world from their homes, offices, cyber cafes and so on. In recent times, internet or web-enabled phones and other devices like iPods, and Blackberry, have made internet access easier and faster. Not so long ago, computers were large, cumbersome devices utilised primarily by government, research and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims (Clough, 2010).

The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes (Clough, 2010). Thus, one major consequence of this

unlimited access to the world has been an increase in the spate of cybercrimes. Numerous crimes of varying dimensions are committed daily on the Internet worldwide. Majid (2006, pp.3-4) expressed it thus:

Businesses cite threats to economic performance and stability, ranging from vandalism to "e-fraud" and "piracy"; governments talk of "cyberwarfare" and "cyberterror", especially in the wake of the September 11 attacks; parents fear for their children's online safety, as they are told of perverts and paedophiles stalking the Internet's "chat rooms" looking for victims; hardly a computer user exists who has not been subjected to attack by "viruses" and other forms of malicious software; the defenders of democratic rights and freedoms see a threat from the state itself, convinced that the Internet furnishes a tool for surveillance and control of citizens, an electronic web with which "Big Brother" can watch us all. The development of the Internet and related communication technologies thus appears to present an array of new challenges to individual and collective safety, social order and stability, economic prosperity and political liberty.

In international relations, cybercrime occupy an important and increasingly strategic role and has reflected in the formation of major international bodies and various treaties and bilateral, regional and international agreements among nations of the world (Kshetri, 2013). The most significant international instrument in the field is the Council of Europe Convention on Cybercrime (2001). As of September 2016, 52 countries had ratified, accessed or signed it. It has been followed by many from developing regions including the Commonwealth Model Law on Computer and Computer-related Crime (2002) and the African Union Convention on Cyber Security and Personal Data Protection, adopted in June 2014. There are also initiatives at the European level.

Similarly, the Shanghai Cooperation Organization (SCO), which has Kazakhstan, China, the Kyrgyz Republic, Russia, Tajikistan and Uzbekistan as its members, has taken significant steps towards cybersecurity cooperation. To institutionalize cybersecurity relations, many countries have also signed bilateral and multilateral treaties and agreements. For instance, in August 2012, Malaysia and China signed a memorandum of understanding (MoU) to combat trans-border crimes, which will focus on human trafficking, drug smuggling, terrorism and cybercrime. The two countries have realized the importance of regional and international cooperation as they involve syndicates with regional and global networks (Kshetri, 2013). Furthermore, laws are rapidly being enacted to control cybercrime. As of November 2014, 117 countries (of which 82 developing and transition economies) had enacted such legislation, and another 26 countries had drafted legislation underway (UNCTAD, 2015).

According to a 2011 World Bank survey, out of the top ten countries in the world with a high level of cybercrime prevalence, Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa). According to another study, the top five hotspots for cybercrime are, first, the Russian Federation, followed by China, Brazil, Nigeria and Viet Nam (Time, 2014). Also, the 2010 Internet Crime Complaint Center Report ranked Nigeria third in the hierarchy of

nations with the highest prevalence of cybercrime (IC3 Report, 2010). Hence, Nigeria is considered one of the major hubs of cybercrime in the world.

Ironically, despite her huge resources and potentials, Nigeria is considered one of the poorest countries in the world. Using the human security approach, this paper examines the menace of cybercrime in Nigeria, and the nexus between cybercrime and poverty in the country. It argues that the alarming increase in poverty level in the country accounts largely for the increase in cybercrime.

This has serious consequence for human security in the country. Many unemployed graduates in the country are involved in cybercrime, most often out of desperation in the bid to survive or to rescue their families out of the grip of poverty. The poverty situation in Nigeria is a paradox since the country is endowed with a lot of natural, material and human resources which can be harnessed, and developed to generate employment and reduce, if not eliminate poverty in the country. The paper suggests measures that could be put in place to help in curbing the menace of cybercrime as well as bringing about poverty alleviation.

PROBLEM

Based on the background above, the problem formulation in this paper contains, among others:

1. What is the Cybercrime ?
2. What is the Condition Cybercrime in Nigeria ?

RESEARCH METHODS

This type of research is a type of normative legal research with secondary data collection through statutory regulations, journals, legal facts, and internet news. The results of the study were analyzed qualitatively to determine the role of the Land and Spatial Planning Service Officials in regulating legal issues for building permits and what are the inhibiting factors for building permits.

DISCUSSION

1. Defining Cybercrime

   A major problem for the study of cybercrime is the absence of a consistent current definition, even among those law enforcement agencies charged with tackling it. According to the Council of Europe (COE) Convention on Cybercrime, cyber-crime involves “action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data” (Council of Europe, 2001). To the Federal Bureau of Investigations (FBI), cybercrimes spans across a diverse scenario including; crimes against children (usually involving child pornography or child rape); theft of intellectual properties and/or publications, phishing, intentional dissemination of malware to national and international internet fraud. Casey considers internet crimes and frauds to be any crime that involves computers and networks, including

crimes that do not rely heavily on computers (Casey, 2004). And Thomas and Loader (2000, p.3) conceptualize cybercrime as those "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".

Thus, in general terms, cybercrime can be defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It encompasses all illegal activities perpetrated by one or more people referred to as scammers, hackers, internet fraudsters, cyber citizens or 419ners, using the internet through the medium of networked computers, telephones and other information and communications technology (ICT) equipment. Cybercrimes target laptops, tablets, mobile phones and entire networks. Mobile merchants are reported to be incurring the greatest fraud losses as a percentage of revenue amongst all merchant segments (LexisNexis, 2013).

It is very difficult to classify cybercrimes in general into distinct groups. Cybercrime can take many shapes and can occur anytime or at anyplace. Cyber criminals utilize several methods, depending on their skill-set and their goal. Regardless of the nature of the intentions, each method of cybercrime requires a set of skills, knowledge, resources, and access to particular data or information systems. One classification that is helpful to this study is that by Wall (2001, pp.3-7). He sub-divides cybercrime into four established legal categories:

a. Cyber-trespass—crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.
b. Cyber-deceptions and thefts—stealing (money, property), e.g. credit card fraud, intellectual property violations also referred to as piracy.
c. Cyber-pornography— breaching laws on obscenity and decency.
d. Cyber-violence—doing psychological harm to, or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking.

It sub-divides cybercrime according to the object or target of the offence: the first two categories comprise "crimes against property", the third covers "crimes against morality", and the fourth relates to "crimes against the person". To these we may also wish to add "crimes against the state", those activities that breach laws protecting the integrity of the nation and its infrastructure (e.g. terrorism, espionage and disclosure of official secrets). Such a classification is helpful, as it allows us to relate cybercrime to exist conceptions of prohibited and harmful acts (Majid, 2006).

2. Cybercrime in Nigeria

Cybercrime is a very popular crime in Nigeria. Cybercriminals in Nigeria are notorious for luring people across the planet into fraudulent scams via spam mails, cash-laundering e-mails, and cleverly designed but pretend company partnership offers. Criminals involved in the advance fee fraud schemes (419) known as "yahoo yahoo" are popularly referred to as "yahoo boys" in Nigeria. Yahoo yahoo is the most popular local

name for cybercrime in Nigeria. It usually involves the use of email, particularly through a Yahoo address or yahoo messenger to con unsuspecting victims. The nation has therefore carved a niche for herself as the source of what is now generally referred to as "419" mails named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

The "yahoo boys" use various methods in getting their victims. Many of these fraudsters patronize cyber cafes, browsing the internet all night, sending scam mails to unsuspecting victims. Many foreigners, especially females, who are seeking for spouses via the Internet have fallen victim of the "yahoo boys". They pretend to be ready to go into a lasting relationship with these women and subsequently start to exploit them. Some of them get their victims to help in procuring travel documents to where they reside or even to assist in getting residential permits for them. Once they have been able to achieve their aims, they stop communicating with the victim and move on to another target (Adesina, 2012).

In other instances, the scammers use stories of severe life circumstances, tragedies, family deaths, personal injuries or other hardships to keep their victims concerned and involved in their schemes. They also ask victims to send money to help overcome alleged financial hardships. Many of the victims just lick their wounds and carry on life, but some of the very bitter victims report to the appropriate authorities who often apprehend and prosecute the suspects. The situation is worsened by the fact that several non-Nigerians apprehended for cybercrimes most often claim to be Nigerians before they are thoroughly investigated and their country of origin established.

Demonstrating the gravity of the problem of cybercrime in the country, in 2007, a young Nigerian musician, Olumide Adegbolu (also known as Olu Maintain) released a hit song called "Yahooze". The song, which sparked a lot of controversies, speaks of a flashy lifestyle, fancy trips and expensive drinks, if the songster is able to "hammer" (obtain) 1 million dollars and coverts it into Naira (Nigerian currency). Critics argued that the song was a glorification of internet fraud or "Yahoo Yahoo", pointing out that for a young man to think of living such a life style if he gets such a huge amount of money, he must be a scammer. This has been vehemently denied by Olu Maintain himself claiming that the song was just a reflection of his rise to fame and the change money has made to his life.

The song and the whole controversy that trailed it reflects the current trend of thinking of many Nigerian youth. The quest to possess and ride flashy cars and live frivolous lifestyles have lured many Nigerian youth into the "yahoo yahoo" business. It is not unusual to enter a cybercafé and find that most of the people there are (mainly) boys in their 20's or early 30's who are browsing the internet in search of potential victims. There is even what is called "night browsing" where, for a fee, they stay on the internet all through the night to carry out their businesses. The boys often team up to practice

their businesses in other to be able to get ideas from each other. Also, as seen in Figure 1 below, many of them also have

A Typical Yahoo Yahoo Operation Source: Nkereuwem, 2010.

However, in recent times, because of some stringent measures put in place by many financial institutions and various organizations that do online transactions, the cybercriminals in Nigeria apparently suffered a setback in their activities. To this end, the more desperate among them has had to resort to spiritual means to enhance their businesses. This is referred to as "Yahoo Plus". Yahoo plus is an advanced form of yahoo yahoo whereby the "yahoo boys" employs traditional spiritual means like voodoo or juju to hypnotize their victims into doing their bidding and parting with whatever amount of money they request for. The yahoo boys indulge in occultic ritual practices to enhance their potential to defraud people. It involves employing traditional spiritual means like voodoo or juju in ensuring that the cybercriminal hypnotizes his victims and thereby brighten the swindler's chances of getting his victims hypnotised. Once this is successfully done, the victim is guaranteed to keep remitting money from wherever he or she is in the world. There are various strategies deployed in achieving this feat. The yahoo boy approaches a spiritualist or diviner who consults, the "oracle" or the "gods". He is then given diverse options of rituals to perform.

CONCLUSION

The paper attempted at establishing a nexus between poverty and cybercrime in Nigeria from the human security perspective. While one can blame cybercriminals in Nigeria as being lazy or greedy, the stark reality is that most of them perpetuate the act as a means of escaping the reality of poverty. To them, yahoo yahoo business is a means of survival. According to the popular maxim, "The idle hand is the devil's workshop"; the situation whereby majority of the people are poor and hungry and a lot of youths are jobless and unemployed, will, doubtlessly, lead to high crime rate in the country.

As noted earlier, cybercrime has negative impact on the economy as well as the image of the country. And with the increased use and dependence on technologies, there is an increase in the risk posed by cybercriminals. Thus, there is need for a holistic approach to combat this crime in all ramifications. To there is a need for educating the Nigerian public on the ills of cybercrime and killing of human beings for the sake of rituals.

Additionally, a strong legislation on cybercrime is imperative for combating the crime. Therefore, there is a need to ensure the effectiveness of the 2015 Cybercrimes Act. Cybercafés in the country must be properly regulated. It must be ensured that they are properly registered with the relevant agencies like the Corporate Affairs Commission. Surveillance hardware that will help in keeping tab on internet usage and detect cybercrime must be put to proper use. Also, the country's intelligence agencies must be equipped with the right skills and equipment that will facilitate detection and handling of cybercrime in the country.

Furthermore, while law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. More international coordination and cooperation are, therefore, essential in fighting the scourge of cybercrime.

Finally, simple vigilance can go a long way in the fight against cybercrime. A significant percentage of cybercrimes can be prevented by just getting the cyber basics right such as updating software, having strong passwords and regular system back-ups.

REFERENCES

Adesina, O. S. (2012). The negative impact of globalization on Nigeria. International Journal of Humanities and Social Science, 2(15), 193-201.

Advanced Fee Fraud Act. (2006). Laws of the Federation of Nigeria.

Ağır, B. S. (2015). European perspective of human security: From a conception to the reality? In I. Dordevic, M. Glamotchak, S. Stanarevic, & Gacic (Eds), Twenty years of human security: Theoretical foundations and practical applications (pp.365-374). University of Belgrade and Institut Français de Geopolitique—Universite Paris 8, Belgrade.

Ajakaiye, D. O., & Adeyeye, V. A. (2002). Concepts, measurement and causes of poverty. CBN Economic & Financial Review, 39(4), 35-45.

Aluko, M. A. O. (2003). Strategies for poverty reduction in Nigeria. Journal of Social Sciences, 7(4), 255-266.

Casey E. (2004). Digital evidence and computer crime. St. Louis, MO: Elsevier Press.

Chapsos, I. (2011). The human security and international organised crime nexus: The "balkan route". RIEAS. Retrieved from http://rieas.gr/images/chapsos.pdf

Chawki, M. (2009). Nigeria tackles advance fee fraud. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/ jilt/2009_1/chawki/chawki.pdf

Clough, J. (2010). Principles of cybercrime. Cambridge: Cambridge University Press.

Commission on Human Security (CHS). (2003). Human security now. Retrieved from http://www.un.org/humansecurity/ sites/www.un.org.humansecurity/files/chs_final_report_-_ english.pdf

Council of Europe (COE). (2001). Convention on cybercrime. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/ html/185.htm

Cybercrimes Acts 2015. (2015). Retrieved from http://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_ 2015.pdf Economic and Financial Crimes Commission (Establishment). (2004). Laws of the Federation of Nigeria Act.

Fields, G. (1994). Poverty changes in developing countries. In R. Van Der Honven & R. Anken (Eds.), Poverty monitoring: An international concern. New York: St. Martins Press.

Fukuda-Parr, S., & Messineo, C. (2012). Human security. In K. B. Graham & A. Langer (Eds.), Elgar handbook of civil war and fragile states (pp.21-38). Cheltenham: Edward Elgar Publishing.

IC3 Report. (2010). 2010 Internet crime report. Retrieved from http://www.ic3.gov/media/annualreport/2010_ic3report. pdf

Iroegbu, S. (2016). Nigeria loses over N127bn annually through cybercrime. Retrieved from http://www.thisdaylive.com/ index.php/2016/04/19/nigeria-loses-over-n127bn-annuall ythrough-cybercrime/

Kshetri, N. (2013). Cybercrime and cybersecurity in the global south. Hampshire: Palgrave Macmillan.

Lasania, Y. Y. (2016). 90 per cent of foreigners involved in cybercrime are Nigerians. Retrieved from http://www. thehindu.com/news/cities/Hyderabad/90-per-cent-offoreigners-involved-in-cyber-crime-are-Nigerians/ article14572630.ece

LexisNexis. (2013). True cost of fraud 2013 study: Manage retail fraud. Retrieved from http://www.lexisnexis.com/risk/ insights/2013-true-cost-fraud.aspx

Majid, Y. (2006). Cybercrime and society. London: SAGE.

McAfee Inc. (2014). Net losses: Estimating the global cost of cybercrime. Retrieved from https://www.mcafee.com/ ca/resources/reports/rp-economic-impact-cybercrime2.

Mutum, R. (2012). Nigeria: 288 jailed for internet fraud–EFCC.

Retrieved from http://allafrica.com/stories/201204170197. html

National Bureau of Statistics. (2010). The Nigeria poverty profile 2010 report, Abuja. Retrieved from http://reliefweb.

int/sites/reliefweb.int/files/resources/b410c26c2921c18a683 9baebc9b1428fa98fa36a.pdf

National Bureau of Statistics. (2011). 2011 annual socioeconomic report. Retrieved from http://www.nigerianstat.gov.ng/uploads/latestRelease/2ff063b27de8aa15b35f1a6f b04bf472c658d939.pdf

Nkereuwem, E. (2010). Nigeria comes 3rd in global cybercrimes survey. Retrieved from http://www.abujacity.com/abuja_ and_beyond/2010/11/nigeria-comes-3rd-in-globalcybercrimes-survey-.html

Ogwumike, F. O. (2002). An appraisal of poverty reduction strategies in Nigeria. CBN Economic & Financial Review, 39(4) , 1-7.

Olowu, D. (2009). Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa. Journal of Information, Law and Technology (JILT), 1, 1-18.

Ribadu, N. (2007). Cyber-crime and commercial fraud: A Nigerian perspective. Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission On International Trade Law), Vienna, Austria, 9-12 July. Retrieved from http://www.cnudmi.org/ pdf/english/congress/Ribadu_Ibrahim.pdf

Richard, O. (2016). Nigeria: Putting the cybercrime law to test in 2016. Retrieved from http://allafrica.com/ stories/201601060369.html

Rishi, R., & Gupta, V. (2015). Strategic national measures to combat cybercrime: Perspective and learning for India. Retrieved from http://www.ey.com/Publication/ vwLUAssets/ey-strategic-national-measures-to-combatcybercrime/$FILE/ey- strategic-national-measures-tocombat-cybercrime.pdf

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

The World's Top 5 Cybercrime HotspotsTime. (2014, August 7).Time. Retrieved from http://time.com/3087768/the-worlds-5- cybercrime-hotspots/

Townsend, P. (1962). The meaning of poverty. The British Journal of Sociology, xii(1), 210-270.

UNCTAD. (2015). Information economy report 2015: Unlocking the potential of e-commerce for developing countries. New York and Geneva: United Nations Publication.

United Nations Development Programme. (1994). Human development report. Retrieved from http://hdr.undp.org/ sites/default/files/reports/255/hdr_1994_en_complete_ nostats.pdf

United Nations. (1998). Statement of commitment for action to eradicate poverty. Retrieved from http://www.unsceb. org/content/acc-statement-commitment-action-eradicatepoverty-22-june-1998

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (Ed.), Crime and the internet. London: Routledge.

World Bank. (1992). Operational directive 4.15. Washington D.C.: World Bank.

World Bank. (2003). Voices of the poor. World development report. Washington D. C.: World Bank.