CSCanada
Canadian Social Science
Vol. 13, No. 4, 2017, pp. 19-29
DOI:10.3968/9394

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

Cybercrime and Poverty in Nigeria

Olubukola Stella Adesina[a],*

[a]Senior Lecturer, Department of Political Science, University of Ibadan, Ibadan, Nigeria.
*Corresponding author.

Received 18 January 2017; accepted 9 March 2017
Published online 26 April 2017

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.

Key words: Cybercrime; Poverty; Nigeria

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science, 13*(4), 19-29. Available from: http://www.cscanada.net/index.php/css/article/view/9394
DOI: http://dx.doi.org/10.3968/9394

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.

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. THE COST OF CYBERCRIME

McAfee Inc. (2014) notes that cybercrime is a growth industry. The returns are great, and the risks are low. They estimated that the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow. The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen—incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China.

The most important cost of cybercrime, however, comes from its damage to company performance and to national economies (McAfee Inc., 2014). Cybercrime damages trade, competitiveness, innovation, and global economic growth. What cybercrime means for the world is that:

- The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.
- Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.
- Governments need to begin serious, systematic effort to collect and publish data on cybercrime to help countries and companies make better choices about risk and policy (McAfee Inc., 2014)

3. CYBERCRIME AND HUMAN SECURITY

There is a nexus between human security and cybercrime and between human security and poverty. Human security is commonly understood as prioritising the security of people, especially their welfare and safety, rather than that of states (Ağır, 2015, p.366). It identifies the security of human lives as the central objective of national and international security policy. It contrasts with, and grew out of increasing dissatisfaction with, the state-centered concept of security as an adequate conceptual framework for understanding human vulnerabilities in the contemporary world and military interventions as adequate responses to them (Fukuda-Parr and Messineo, 2012). It is defined as freedom for individuals from basic insecurities caused by gross human rights violations and includes both freedom from fear, through the protection of individuals and communities from direct violence, and freedom from want, through the promotion of unhindered access to the economy, health and education (UNDP, 1994).

The Commission on Human Security, in its final report *Human Security Now*, defines human security as:

> … to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment. Human security means protecting fundamental freedoms – freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity. (CHS, 2003, p.4)

Thus, human security, goes beyond military threats; it is primarily focused on the standards of everyday living, human dignity and safety from diachronic threats such as lack of food and medicine, poverty and restrains. Essentially, those who suffer from "want" are exposed to diverse types of threats. Consequently, the vulnerability of the populations affected by bad governance, poverty, lack of the basic human needs and principle rights for a decent

life and dignity, guide them to an inevitable effort for amelioration by any means (Chapsos, 2011).

4. POVERTY SITUATION IN NIGERIA

One major factor adduced for the rise in various crimes in Nigeria, most especially cybercrime is poverty. In examining the relation between cybercrime and poverty, it is important not only to define what is meant by cybercrime, but what is meant by poverty, as well. Poverty can be defined in many ways. While some scholars reduce it to numbers, others argue that a more ambiguous definition must be used. While some define it in relations to income, many treat poverty as multidimensional, using indicators such as (i) low income, (ii) low levels of education and health, (iii) vulnerability (to health or income loss, natural disaster, crime and violence, and education curtailment) and (iv) voicelessness and powerlessness (feeling discrimination, lacking income earning possibilities, mistreatment by state institutions, and lacking status under the law).

McConnell and Brue (2005) define poverty as a condition in which a person or a family does not have the means to satisfy basic needs for food, clothing, shelter and transportation. The means include, currently earned income, transfer payments, past savings and property owned. The basic needs have many determinants, including family size and the health and age of its members. Fields (1994) also defines poverty as the inability of an individual or a family to command sufficient resources to satisfy the basic needs such as food, clothing, shelter, healthcare and other necessities of life. In 1998, a United Nations (1998) Statement on poverty, signed by the heads of all UN agencies stated:

> Fundamentally, poverty is a denial of choices and opportunities, a violation of human dignity. It means lack of basic capacity to participate effectively in society. It means not having enough to feed and cloths a family, not having a school or clinic to go to, not having the land on which to grow one's food or a job to earn one's living, not having access to credit. It means insecurity, powerlessness and exclusion of individuals, households and communities. It means susceptibility to violence, and it often implies living on marginal or fragile environments, without access to clean water or sanitation.

Also, according to the World Bank (2003), the major indicators of poverty are: lack of freedom of action and choice; lack of adequate food, shelter, education and health; vulnerabilities to ill health; economic dislocation; maltreatment by public agencies; and exclusion from key decision-making processes and resources in society. Accordingly, poverty depicts a situation in which a given material means of sustenance within a given society is hardly enough for subsistence in that society (Townsend, 1962). Thus, people are considered to be poor if their standard of living falls below the poverty line, that is, the amount of income (or consumption) associated with a minimum acceptable level of nutrition and other necessities of everyday life (World Bank, 1992). In essence, when people are unable to eat, go to school, unable to find employment, or have access to health care, then they can be considered to be in poverty, regardless of their income.

Ajakaiye and Adeyeye (2002) note that poverty can be structural (chronic) or transient. Structural poverty is defined as persistent or permanent socio-economic deprivations and is linked to a host of factors such as limited productive resources, lack of skills for gainful employment, endemic socio-political and cultural factors and gender. Transient poverty, on the other hand, is defined as transitory/temporary and is linked to natural and man-made disasters. Transient poverty is more reversible but can become structural if it persists.

The issue of poverty in Nigeria is a paradox. While Nigeria is a leading oil-producing nation and highly endowed in terms of various natural resources, most of her people are economically poor. As a national data shows, over one-third of Nigerians (35%) live in extreme poverty while 54% are relatively poor. For instance, the Nigeria Poverty Profile 2010 Report of the National Bureau of Statistics provides an insight into the level of poverty in the country. More than half of the Nigerian population lives on less than a dollar a day. The major findings from the survey are as follows:

(a) Relative Poverty is defined by reference to the living standards of majority in a given society. In 2004, Nigeria's relative poverty measurement stood at 54.4%, but increased to 69% (or 112,518,507 Nigerians) in 2010. The North-West and North-East geo-political zones recorded the highest poverty rates in the country with 77.7% and 76.3% respectively in 2010, while the South-West geo-political zone recorded the lowest at 59.1%. Among States, Sokoto had the highest poverty rate at 86.4% while Niger had the lowest at 43.6% in the year under review.

(b) Absolute Poverty is defined in terms of the minimal requirements necessary to afford minimal standards of food, clothing, healthcare and shelter. Using this measure, 54.7% of Nigerians were living in poverty in 2004 but this increased to 60.9% (or 99,284,512 Nigerians) in 2010. Among the geo-political zones, the North-West and North-East recorded the highest rates at 70% and 69% respectively, while the South-West had the least at 49.8%. At the State level, Sokoto had the highest at 81.2% while Niger had the least at 33.8% during the review period.

(c) The-Dollar-Per-Day Measure refers to the proportion of those living on less than US$1 per day poverty line. Applying this approach, 51.6% of Nigerians were living below US$1 per day in 2004, but this increased to 61.2% in 2010. Although the World Bank standard is now US$1.25, the old reference of US$1 was the standard used in Nigeria at the time that the

survey was conducted. The North-West geo-political zone recorded the highest percentage at 70.4%, while the South-West geo-political zone had the least at 50.1%. Sokoto had the highest rate among States at 81.9%, while Niger had the least at 33.9%.

(d) Subjective Poverty is based on self-assessment and "sentiments" from respondents. In this regard, 75.5% of Nigerians considered themselves to be poor in 2004, and in 2010 the number went up to 93.9%. FCT recorded the most number of people who considered themselves to be poor at 97.9%. Kaduna recorded the least number of people who considered themselves poor at 90.5%.

A major indicator of poverty in Nigeria is unemployment. In broad terms, the term unemployment denotes a condition of joblessness or lack of employment. In other words, anyone who is fit and available to work but fails to get one may be considered as being unemployed for the concerned period. Statistics reveal that the unemployment rate is very high among youth in Nigeria, most of who are university graduates with computer and internet competence. According to statistics from the 2011 National Bureau of Statistics, Nigeria's overall unemployment rate amounted to 23.9 % of total Labour Force in March 2011, indicating a sharp increase from14.9% in March 2008 to 19.7% in March 2009 and 23.9% in 2011 (see Table 1). When disaggregated by sector, 17.1% of these are in the Urban areas, while 25.6% are from Rural areas. The surveys also reveal that persons aged 0-14 years constituted 39.6%, those aged between 15-64, which is the economically active population, constituted 56.3%, while those aged 65 years and above constituted 4.2%. According to the NBS, the Labour Force in 2011 stood at 67,256,090, of that 51,181,884 are employed while the unemployed are 16,074,205.

Table 1
Overview of Employment Situation in Nigeria (2006-2011)

	2006	2007	2008	2009	2010	2011
Nigeria population	140,431,790	144,925,607	149,563,227	154,349,250	159,288,426	164,385,656
Ecnomically active	78,922,666	81,448,191	84,054,533	86,744,278	89,520,095	92,384,738
Labour fore	57,455,701	59,294,283	61,191,700	63,149,835	65,170,629	67,256,090
Employed	50,388,650	51,763,909	52,074,137	50,709,317	51,224,115	51,181,884
Unemployed	7,067,051	7,530,374	9,117,563	12,440,517	13,946,515	16,074,205
Newly unemployed		463,323	1,587,189	3,322,954	1,505,997	2,127,691

Source: *National Bureau of Statistics* (2011).

From the table above, one can see the magnitude of unemployment in Nigeria. These unemployed youths have time on their hands and have easy access to the internet to perpetuate cybercrimes. Even if they do not have access to Internet at home, cyber-cafés are readily available throughout the country at relatively low rates for Internet access. All these factors combine to create a new generation of local hackers and cyber-criminals (Olowu, 2009). Although, they may not have deep programming knowledge like experienced hackers who can create their own malware or viruses, they take advantage of many websites available for free that help them understand the basics behind hacking techniques with links to underground hacking sites and even free tools to use.

5. CYBERCRIME IN NIGERIA: YAHOO YAHOO AND YAHOO PLUS

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 laptops that they use to perpetrate this crime.

Figure 1
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. These include sleeping in a coffin for certain numbers of days, sleeping in the cemetery, bringing body parts. In other words, he kidnaps a victim, kills him/her and extracts the body part needed. Some are even told to sleep with virgins as part of the rituals. Most often, young girls are kidnapped and raped and sometimes killed by these ambitious people.

Other forms of rituals performed include sleeping with pregnant women or mad women and sometimes, the yahoo boy may be told not to take his bath for days or months as doing so may have terrible repercussions.

Another popular "yahoo" crime in Nigeria is phishing. Phishing is an attack that typically involves sending an email to a victim that looks to the unsuspecting recipient as if it comes from a legitimate source, for instance, a bank. For phishes, an email is sent asking the victim to verify personal information through a link to a fraudulent web page. Once that is provided, the hacker can access the victim's financial information. According to Richards (2016), the year 2015 recorded high number of phishing emails from suspected cyber criminals in Nigeria, peaking when the Central Bank of Nigeria (CBN) announced deadline for Bank Verification Number (BVN). Cyber criminals swamped unwary bank customers with phish emails to warn them that their accounts were about to be blocked and consequently steal their credentials once they supply their details.

6. IMPACT OF CYBERCRIME ON NIGERIA

The proliferation of cybercrime has negative impact on Nigeria. According to the National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd), the 2014 Annual report of the Nigeria Deposit Insurance Corporation (NDIC), shows that, between year 2013 and 2014, fraud on e-payment platform of the Nigerian banking sector increased by 183%. Also, a report

published in 2014 by the Centre for Strategic and International Studies, UK, estimated the annual cost of cybercrime to Nigeria at about 0.08% of our GDP, representing about N127 billion (Iroegbu, 2016).

Apart from economic loss, cybercrime has brought disrepute to Nigeria from all over the world. For instance, in India, it was claimed that about 90% of foreign nationals arrested for cybercrimes in Hyderabad city since September 2015 were Nigerians. According to the source, of 67 foreigners arrested for online fraud, 60 were from Nigeria, five from Cameroon, and the other two were South African nationals. There are three basic types of online frauds through which Nigerians perpetrate the crime—lottery, jobs, and matrimonial scams (Lasania, 2016).

Fundamentally, Nigerians are treated with suspicion in business dealings. As pointed out by Ribadu (2007),

> cybercrime is depressing trade and investor confidence in our economy and to that extent it is a present and clear danger to our national security and the prosperity of our citizens. Indeed, of all the grand corruption perpetrated daily in our communities, most are of the nature of cybercrime executed through the agencies of computer and internet fraud, mail scam, credit card fraud, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting, laundering, embezzlement, as well as economic and copyright/trade secret theft.

The situation is such that international financial institutions now view paper-based Nigerian financial instruments with scepticism. Nigerian bank drafts and checks are not viable international financial instruments. Nigerian Internet Service Providers (ISPs) and email providers are already being black-listed in e-mail blocking blacklist systems across the Internet. Also, some companies are blocking entire Internet network segments and traffic that originate from Nigeria. Newer and more sophisticated technologies are emerging that will make it easier to discriminate and isolate Nigerian e-mail traffic (Chawki, 2009).

7. LEGISLATION ON CYBERCRIME IN NIGERIA

Having good legislation in place is one of the major steps in curbing cybercrime. In 2004, the Nigerian government established the Nigerian Cybercrime Working Group comprising representatives from government and the private sector to develop legislation on cybercrime. Furthermore, in 2007, the government established the Directorate for Cyber Security (DfC), which is an agency responsible for responding to security issues associated with growing usage of internet and other information and communication technologies (ICTs) in the country. It was provided with a funding of N1.2 billion (approximately USD9.8 million using 2007 exchange rates) to carry out its mission.

Apart from these initiatives, there are general laws that are not specifically related to cybercrime but are being enforced to deal with the crime. Some of these laws, which are examined below, are: the Nigeria criminal code (1990), Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006.

7.1 The Nigeria Criminal Code Act 1990

The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Even though cybercrime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. Chapter 38 of the Act deals with "obtaining Property by false pretences—Cheating." The specific provisions relating to cybercrime is section 419, while section 418 gave a definition of what constitutes an offence under the Act. Section 418 states that:

> Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.

While section 419 states:

> Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

7.2 The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provides the legal framework for the establishment of the Commission. This Act repeals the Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2002. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

• The investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;

• The coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;

• The examination and investigation of all reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;

• Undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;

• Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney- General of the Federation;

• The coordination of all investigating units for existing economic and financial crimes, in Nigeria;

• The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud-Related Offences Act 1995 ; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act (EFCC, 2004) .

7.3 Advance Fee Fraud and Related Offences Act 2006

According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006):

> False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.

Section 383 sub-section 1 of the Nigerian Criminal Code states: "A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing". Advance Fee Fraud and Other Fraud Related Offences Act 2006 deals with internet crime issues, however, it only covers the regulation of internet service providers and cybercafés, it does not deal with the broad spectrum of computer misuse and cybercrimes.

7.4 The Cybercrimes Act of 2015

All the above legislation has proven ineffective in curbing cybercrime as it is on the increase. In a bid to put in place stronger legal framework to curb cybercrime, a revision of the existing cybercrime legislation was put forward by the Government in September 2008. The bill titled "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters," passed second reading in November 2012 at the Senate. In May 2015, the cybercrime bill was signed into law, properly defining the act as unlawful with penalties attached to any disobedience of the law. The Act, known as the Cybercrimes (Prohibition, Prevention etc.) Act 2015 creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters. Particularly, the Act engenders a platform for cyber security and in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information.

The Cybercrimes Act 2015 is, thus, the first legislation in Nigeria that deals specifically with cybercrimes and cyber security. The Act, which was signed into law on May 15, 2015 stipulates that, any crime or injury on critical national information infrastructure, sales of pre-registered SIM cards, unlawful access to computer systems, Cyber-Terrorism, among others, would be punishable under the new law. The Act prescribes stringent penalties for offenders and perpetrators of cybercrime. The Cybercrimes Act is made up of 59 Sections, 8 Parts; and 2 Schedules. 1st Schedule lists the Cybercrime Advisory Council; 2nd Schedule lists businesses to be levied for the purpose of the Cybersecurity Fund under S.44(2)(a): GSM service providers and all telecom companies; Internet service providers; banks and other financial institutions; Insurance companies; and Nigerian Stock Exchange.

Some of the provisions of the Act include:

• It gives the president the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furtherance of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

• It prescribes the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that result in the death of an individual (amongst other punishments for lesser crimes).

• Hackers, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

• It makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment.

• It specifically creates child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.

• It outlaws Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine of not less

than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

• It prohibits cybersquatting, which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.

• It forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g. Facebook and Twitter), it also prohibits the use of threats of violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10million or to both fine and imprisonment.

• It mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy, and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

• It allows for the interception of electronic communication, by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings (Cybercrimes Act, 2015).

Apart from the Cybercrimes Act, the Economic and Financial Crimes Commission (EFCC) has also been monitoring and raiding internet cafes, and in most cases, stopping night browsing at the cafes. According to the former Chairman of the commission, Ibrahim Lamorde, more than 288 persons have been convicted for various cases of cybercrime across the country; another 234 cases are still under prosecution in various courts nationwide while four fugitives have been extradited to the United States of America (Mutum, 2012).

8. POVERTY REDUCTION STRATEGIES IN NIGERIA

The reduction of poverty is the most difficult challenge facing any country in the developing world where on the average majority of the population is considered poor (Ogwumike, 2002). In a bid to overcome poverty of Nigeria, government initiated different policies and structural programmes between 1977 till date. These programmes include: Directorate of Food, Roads and Rural Infrastructure (DFFRI), Better Life Programme (BLP), National Directorate of Employment (NDE); People" Bank of Nigeria (PBN); Community Bank (CB); Family Support Programme (FSP); Family Economic Advancement Programme (FEAP); Poverty Eradication Programme (PEP); National Poverty Eradication Programme (NAPEP); and National Economic Empowerment Development Strategy (NEEDS). Their aims are to ameliorate the suffering of the people by providing them employment opportunities as well as access to credit facilities to enable them to establish their own businesses.

Yet, despite the many policies and poverty alleviation strategies of the Nigerian government, poverty is on the rise in the country. Aluko (2003) notes that in Nigeria, government efforts at poverty reduction have not succeeded in reducing poverty. Some of the factors responsible for this lie the socio-political and economic structures, which alienate and exclude the poor from decisions affecting their welfare. Programmes are imposed from the top, with huge overheads, which favour contractors, consultants and the cronies of those in power. The politicisation of policies aimed at poverty reduction and the interplay of corrupt practices has often led to the displacement of goals and the objectives of programmes designed to reduce the incidence of poverty. Coupled with this is the problem of political instability, the rapid turnover of programmes of action and office holders, leading to the truncation of programmes midstream and unnecessary duplication and waste.

9. COMBATING CYBERCRIME IN NIGERIA

First, there is a need to tackle poverty headlong in the country. There is a need for a development plan that will revitalize the economy and provide relevant strategies for combating unemployment and poverty in Nigeria. The government needs to consider massive employment generation as an issue of major focus on national development and economic growth plan. To tackle poverty in the country, the government needs to formulate and implement programs that will directly benefit the poor, by restructuring sources of Nigeria's gross domestic product to significantly include variety of industries that are labour intensive, such as agriculture and industrialization. This would lead to the diversification of the country's sources of revenue, thereby reducing its overdependence on oil revenue.

Secondly, cybercrime can only be effectively countered when there is a proper coordination and guidance available for various stakeholders in Nigeria. Tackling cybercrime is, and always will be, a shared responsibility between individuals, industry and government. This means forging mutually beneficial partnerships to share information and combine efforts to combat cybercrime.

It is better to prevent cybercrime from happening than to respond to it after it has occurred. In many cases, effective preventative measures are relatively low cost and easy to implement. Users need to take steps to avoid falling victim to cybercrime and governments and industry need to be proactive in anticipating where new threats might emerge.

In addition, most cybercrimes go unreported and when they are reported, a lot of the victims often do not cooperate with law enforcement agents. There is a need for victims of cybercrime, whether individuals or organizations, to cooperate with law enforcement agencies for effective response. It is also important to spread awareness on cybercrime prevention to the members of the society since the cybercriminals are constantly inventing innovative ways to attack and are in search of potential victims. There is a need to put centralized online cybercrime reporting mechanism in place, which provides victims of cybercrime, a convenient and easy-to use reporting mechanism that alerts authorities of suspected cybercriminals.

Furthermore, to combat cybercrimes, international cooperation is very crucial. Being transnational in nature, it is but obvious that nations across the globe need to strengthen their cooperation and form alliances as well as ensure that their legal, technical and institutional measures structures are created and work in coherence. Therefore, it is necessary for nations to reach consensus and work toward establishing a framework of international cooperation (Rishi & Gupta, 2015).

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-annually-through-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-of-foreigners-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.pdf

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/b410c26c2921c18a6839baebc9b1428fa98fa36a.pdf

National Bureau of Statistics. (2011). *2011 annual socio-economic report*. Retrieved from http://www.nigerianstat.gov.ng/uploads/latestRelease/2ff063b27de8aa15b35f1a6fb04bf472c658d939.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-global-cybercrimes-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-combat-cybercrime/$FILE/ey-strategic-national-measures-to-combat-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-eradicate-poverty-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.