IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 25, Issue 6, Series 8 (June. 2020) 08-16
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Tapeworm in the Bloodstream: Addressing the Effect of Cybercrime for Human Security and Development in Nigeria

ONYEMAECHI AUGUSTINE EKE Ph.D
Department of International Relations Gregory University, Uturu, Abia State, Nigeria
and
HEARTS G. A. OFOEZE Ph.D
Department of Public Administration Abia State University, Uturu, Abia State, Nigeria

ABSTRACT: Cybercrime is fast becoming a threat to technology as a tool for human security and development. Hyper-connectivity, brought about by the information and communication technology has expanded literacy beyond reading and writing to 'operation of the computer' thus subjected mankind to continuous learning to catch up with the new system of interaction and doing business. Internet application sends a scary feeling that the technology comes hackers and that the world was fast losing grip in the fight against corporate and personal dimensions of cybercrime through e-transactions such as e-government and e-commerce as well as impacting developing stress on the developing regions of the world. In spite of the scary situation, the effect of cybercrime on human security and development in Nigeria has not received adequate investigation. Our broad objective is to examine the role of cybercrime on national development. Our specific objective is to investigate the effect of cybercrime on human security and development in Nigeria. We adopted the *ex post facto* (quasi-experimental) design and analysed, qualitatively, data assembled from secondary sources of vast array of literatures, including tables and figures. We used two complementary theories of 'social-crime' and 'social-learning' to conclude that cybercrime is a social challenge to the human security and development in Nigeria.

KEYWORDS: cybercrime, cyber-security, human security, development

---

Date of Submission: 03-06-2020 Date of Acceptance: 18-06-2020

I. BACKGROUND TO THE STUDY

Cybercrime is a global transnational threat (Herjavec Group, 2019); a lot of cybercrime emanates from Africa (Quarshie and Martin-Odoom, 2012, p. 98) and of top ten cybercrime countries in the world, Nigeria leads other three African countries () from a global third position which is "a major concern for the global community" (Chwki, 2009, p. 2). A computer-wired world with related acts for personal or financial gain or harm, identity-related crime and computer content-related acts (such as copyright infringements, racism, xenophobia, child pornography) fall within the concept of the new form of threat referred to as cybercrime.

Cybercrime is perpetrated against individuals or corporate entities through the Internet, computers, smart-phones or other unlawful acts using the computer as either: a tool, for example, to commit fraud, forgery, identity theft, phishing scams, spams, junk e-mails, pornography, online gambling, intellectual property crime, cyber defamation, cyber stalking, etc.); or a targeted victim, for example, unauthorised access to computers networks, electronic information theft, denial of service (DoS) attacks, malware, malicious codes, e-mail bombing, data diddling, salami attacks, logic bombs, web jacking, internet time theft, Trojan attacks, etc) (Kamini, 2011).

Top 10 countries where the most online attacks originate include China, with 41 per cent of the world's attack traffic, distantly followed by the U.S. with about 10 per cent; others are Nigeria, Russia, Eastern Europe, Indonesia, Brazil, Romania, South Korea and Vietnam. In the case of Nigeria, the country is recon to be one of the primary sources of scam and phishing emails by groups of young, disenchanted, unemployed and relatively tech-savvy individuals who spend significant amounts of time establishing online fraud schemes. In terms of the annual cost of cybercrime to the ten leading economies, the U.S. leads others with $108bn; China follows with $60bn. In the same order are Germany ($59bn), Brazil ($7.7bn), UK ($4.3bn), India ($4bn), France ($3bn), Russia ($2bn), Japan ($980m), and Italy ($900m). The annual cumulative cost for the ten leading economies is $250 billion (about 56.2 per cent) of $445 billion on the global economy (Blake, 2017, p. 8).

Cybercrime has become the catch-phrase of Nigeria's "Yahoo-Yahoo" Boys for criminal activities such as obtaining by trick (alias 419), kidnapping, drugging, raping and stealing pants of women, ritual killing,

body-parts merchandise, and other occult practices. Cybercrime confers the understanding that these criminal activity happens through the internet by people in pursuit of fast wealth and other illicit gains. These developments in Nigeria "reveal ambivalence created in the entanglements of class and kinship, military rule and patron-clientism, as well as individual desires and social obligations" (Smith, 2001, p. 804).

The effect of cybercrime on human security and development has become grave concern and will continue to be one of the biggest challenges to humanity in decades to come if not prevented. Cybercrime is considered "the greatest threat to every company in the world, and one of the biggest problems with mankind" which could cost the world in excess of $6 trillion annually by 2021 from $3 trillion in 2015, representing "the greatest transfer of economic wealth in history" and far more profitable than the global trade of all major illegal drugs, combined" (Herjavec Group, 2019).

Cybercrime of corporate and personal dimensions have evolved alongside the epochal opportunities offered by the rapid increase in the application of the Internet for e-transactions such as e-government and e-commerce as well as impacting developing stress on the developing regions of the world. Our broad objective is to examine the role of cybercrime on socio-economic development. Our specific objective is to investigate the effect of cybercrime on the socio-economic development of Nigeria. We adopted the *ex post facto* (quasi-experimental) design and analysed qualitatively our data assembled from secondary sources of vast array of literatures, including tables and figures. We used two complementary theories of 'social-crime' and 'social-learning.'

Theory of social-crime provides the social structural reasons (such as the breakdown of the family, urban decay, social disenchantment, social alienation, drug abuse, peer pressure, poverty, unemployment, etc) young people commit crimes (Krohn et al, 1987). The theory assumes that crimes are social or sociological in character and, therefore, focuses on reduced self-control and the preparedness to take risk for short-term gains or even to occasion harm on a victim. This type of crimes can be facilitated or enhanced by electronic communications and the internet. In such criminal environment, individuals who are exposed online to cybercrime perpetrators and peers may themselves turn to engage in cybercrime (Holt et al, 2010). The environmental factors that influence both the perpetrator and the victim of cybercrime include the physical, social, family, community, economic, cultural and political.

The social learning theory was first proposed by Burgess and Akers (1966) and was originally called the "differential association-reinforcement theory". The duo employed the principles and vocabulary of operant conditioning to specify the learning process and argued that offenders of cybercrime more often than not, need to learn specific computer skills, techniques, competences and procedures (Skinner and Fream, 1997) to be better able to outwit or outsmart their victims.

Theory of social learning and the theory of crime share mutual inclusiveness, in that individuals with reduced self-control may in more active ways seek out similar others and coalesce in virtual environments, the same way in the real world. Online connectivity and peer-learning is much more central to the engagement of organised criminal groups in cyber criminality such as *cyber-terrorism*, c*yber-espionage*, *online child abuse and exploitation* and *hacking* (Osho and Onoja, 2015, p. 123; Buchanam, 2017, p. 5-6; Valeriano et al, 2018; Gomez, 2019, p. 2-3; Eke, 2019, p. 13; United States Congress, 1977). Social-crime and social-learning are central to underscore that cybercrime is a social challenge to the economic growth and development in Nigeria.

This research is divided into six reinforcing sections: one, Background to the study; two, exams internet as driver of cybercrime; three, examines cybercrime plus spiritualism in Nigeria; four, investigates relationship between cybercrime and human security in Nigeria; five, analyses policy strategies to curb cybercrime for human security and development in Nigeria; and six is the conclusion.

Internet Age and cybercrime

The revolution into the information age and global hyper-connectivity brought about by the information and communication technology (ICT) has expanded literacy beyond reading and writing to include 'operation of the computer'. This reality imposes on mankind the challenges of continuous learning to catch up with the benefits and dangers of new system of transaction and communication. Digitalisation can reduce transaction and communication costs but, on the contrary, increase cyber-related crimes due largely to the outcomes of Siamese "digital divide" and escalating economic inequality between the North and the South.

Defenders of cybercrime appreciate that it is illegal transaction but point at the North-South divide in global economic structure to argue that the "digital divide" escalates Africa's economic dependency and inequality by denying developing countries access to job opportunities in the technology sector (ILO, 2001) and that the developed North capitalise on the digital divide to perpetrate sharp business practices in Africa. Africa was ripped off over $1 trillion dollars in 50 years on annual average of $50 billion dollars on illicit transfers, 60 per cent was through aggressive tax evasion by the giant multinational corporations (MNCs) owned by the developed North. The whooping sum could have been used to develop Africa instead of lagging behind other regions.

To these defenders of cybercrime, the Nigerians who engage in the Yahoo plus without serious education, training and skill in ICT serve the gap-filling strategy to extract reasonable reparation by out-conning the 'greedy' Western business partners in the cultural globalisation promoted by digital technology (Hart, 2010, 3681).

With the invention of the World Wide Web in 1989, which has increased to nearly 1.9 billion, today, internet users have also increased from 2 billion in 2015 to 4 billion in 2018 and it is predicted by Cybersecurity Ventures that there will be a further increase in internet users to 6 billion by 2022 and more than 7.5 billion by 2030, approximately 90 per cent of the projected world population. There is the expectation that by 2020, the world would be run by about 21 billion "internet of things" (IOT) capable of identifying, communicating, locating, sensing and computing from the costless internet protocol (IP) addresses that will be fitted in pens, watches, shoes and clothes (Sharma and Kaur, 2019, p. 37).

The increasing number of platforms to connect people, while they do nothing in practical terms in cybercriminality, is put into illegal use by criminal individuals and groups to interact and do business with others. Cybercrime economy, through the illegal approach to generate revenues, plays two discernible roles in platform economics which are basically:

(i) exploiting existing legitimate platform; and

(ii) developing new crime-specific platforms

Cybercrime is not a recent development. The first recorded cybercrime in history was in 1820; the first spam email took place in 1978 when it was sent over the Arpanet; and the first Virus was installed on the Apple Computer in 1982 (Buch et al, 2018, p. 22).

Since the first recorded global cybercrime in 1820, cybercrimes have posed threat to cyber-security and have steadily grown hydra-headed into 12 types to include hacking, virus dissemination, logic bombs, denial of service attack, phishing, bombing and spamming, jacking, cyber stalking, data diddling, theft and credit card fraud, slicing attack, and software privacy. These types of cybercrimes fall into three major categories: cybercrime on individuals, cybercrime on property; and cybercrime on government (Sharma and Kaur, 2019, p. 37). The growing anxiety is that Cyber Security Breaches Survey 2018 reported that 43% of businesses were a victim of a cyber security breach in 12 months of the survey. Michael McGuire also reported that in 2018, cybercrime which has evolved into an entire economy rife with professionalism and filled with parallels to legitimate industries with low-investment, high-yield and low-risk operations will rake in profits in excess of annual revenue of $1.5 trillion as a new platform of capitalism which ranks cybercrime economy as the 13th world largest GDP, if it were a nation. The sources of crime and revenue are found in the table 1 below.

Table 1: Sources of Cybercrime and Revenues in 2018

Crime	Annual Revenue
1. Illegal Online Markets	$860 Billion
2. Trade Secrets, IP Theft	$500 Billion
3. Data Trading	$160 Billion
4. Crime-Ware/CaaS	$1.6 Billion
5. Ransomware	$1.0 Billion
Total	**$1.5 Trillion**

Source:

From table 1 above, it could be gleaned that over 50 per cent of cybercrime revenues are generated from online markets.

The World Bank revealed that Africa was harbouring four (Nigeria, Cameroon, Ghana, and South Africa) of the top ten countries in the world with high level of cybercrime prevalence. Additionally, U.S. Attorney Nick Hanna, accompanied by officials from the Federal Bureau of Investigation (FBI), the Los Angeles County Sherif's Department and Los Angeles County District Attorney's office, unsealed indictment, by Federal grand jury, of 80 cybercriminals charged with conspiracy to commit fraud, conspiracy to launder money, and aggravated identity theft (*The Nation*, 23 August 2019, p. 6). Of the 80 cybercriminals indicted, about 77 are Nigerians, most of who are located in Nigeria. The statistics indicates Nigeria's global rating as the third largest in cybercrime.

Cybercrime plus Spiritualism in Nigeria

Cybercrime is a side-product of internet development, a popular crime in Nigeria (Adesina, 2017) and a world-wide challenge (Hassan et al, 2012) with no geographical boundaries or time restrictions. In Nigeria, it assumes a more complex dimension with the Yahoo Boys fine-tuning the social engineering techniques against society – big and small individuals and corporations. In the early period in the development of cyber fraud in

Nigeria, a small local, frauds were perpetrated by con artists who would mail out letters informing victims that a prince was looking to deposit large amount of money in the mark's bank accounts, and would reward him for helping to get the money out of the country (Devine, 2011). In the 1960s and 1970s, the cybercrime which was "computer crime", in fact, was different from cybercrime we faced with today, because availability of internet was restricted within some sections, e.g., the U.S. military (Obiora et al, 2017).

Of the globally known types of cybercrime such as malware, web-based attacks, web application attacks, distributed denial of service (DDoS), botnets or "zombie computers", phishing, spam, ransomware, insider threats, physical manipulation, exploit kits, data breaches, identity theft, information leakage, and cyber espionage (Ossip, 2019, pp. 8-10), what makes cybercrime in Nigeria more complex, dangerous and nerve-racking is the introduction, into "Yahoo plus" version, of spiritualism embodying witchcraft, occult practices and other forms of criminality to maximise illicit gains. Though Yahoo plus and the spiritual demands form the reason for kidnapping, severing of human parts – heads, breasts, penis, vagina, or stealing of women pants, sanitary pads, etc., some other kidnapped victims may sold, placed for ransom or their body organs, for example, bladder, hearts, kidney, liver, lungs sold to their Western clients.

Nigerian Yahoo plus, whether hacking, terrorism, espionage, online child abuse and exploitation through kidnapping for ransom, rape, trafficking and body parts merchandise for illicit gains, pose grave insecurity both to the sovereignty and population of Nigeria through physical "injury or death to persons" and/or "damage or destruction to objects" (Schmitt, 2017, p. 417).

Cybercrime in Nigeria reflects an index of state failure in addressing social decadence, economic inequality and resort to occult activities to add up. The unsealed indictment of the Nigerian Yahoo Boys by FBI revealed more complex and sophisticated syndicate, including:

- Business Email Compromise (BEC) scam in which the fraudsters hack companies' email system, impersonate companies' personnel and direct payments to choice banks in Nigeria;
- Romance Scam, in which the fraudsters build fake dating relationship luring victim-lover into wiring money to the criminals; including other online schemes.

Some apologists of cyber-criminality hold that cybercrime against the West is a form of reparation for greed and economic sabotage of the Western countries and their citizens who, in their illicit businesses, are out-conned. This group leverages reports such as the Report of African Union/United Nations High-Level Panel on illicit transfers from Africa through "abusive transfer pricing, trade mispricing, misinvoicing of services and intangibles using unequal contracts, all for purposes of tax evasion, aggressive tax avoidance and illegal export of foreign exchange (Lépissier, and Cobham, 2015, p. 24). The report revealed a 50-year illicit transfers by international corporations from African countries that amounts to over one trillion U.S. dollar with illicit financial flows currently standing at 50 billion U.S. dollars per year, 60 per cent of loss are due to aggressive tax avoidance by multinational corporations – total of which could have been used for sustainable development of Africa (AU/UN, 2015; Ighobor, 2016).

Howbeit, these scams are perpetrated, using social media to obtain by trick (OBT, *alias* 419), kidnapping and ritual killing, body-parts merchandise, and other occult-ritual practices, under pseudo-names and other identity thefts of which Nigerians are the worst heat in human security fronts. Ritual killing and occult practices, albeit weird, are popularised by "modernity of witchcraft" (Geschiere, 1997) which formed the spiritual dimension of cybercrime, referred to as 'yahoo plus' (Tade, 2013) which although challenges the social, moral, and emotional fabrics of the Nigerian society, place the Yahoo Boys who, in the words of Adam Meyer, have become "more like a crew from the mafia in the day" with exotic life-styles, glamorised such as in Olu Maintain's "Yahooze" rap music watched by over 8 million in You-tube.

Logically, Nigerians go into witchcraft for reasons of domestic tension, jealousy and egotism (Jayeola-Omoyeni et al, 2015, p. 369). Ego is the dangerous human attribute that promotes lust for power, greed, selfishness, jealousy and primitive accumulation to sustain self-pride in a society, like Nigeria, organised around obligations and reciprocal exchange. Adducing reasons for the resurgence of witchcraft and occult practices in Nigeria, Johannes Harnischfeger wrote:

The decline of the state might be contributing to the return of the occult in yet another way. Since power is hardly regulated institutionally anymore, it has become unpredictable and seems to be connected to hidden forces, and everyone in society has an interest in manipulating these forces. In all spheres of life, it now seems advisable to take occult influences into consideration. In the universities, for example, students seek the help of miracle doctors or (Christians) sprit mediums in order to pass their examinations. Government employees seeking promotion or businessmen looking for customers arm themselves with amulets against the evil magic of their opponents, and in politics, too, the rise and fall of powerful figures seems to depend on invisible forces (Harnischfeger, 2006, p. 74).

More worrisome of the popularisation of occult and witchcraft practices in Nigeria is that the archetypical witches, posited Smith (2001, p. 806), "consume their kin to satisfy avaricious desires to prosper at

the expense of others". The cannibalism that surrounded the "Otoko" saga and later, the "Okija" saga, in 1996 and 2004, respectively, or Wadume and Eddy Nawgu nefarious activities of kidnapping and human sacrifice, are no distant experiences.

In September 1996 in Owerri, a local television showed a man, named Innocent Ekeanyanwu, holding a freshly severed head of an 11-year-old child, named Anthony Ikechukwu Okonkwo. Riot ensued following alleged killing of Ekeanyanwu in Police custody to cover the involvement of the bigwigs, including the principal sponsor – Chief Vincent Duru (owner of Otokoto Hotel, alias "Otokoto") and the Chairman of Traditional Rulers Council of Imo State Eze Onu Egwunwoke who conferred chieftaincy titles on the members of the ritual network. The Otokoto affair was an eye-opener of how the 419 network of criminals and influential people in society complemented other forms of fraud with body-parts merchandise.

In Okija shrine in Okija, the police discovered 83 corpses, including 63 that were headless, 20 skulls and made arrests, including Okija shrine priests (Nwabueze, 2007). The Okija saga, not only revealed how political godfathers in Anambra, as elsewhere in Nigeria, relayed their power through wealthy individuals, and via traditional rulers and shrines, oftentimes with Christian clerics who partake in the patronage network but transfer the belief in occult and witchcraft to the younger generations, who have embedded these values of spiritualism in "Yahoo plus" cybercrime. Yahoo plus introduces the spiritual complement to the physical as the two aspects man's life identified by Nwolisa (2012). The sources of spiritual powers are "local deities, juju, witchcraft, curses, oath-taking mercantile native doctors, possessed plants, animals and stones, oath-taking and breaking, ghosts and ancestral spirits, bewitched or charmed objects, spiritual covenants, and hypnotism" (Nwolisa, 2012, pp.18-26).

The Wadume saga in which Hamishu Bala Wadume is the tactical field commander in the kidnapping ring also links the Nigerian security among politicians and other influential people into kidnapping activities. Arraigned before the Rear Admiral Ibikunle Olaiya-led Special Investigation Panel, the suspect Wadume gave account of how he alleged paid money to Army Captain and the other security personnel that were on his payroll (Igbonwelundu, 23 August 2019, pp. 1 and 6).

The return to spiritualism, witchcraft and occult practices is evident of Nigerians' belief in sorcerers, for example, Prophet Edwin Okeke, alias "Jesus from Nawgu," "Alusi n' eje uka (the Deity that goes to Church), "Okalla Mmadu, Okalla Muo" (Half man, half spirit), who was widely known as "Eddie Nawgu" had façade of Christian piety and healing centre which was a monstrous crime-center of ritual murders, kidnapping, aiding and abetting infamous criminals, partaking in rituals involving use of human body parts, human sacrifice, etc., until the power of his magic wand died with him after being beheaded on 9 November 2000, by the Bakassi Boys at the Ochanja Market in Anambra State.

The four cases point to ominous spectacle that the resurgence and transfer of the subculture of witchcraft and occult practices to the younger generation of Nigerians has wrought serious ethical and moral challenges implicit in the Yahoo plus network where these cybercriminals and their faceless sponsors - political, cultural, and economic - kidnap for ransom, ritual practice, body parts merchandise, or a combination of these to maximise illicit gains.

Cybercrime and Human Security and Development in Nigerians

Human security has become a strong pillar for sustainable development either for realising the United Nations' '2030 sustainable development goals (SDGs)' or the African ' Agenda 2063'(HDR, 1994, pp. 24-25; Eke, 2019, p. 5). Human security involves seven broad dimensions – personal, community, economic, health, food, environmental, and political. The core objectives of human security are:

- transition to peace and sustainable development in fragile and conflict-affected communities;
- protection and empowerment of victims of human trafficking;
- responding to issues of environmental degradation and climate-induced threats;
- reducing urban violence and its effects on health, education, economic, personal, and community security;
- poverty reduction, social inclusion, and community-based development; and
- economic, environmental and social components of health-related insecurities (Eke, 2019, p. 8).

Human security is a 'complement', not 'substitute' to security; and a supplement to development in the global world where equating national security to national borders has become obsolete with the transnational network of the Internet. Human security is a supplement to development because development is characterised by enlargement of human or people's freedoms (positive freedom) to exercise choices safely and freely (HDR, 1994, p. 23) so that they can be confident that the opportunities they have are protected. Man is at the centre of development!

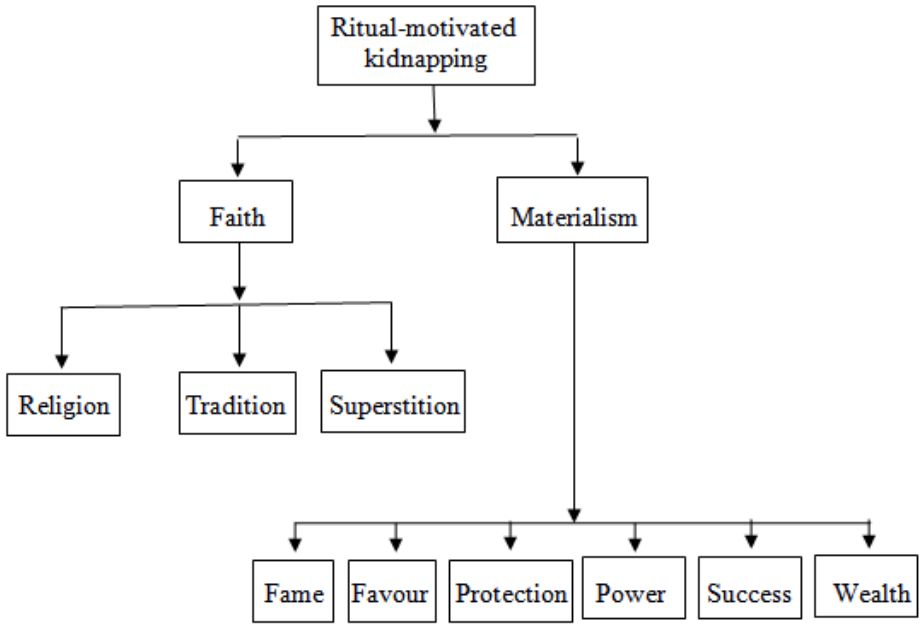
Cybercrime, like other crimes, involves associated behaviours that break the formal written laws of the Nigerian society and logically impacts negatively on human security and development. The Nigerian scenario aptly reflects the United Nations' assertion that contemporary cybercrime is tied to the growth of connectivity

and the use of globalised ICT for committing criminal acts with transnational effects in many countries, particularly developing countries, across the globe, where young men have acquired the subculture of financial fraud because cybercrime no longer requires complex or sophisticated skills or techniques, at a time of economic and demographic transformations, with ever-growing disparities, tightened private sector spending, and decreased financial liquidity (United Nations, 2013: xvii and 6).

With investigation on the 80 Nigerians indicted for internet-related crimes by the U.S. Federal Bureau of Investigations (FBI), the Nigeria Economic and Financial Crimes Commission (EFCC) promised to unravel "bigger suspects" because the figure released by the FBI was mere 1 per cent of the group of persons involved in the cybercrime network (*Punch*, 28 August 2019). The position of the EFCC may have been drawn from the available five-year statistics of ₦25 billion cyber fraud in Nigeria (Ochaya, 2019, p. 8).

To understand the relationship between cybercrime and occultism in the "Yahoo plus" leads to why kidnapping, ritual murders, rape, witchcraft and other occult practices characterise the 'plus' motivation in Yahoo. For instance, the F**ig. 1** illustrates the motivation for ritual kidnapping in Nigeria.

Fig. 1: *Motivation for Ritual Kidnapping in Nigeria*



Source: Oyewole, S. (2016) "Kidnapping for Rituals: Article of Faith and Insecurity in Nigeria"

The state failure in Nigeria characterised by corruption, ethnic patron-client relationship in pursuit of private enrichment by the dominant class in occult class in which the Nigerian child is born and nurtured, to a greater extent, mould the child's character and personality and sufficiently account for the growing cases of criminality including cybercrime. Belief in witches and occult powers for personal aggrandisement takes Nigerians back to the pre-colonial days and worse, with witchcraft power moving from the marginal persons to the ruling elite and now being transferred to the youth (leaders of tomorrow) who also seek spiritual powers for power, wealth, status, influence and protection thus legitimising the collective trauma that the world is unsafe in the hands of men who rule with "dark forces."

It is of grave concern that Nigerian students, for power, status, influence wealth and protection have introduced a new Yahoo practice – the "Yahoo plus". Yahoo plus introduced the spiritual dimension to cybercrime in Nigeria and blends spiritual elements with internet suffing to enhance victimisation rates on the web. The 'plus' implies the addition of spiritual elements such as consultations with occult diviners and sorcerers, etc., to maximise business security and yield. The moral panic, confusion or total collapse (Kalu, 2002, p. 678) underlies human development in Nigeria.

Cybercrime and its associated evils on humanity conduce appropriately to challenges against human security as articulated by the Commission on Human Security. The Commission defines human security as protecting:

… the vital core of all human lives in ways that enhance human freedoms and human fulfillment. 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 peoples' strengths and aspirations. It means creating political, social, environmental, economic, military, and cultural systems that altogether give people the building blocks of survival, livelihood and dignity (CHS, 2003, p. 4).

Extrapolating from the definition, one logically argues that human security guarantees freedoms – choices and opportunities - to political, social, environmental, economic, military, and cultural values which allow people to meet their aspirations for survival, livelihood and dignity. Fundamentally, cybercrime carries with it anxiety, deprivation, denial of the building blocks of survival and livelihood which in the view of the United Nations (1998), breeds 'poverty' as a denial of choices and opportunities and a violation of human dignity.

As impediment to human security, witchcraft and occult practices associated with Yahoo plus are grave and growing. The data from Nigeria Watch database recorded since 1 June 2006 reveals that witchcraft accounted for 661 violent deaths in the eight years between 2006 and 2014 (Akinpelu, 2015, p. 2). The recognition and conferment of chieftaincy honours and titles on criminals in Nigeria and the portrayal of cybercriminal as skillful entrepreneurs who succeeded in outsmarting or out-conning greedy opponents give credibility to cybercrime economies and enlist more people who admire and envy the flamboyant life-styles of the Yahoo Boys in town. Majority of cybercriminals in Nigeria are found in the universities who belief in spiritualism and witchcraft. Cyber spiritualism involves the extension into mystical, spiritual and supernatural powers by Yahoo Boys to cast a spell on their victims (Tade, 2013, p. 690). The UNDP HDR contention that human security is not a concern with weapons but a concern with human life and dignity (HDR, 1994, p. 22) helped to shape opinions that cybercrime shifted human security from physical threats towards psychological harm, leading to human security disruptions (Ossip, 2017, p. 3).

The Yahoo plus-type of cybercrime in Nigeria has proven that rather than the distinctive shift from physical insecurity to psychological insecurity, cybercrime combines elements of human insecurity. Howbeit, cybercrime as one the new threats is a proof that "as the world is constantly changing and moving more into the online space, human security fails to fulfill its components in order to retain its meaning and relevance (Ossip, 2019, p. 12). It is instructive to note that while cybercrime is a global phenomenon, its impact on the human security and development on Nigerians is monumental, complex and overwhelms the state.

Curbing Cybercrime for Human Security and Development in Nigeria

Nigeria created legal provisions against cybercrime but not the political will to implement them. Cybercrime "has become one of the legal frontiers" because the cyber world has no definite territorial boundary (Decker, 2008, p. 959). Nigerian National Assembly enacted the "Cybercrimes (Prohibition, Prevention, Etc.,) Act, 2015, to shore cyber-security through:

(a) provision of an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber-security and the protection of computer systems and networks, electronic communications, data and computer programmes, intellectual property and privacy rights.

In spite of the presence of national legal frameworks to curb cybercrime in Nigeria, the Executive has not mustered the requisite political will to effectively implement the law through the judiciary. The inactive operationalisation of Nigerian cyber laws indicates weakness or absence of international regimes governing ICT-related activities (Hart, 2010, p. 3683) in ensuring that governmental policy adheres to global rules and norms (Hongbo, 2014, iv) of industry-level governance.

Policy frameworks to curb cybercrime for human security and development in Nigeria must first situate cybercrime as transnational threat vis-a-vis global governance. In this way, realisation that cybercrime is a global challenge requiring partnership with Nigerian government crystallises for countries, through regional or triangular cooperation models, for instance, the German triangular recipe of "a Marshall Plan with Africa" (Federal Ministry for Economic Cooperation and Development, 2017) to pool resources (expertise, finance, and staff) together to pursue a cooperative action to deal with cybercrime challenge.

Since global governance attempts to "find an appropriate political response to increasing globalised context" (Bersheim, 2012, p. 7) through an innovative political rule of multi-layer (local, regional, national or regional) process of governance system, there is the increased need for partnership in spirit and letter of the United Nations Sustainable Development Cooperation Framework. The UN Framework was created by the General Assembly resolution 73/279 0f 2019, co-designed and co-signed by the UN development system and the Government for Agenda 2030. The Framework has objective focus on "a renewed push for collective action and partnerships", and a "laser-like focus on helping countries achieve the Sustainable Development Goals (SDGs), leaving no one behind. For emphasis, the Framework specified four objective processes for meeting the human security and development needs :

- collective response to help countries address national priorities and gaps in their pathway towards meeting the SDGs;
- spirit of partnership that are the core of the 2030 Agenda;
- collective promise to leave no one behind into tangible action for people on the ground, especially those furthest behind, mostly the marginalised and vulnerable group; and
- UN country teams (UNCTs) with the tools to tailor responses to a Member State's specific needs and realities ensuring that all entities, whether present on the ground or not, can effectively support national implementation of the 2030 Agenda (Mohammed, 2019, p. 4).

II. CONCLUSION

Cybercrime is a world-wide crime with monumental impact on human security and development in Nigeria which has overwhelmed the state and its citizens and requires strengthening global governance and global rules relating to enforcement capacity with the requisite political backing of the Nigerian state through development-oriented education and more effective and transparent system of reward of merit in order to promote the goals of human security and sustainable development in Nigeria.

REFERENCES

[1]. Akinpelu, B. A. (2015) "trends and Patterns of Fatalities reslting from Cult Societies and relief in Witchcraft in Nigeria (2006-2014)", IFRA-NIGERI ePapers Series 2015, n°40.
[2]. AU/UN (2015) Final Report of the High Level Panel on Illicit Financial Flows from Africa.
[3]. Buch, R.: D. Ganda, P. Kalola and N. Borad (2018) "World of Cyber-security and Cybercrime", Recent Trends in Programming Languages, Vol. 4(2), p. 18-23.
[4]. Buchanam, B. (2017). The Cybersecurity Dilemma: Hacking Trust and Fear Between Nations. London: Hurst & Company.
[5]. Burgess, R. L. and R. L. Akers (1966) "A Differential Association-Reinforcement Theory of Criminal Behaviour", Social Problems, 14, pp. 128-147.
[6]. Chawki, M. (2009) "Nigeria Tackles Advanced Fee Fraud, 2009 (1)", Journal of Information, Law & Technology (JILT), http://go.warwick.ac.uk/jilt/2009_1/chawki
[7]. Decker, C. (2008) "Cybercrime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cybercrime", South California L. R., Vol. 81, p. 959.
[8]. Devine, J. (2011). History of 419 Internet Fraud. Ezine Articles: file:///C:/Users/jegede/Documents/TheHisrory of 419 Internet Fraud.htm
[9]. Eke, O. A. (2019). "Governance and State-Building: Roadmaps to Human Security in Nigeria", GUU Public Lecture Series, No. 2, Thursday 6th June 2019. Uturu: Gregory University Press.
[10]. Federal Ministry for Economic Cooperation and Development (2017) Africa and Europe - A New Partnership for Development, Peace and a Better Future: cornerstones of a Marshall Plan with Africa. Bonn, Germany: BMZ Bonn.
[11]. Gomez, M. A. N. (2019) "Sound the Alarm! Updating Beliefs and Degradative Cyber Operations," European Journal of International Security. Online: Doi:10.1017/eis.2019.2
[12]. Harnischfeger, J. (2006) "State Decline and Return to Occult Powers: The Case of Prophet Eddy in Nigeria", Magic, Ritual, and Witchcraft, Vol. 1(1), pp. 56-78.
[13]. Hart, J. A. (2010) "Information Technology and the Global Political Economy:, in R. Denemark ed., The International Studies Encyclopedia. United Kingdom: Wiley, pp. 3674-3687.
[14]. Hassan, A. B and Laas, F. B and Makinde. J. (2012). "Cybercrime in Nigeria: Causes, Effects and the Way Out," ARPN Journal of Science and Technology: 2(7), pp. 626 –631.
[15]. Herjavec Group (2019) 2019 Official Annual Cybercrime Report. United States: Cybersecurity Ventures.
[16]. Holt, T. J.; G. W. Burruss and A. M. Bossler (2010) "Social Learning and Cyber Deviance:Examining the Importance of a Full Social Learning Model in the Virtual World", Journal of Crime and Justice, 33(2), pp.31-61.
[17]. Hongbo, W. (2014) "Foreword" in: Committee for Development Policy, Global Governance and Global Rules for Development in the Post-2015 Era. New York: United Nations Publications.
[18]. Ibekwe, C. R. (2015) "The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions". A Thesis Submitted to the School of Law, University of Stirling for the Degree of Philosophy (Ph.D), July 2015.
[19]. Igbonwelundu, P. (23 August 2019) "Wadume Testifies before HQ Panel as More Suspects Held", The Nation. Lagos: Vintage Press Limited, pp.1 and 6.
[20]. Ighobor, K. (2016) "Mbeki Panel Ramps up War against Illicit Financial Flows," African Renewal, April 2016, https://www.un.org
[21]. International Labour Organisation (ILO) (2001) World Employment Report 2001: Life at Work in the Information Economy. Geneva: ILO.
[22]. Jayeola-Omoyeni, M. S.; E. U. Oyetade and J. O. Omoyeni (2015) "Witchcraft in the 20th and 21st Centuries

in Nigeria: An Analysis," European Scientific Journal, Vol. 11(28), pp. 361-373.
[23]. Kalu, O. U (2002) "The Religious Dimension of the Legitimacy Crisis, 1993-1998," in T. Falola (ed.) Nigeria in the Twentieth Century. Durham, N. C.: Carolina Academic Press, pp. 667-685.
[24]. Kamini, D. (2011). "Cybercrime in the Society: Problems and Preventions". Journal of Alternative Perspectives in the Social Sciences, Vol. 3 (1).
[25]. Krohn, M. D.; J. L. Massey and W. F. Skinner (1987) "A Sociological Theory of Crime and Delinquency" in E. K. Morris and C. J. Braukmann eds, Behavioural Approaches to Crime and Delinquency. Boston, MA: Springer, pp. 455-475.
[26]. Lépissier, A. and A. Cobham (2015) Illicit Financial Flows: Report of the High Level Panel on Illicit Financial Flows from Africa. Commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development – Technical Report.
[27]. Nwolise, O. B. C. (2012) "Spiritual Dimension of Human and National Security," Eighteenth Faculty Lecture Series. Faculty of Social Sciences, University of Ibadan, April 26, 2012.
[28]. Obiora, C. A. and J. E. J. Tiebiri and O. U. Mmaduabuchi (2017) "Cybercrimes and the Challenges of Economic Development in Nigeria," Journal of social Development, Vol. 6(6), pp. 59-70.
[29]. Ochanya, C. (2019) "Nigeria Records ₦25bn Cyber Fraud in 5 Years – CIFIAN", Vanguard. Lagos: Vanguard Media Limited, Monday, April 8.
[30]. Osho, O. and A. D. Onoja (2015). 'National Cyber- security Policy and strategy of Nigeria: A Qualitative analysis', international journal of Cyber Criminology, Open access, August 2015. DOI: 10.5281/zenod0.22390.
[31]. Ossip, S. M. (2017) "Cyber Threats and Cybercrime: A Disruption of Human Security", MA Thesis International Studies, Faculty of Humanities. Leiden University, Brussels.
[32]. Oyewole, S. (2016) "Kidnapping for Rituals: Article of Faith and Insecurity in Nigeria", Africology: The Journal of African Studies, Vol. 9(9), pp. 35-52.
[33]. Punch (28 August 2019) "FBI List: We'll Unravel Bigger Suspects – EFCC", Punch, 28 August 2019, punchng.com
[34]. Quarshie, H. O. and A. Martin-Odoom (2012) "Fighting cybercrime in Africa", Computer Science and Engineering, Vol. 2(6), pp. 98-100.
[35]. R. N. Nwabueze (2007)"Dead Bodies in Nigerian Jurisprudence", Journal of Nigerian Law 51, pp. 117-150.
[36]. Schmitt, M. N. (2017) Tallinn Manual 2.0 on the International Law Application to Cyber Operations. Tallinn: Cambridge University Press.
[37]. Sharma, M. and S. Kaur (2019) "Cybercrimes Becoming Threat to Cybersecurity", Academic Journal of Forensic Sciences, Vol. 02(01), pp. 36-40.
[38]. Skinner, W. F. and A. M. Fream (1997) "A Social Learning Theory Analysis of Computer Crimeamong College Students", Journal of Research in Crime and Delinquency, 34(4), pp. 495-518.
[39]. Smith, D. J. (2001) "Ritual Killing, 419, and Fast Wealth: Inequality and the Popular Imagination of Southeast Nigeria", American Ethnlogist, Vol. 28(4), pp. 803-826.
[40]. Smith, R. G.; P. Grabosky, and G. Urbas (2004) Cyber Criminals on Trial. Cambridge: Cambridge University Press.
[41]. Tade, O. (2013) "A Spiritual Dimension to cybercrime in Nigeria: The 'Yahoo plus' Phenomenon', Human Affairs, Vol. 23(4), pp. 689-705.
[42]. The Nation (23 August 2019), "US Charges Nigerians for Stealing Millions of Dollars", The Nation. Lagos: Vintage Press Limited, pp. 6-7.
[43]. United Nations Depvelopment Programme (1994) Human Development Report 1994. Oxford: Oxford University Press, Ch. 2.
[44]. United Nations Office on Drugs and Crime (NODC) (2013) Comprehensive Study on Cybercrime: Draft. New York: united Nations.
[45]. United States Congress (1977) Bill S.1766, The Federal Computer Systems Protection Act, 95th Congress, Ist Session, 123 Cong. Rec. (1977) 20; 953.
[46]. Valeriano, B.; B. Jensen and R. Maness (2018). Cyber Strategy: The Evolving Character of Power and Coercion. New York: Oxford University Press, pp. 22-52.

ONYEMAECHI AUGUSTINE EKE Ph.D, et. al. "Tapeworm in the Bloodstream: Addressing the Effect of Cybercrime for Human Security and Development in Nigeria." *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, 25(6), 2020, pp. 08-16.