CYBERCRIME AS AN EMERGENT SECURITY ISSUE IN NIGERIA: IMPLICATIONS FOR NATIONAL DEVELOPMENT

BY

Ugwu Ude Dave, Ph.D
INSTITUTE OF PUBLIC POLICY & ADMINISTRATION
UNIVERSITY OF CALABAR
E-mail: ugwudave@gmail.com
+234 (0) 803 09 45 800

Bassey Oben, Ph.D
DEPARTMENT OF MODERN LANGUAGES& TRANSLATION STUDIES
UNIVERSITY OF CALABAR
E-mail: basseyoben1@gmail.com, obenbassey@unical.edu.ng
+234 (0) 803 09 46 701

ABSTRACT

The advent of globalization facilitated by information and communication technology (ICT) launched Nigeria into the 21st century. As a consequence, Nigeria's socio-cultural space today is one where local events are being shaped by external forces at varied spheres. Cybercrime is one of the low sides of the introduction of ICT transactions, which today encompass all sectors of the nation's economy. The scourge of cybercrime has festered for some time, growing in leaps and bounds to become a major source of concern for corporate governance and planning in Nigeria. The need, therefore, for corporate security strategies to stem the menace cannot be overemphasized, especially in the banking sub-sector of the nation's economy where transactions are being encouraged through e-payment and cashless mechanisms. This paper takes an overview of the phenomenon of cybercrime in Nigeria. It takes cognizance of the age bracket of the culprits involved, its victims and the likely implications of the trend for national development and indeed, the image of the country as an

emerging global player in Africa. Security strategies to combat the menace of this hydra-headed monster in Nigeria and the world at large are also proposed.

Key words: Cybercrime, National Development, Security Strategies, Cashless Monetary Transactions, Advanced Fee Fraud, Money Laundering, Sustainable Development Goals.

INTRODUCTION

The advent of information communication technology (ICT), or the information superhighway and its concomitant challenges has introduced the incidence of cybercrime into the Nigerian socio-economic space. Cybercrime or computer crime has become a major source of concern to development planners and economists because of its negative effects on the economy, especially in the banking industry.

Cybercrime is the criminal activity involving information technology infrastructure. It includes illegal access to or unauthorized interception and manipulation of information through the information superhighway via a computer system which could be a laptop, desktop, palmtop, Ipad or such other devices that can guarantee unauthorised access to classified data. Put differently, cybercrime has to do with information interference or deliberate tampering with classified data through an electronic device with the aim of damaging, deleting, altering, suppressing or causing value reduction of such information to one's predetermined advantage. In its crudest sense, cybercrime is electronic theft or fraud.

As a matter of fact, cybercrime came in the wake of the emergence of digital technology to process information using hardware, software and internet systems. It is the vision of cyberspace to create a conducive atmosphere for internet platforms to fast track economic growth in nations of the world. The information superhighway created by the internet provides limitless opportunities for business expansion through the removal of barriers to economic development of nations. This advantage has been utilized by people, the world over to access the unique services provided by internet platforms. Unfortunately,

however, the ICT revolution in Nigeria has also created a volte-face scenario in the country by the thriving new crime wave orchestrated by internet fraudsters and scammers.

CAUSES OF CYBERCRIME IN NIGERIA

Crime, according to the French sociologist Emile Durkheim,

> is normal, because it is impossible to have a society without it. To classify crime among the normal phenomena of sociology, is not merely to say it is inevitable, though a regrettable phenomenon due to the incorrigible wickedness of man, it is to affirm that it is a factor in public health, an integral part of all healthy societies. (Dambazau, 20)

Philosophers and theorists alike have defined crime in the context of man and the society. That crime and society are inseparable is a normal assumption. The emergence of different dimensions of crime in the society is a function of social dynamism, integration and differentials. Durkheim further asserts that;

> Fundamental conditions of social organization logically imply that crime is not due to imperfections of human nature or social any more than birth and death. A society exempt from crime would necessitate a standardization of the moral concepts of all individuals which is neither possible, nor desirable. (76)

It needs be added, however, that cybercrime is not a cultural temperament of the Nigerian society. As earlier stated, it transcends from the advent of ICT through the medium of cyberspace.

The emergence of cybercrime has also been attributed to socio-economic rivalry. Interpersonal needs, social needs, demands of social functions, as well as social status, have been fingered as some of the possible causes of cybercrime among others. Because individuals need to measure up to social standards, the need to acquire the wherewithal becomes imperative. To shore up to these demands, those who are computer savvy indulge in internet fraud as an easy way out. The introduction of the internet as a result of the improvement and advancement in information technology is a potent factor for the emergence of cybercrime in Nigeria.

Individual criminality is not out of the question. Unemployment can be excused from it because criminal tendencies pervade every sector of the economy and indeed all ages and categories of people. People engage in internet scams because of their criminal minded nature. The desire or temptation to defraud the other person is inherent in human nature. Sometimes it begins with exchange of addresses, then other data and finally ends in the commission of crimes. Most youths or "yahoo boys" (youth adept at the computer system and who manipulate it to perpetrate internet scams) see it as a hobby. They can be seen glued to the internet as their duty post. Criminal minded youth in the country commit atrocities with the aid of the internet through online business transactions. Originally thought to be a blessing because of the numerous opportunities it exposes users to, the internet has today become a huge source of discomfort that hurts national development efforts in Nigeria, especially in the banking industry.

MANIFESTATION OF CYBERCRIME IN NIGERIA

Cybercrime has assumed a worrisome dimension in Nigeria. It may generally be categorized into two namely: crimes that target computer networks and such internet devices; and crimes that are targeted at individuals and business corporations such as banks.

Nigeria was recently classified as the innocent and passive player in cyberspace. The capture of Al-Qaeda's operative, Muhammad Naeem Noor Khan provided the Pakistan and American intelligence Agencies with some of Al-Qaeda's internet communication strategies. It also discovered that Nigerian websites and E-mail systems were hacked into by Al-Qaeda and were used to disseminate internet information to its formations and cells across the world. These discoveries brought to the fore the issue of the safety and security of Nigeria's cyberspace.

The categories and dimensions of cybercrime in Nigeria are alarming from the simple to the complex. The "simple" cases referred to here are the ones targeted at individuals. Here is a common process of a potential scam in Nigeria:

ACCOUNT BLOCK:

Dear customer your ATM debit card has been blocked by CBN due to BVN error.
Quickly call us@ 08106218359 to reactivate it under 24 hours.

Upon receipt of the text message, the unwary account holder is expected to place a call to the advertised phone number, whereupon the "bank official" at the other end will extract relevant data concerning the account in question with the supposed intention of rectifying "an error" which did not exist in the first place. Having obtained all relevant information regarding the account the scammers will then proceed to be making withdrawals from the tracked account.

The stock exchange is another danger pool for criminal activities by cyber hoodlums. It is common knowledge that stock exchange transactions are always done online. Without proper security measures in place, a country's stock exchange becomes the playground for cyber criminals. Through fraudulent methods, a nation's resources in the stock exchange market could be easily liquidated, as anyone can gain access to the net and appropriate its resources. It is a major threat in India as it is in Nigeria. For instance, in 2009, Punjab National Bank suffered huge losses when its computer recorders were deliberately manipulated to create false debits and credits. In the Bank of Baroda, a lot of funds were misappropriated through the computerized creation of false bank accounts. And in Delhi, a junior telecom operator working for Mahanager Telephone Nigam Ltd. was charged for reversing the electronic telephone meter recording system, thereby allowing some corporate users to make overseas calls without any charges directed to their telephone numbers (Ehimen and Adekanle, 2010).

In Nigeria, the banking industry has been computerized. This means that individual customers can access their accounts anywhere in the country. There are new platforms for e-banking, e-payment and other forms of cashless transactions which are now operational and which aim at making banking pleasurable and devoid of stress, even from the comfort of one's home. Unfortunately, the ATMs are prone to fraud conversion modules by "yahoo boys". *Daily Sun* foreign news documents that "Nigerians top that list of internet fraudsters in the Netherlands", (Tuesday, June 19 2007, p. 39). According to the report, police in Amsterdam arrested more than one hundred West Africans as part of a seven month long investigation into internet fraud. There is no gainsaying the fact that Nigerian internet fraudsters are spread all over Africa, Asia and Europe where they ply their trade.

Ehimen and Adekanle (2010) have pointed out that technology has integrated nations of the world into a single global village. The economy of most nations of the world is accessible via the internet through the aid of electronic devices. Since the electronic market is open to everyone, it also makes room for eavesdroppers, interlopers and criminals. Internet or cybercriminals take advantage of e-commerce platforms available on the net to con unsuspecting victims, mostly foreigners of millions of Naira.

In a vanguard newspaper report of Wednesday September 3, 2009, EmekaAginam highlighted the fears and dimensions of cybercrime in Nigeria as well as its increasing propensity. Sometimes cybercriminals fraudulently present themselves as having particular goods or services to sell, or that they are involved in a certain loan scheme. They could also pose as proprietors of financial institutions offering aid or grants to prospective investors. A certain some of money may be required to conclude registration formalities for eligibility. Once the registration fees are paid (and this comes from all over the world) the scammers disappear with their loot into thin air.

Merchants who place or take orders for merchandise on credit are also counting their losses as a result of cyber fraudster. Hoodlums also take undue advantage of foreign ladies who search for spouses through the internet. The fraudsters show interest as willing lovers of spouses. They present false curriculum vitae of themselves to desperate foreign ladies. The victims are cajoled into sending dollars to facilitate travel documents and residence from their victims. Once this is achieved, the "lover boys" clearly jump ship, go underground or simply disappear from the radar. There is the recent celebrated case of the Nigerian medical doctor turned cyber fraudster, trained in Canada and Ukraine. He had a promising career in medicine, but had to abandon it for internet criminality. Upon interrogation, he confessed he could hack into any banking platform in Nigeria within 67 minutes and transfer any amount of money he needed to any account he wished without being found out!

CYBERCRIME AND NATIONAL DEVELOPMENT

Cybercrime and insecurity are arguably the most dangerous threat to national development efforts in Nigeria today. The presence of cyber fraud impedes capacity building in the nation's ICT industry which is a major driver to rapid socio-economic transformation of the country. Issues involving ICT development are critical and vital on the global development agenda for all governments. As we migrate deeper into the unknown world of the digital revolution, no nation will be capable of achieving the objectives of the Sustainable Development Goals (SDGs) nor attain national development targets unless the hydra-headed monster of cybercrime is confronted head long. Nigeria is the most populous African nation as one in every six Africans is a Nigerian. The nation thus faces a herculean task of how to respond appropriately to the challenge of cyber criminality and insecurity. Non resolution of this burden will seriously hurt national development efforts on the long run.

CONTROLLING CYBERCRIME IN NIGERIA

As a responsible government, Nigeria has employed several strategies to combat not only cybercrime, but also to contain other allied financial atrocities and scams as they manifest. For instance, there is the National Drug Law Enforcement Agency (NDLEA) Act No. 48 of 1989, which is aimed at fighting the menace of money laundering through illicit drug peddling. This was done in conformity with the Vienna Convention. There is the Failed Banks (Recovery of Debts and financial malpractice) Act No. 18 of 1994, which was promulgated to check money laundering and round-tipping through insider sources in Banks. There is also the money laundering Act of 1995; the Advanced fee fraud (419) Act of 1995; as well as the Banks and Other Financial Institutions Act (BOFIA) and the CBN Acts of 1999, which established the independent corrupt practices and other related offences commission (ICPC).

On its part, the Nigerian National Assembly has debated and passed bills aimed at regulating the operations of cyber activities in the country with a view to curbing internet-assisted crimes. These include the Internet Freedom Bill and the Electronic Data Bill (2001). In the same year, the Nigerian government set up the National Committee on Advanced Fee Fraud (NCAFF) with a charge to develop strategies to nip the activities of fraudsters and their agents in the country in the bud. This came against the backdrop that Britain, France and the USA were planning to blacklist the country unless serious deliberate measures were put in place by government to combat mindless theft of public funds by Nigerian government functionaries and their foreign collaborators. With a deadline set at December 2002, the efforts of this committee led to the promulgation of the Economic and Financial Crimes Commission (EFCC), with unlimited powers to trace, track and investigate accounts of any person suspected to be involved in such frauds.

Then there is the National cyber security initiative, a product of the Nigerian cybercrime working group whose membership includes all the country's security and ICT

agencies, including the police, the DSS, EFCC, the National Security Adviser, the Nigerian Communication Commission, the National Intelligence Agency and the Nigerian Computer Society. The task of this group is to develop cybercrime and cyber security regulations in the country. Also, with the assistance of the FBI, Nigerian and Ghanaian officials were trained in 2005 on strategies targeted at reducing cybercrimes and other related economic and financial crimes in these countries.

Following from the above, there is no gainsaying the fact, that the EFCC in Nigeria has secured a lot of convictions against many high profile former government functionaries who were involved in fraud while in office. This list which includes former state governors, top military brass and private business collaborators, has led to the recovery of a huge chunk of slush funds embezzled and laundered abroad by these former political henchmen in Nigeria.

CONCLUSION

In this paper, we have discussed cybercrime as the use of the computer and internet mediated communication to commit crimes. Cybercrime by our understanding is a generic term for frauds involving e-mail scams, hacking and distribution of hostile software (viruses), denial of access to service, attacks, deletion and theft of data, extortion, fraud and impersonation, among others. The common denominator for all the above listed misdemeanors is that they are computer-aided crimes.

The efforts of government and public agencies in the fight against cybercrime are commendable, but there is clearly need to do more. The Nigeria Police Force, for instance, lacks the internet policing capacity. At present, the Nigeria Police is still technologically blank and is therefore incapable of tracking cybercrimes. The lack of adequate forensic training for its personnel renders the force ill-equipped for this fight of wits and savviness. It

is important therefore, to have cyber police, whose personnel are trained and equipped to stay ahead of cyber hoodlums.

The need for a National computer crime resource centre, to advise government and other investigative agencies to better organize and co-ordinate cyber terrorism cannot be over emphasized. This centre will regulate standards and authenticate citizens' records, as well as staff of established organizations, firms and industries online. Also, a forensics commission to form the training of forensic personnel will not be out of place in the country. Generally, the National Orientation Agency (NOA) needs to refocus its agenda aimed at debriefing Nigerians, especially the youth, on the dangers of cyber criminality.

Finally, it is also hoped, that the whistleblower policy recently introduced by the government of President Muhammadu Buhari will help to bring some sanity to bear on the magnitude of not just cybercrimes but also other ancillary financial crimes being perpetrated in the country. All these measures, it is hoped, will make investing in the nation's economy safer and national development will be the logical outcome of such enterprise.

REFERENCES

Adams, J. A. (2003). Political corruption and National economic decline: An assessment of the impact of corruption on the Nigerian economy. *Calabar Journal of Politics and Administration, 2*(1): 105-119.

Awamleh, R., Evans, Jr., &Mahale, A. (2003). "Internet banking in emergency market: The case of Jordan- A note". *Journal of Internet Banking and Commerce, 8*(1).

Bachanan, J. & Grant, A. J. (2001). Investigating and prosecuting Nigeria fraud". *United States Attorney's Bulletin*. November 2001: 39-47.

Central Bank of Nigeria.*Guidelines on Electronic Banking in Nigeria*. August, 2010. (http//www.centralbank.org/OUTPUBLICATIONS/BSD/2003/E-BANKING.PDF). Retrieved 20th October 2010.

Centre for Law Enforcement Education (2010). *National crime and safety survey*. Lagos: CLEEN Foundation.

Daily Sun (Nigeria) *Newspaper*, June 19, 2009, P. 11.

Dambazau, Abdulrahman Bello (2007). *Criminology and criminal justice*. Ibadan: Spectrum.

Durkheim, Emile (1895). "Rules of sociological methods" in E. McLaughlin et al (eds) 2008. *Criminological perspectives: Essential Reading, 2nd* Edition. London: Sage Publications.

Ehimen, O. R. & Bola, A. (2010).Cybercrime in Nigeria.*Business Intelligence Journal, 3*(1): 93-99.

Ezeoha, Abel, E. (2005). Regulating internet banking in Nigerian: problems and challenges part 1". *Journal of Internet Banking and Commerce, 10*(2) December 2005.

Hunda, Ramjit Singh et al. (2004). Aspects of digital evidence.*Law Journal, Nanak Development University, Amristar 8(1):2004.*

Kumar, Krishna (2003).C*yber laws, international property and e-commerce security*. New Delhi: Dominant Publishers and Distributors.

Longer, O. B. &Chiemeke S. C. Cybercrime and criminology in Nigeria: what role are internet access points playing? *European Journal of Social Science 8* (2): 132-144.

Okonkwo, C. O. (1996). *The police and the public in Nigeria*. London: Sweet and Maxwell.

Vanguard (Nigeria) *Newspaper*. September 3, 2009. P49.