Lapai Journal of Humanities *Vol. 13 No. 1, June 2022*
(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

Impact of Cybercrime on National Development: A Review on Nigeria

Juliet Jenebu Obajobi,[1] Francis Ojima Akoji[2] & Chubado Umaru[3]
[1]*Ahmadu Bello University, Zaria, Nigeria*
julietokp@gmail.com
[2]*Principal Partner, Dei Donum Legal, Abuja, Nigeria*
akojif@yahoo.com
[3]*Office of the Deputy Vice Chancellor Administration,*
Federal University Gusau, Nigeria
chubadoumaru@fugusau.edu.ng

Abstract

Humans will continue to seek ease of life and consequently record breakthroughs in diverse aspects of life. Often, this growth and development will have its positive and negative sides, one of which is cybercrime. The internet with its benefits has a plethora of downsides and it has wrought a lot of havoc on socioeconomic and political wellbeing of nations. The drive of every nation is to develop to its full capacity and potentiality, but this among other factors continues to act as a stumbling block to this development. This work will consider the impact of cybercrime on national development in a bid to recommend ways of curbing cybercrime and positioning the national interest before individual interest which hampers the direction of national development including an examination of the legal instrument of control both locally and at the international plane. In the end, this study concludes that the growth of cybercrime in relation to fraud is a digital pandemic that will continue to spread in Nigeria in the years to come if offenders are not dealt with according to law, to serve as deterrence to intending offenders. The research methods employed are derived from secondary sources such as the internet, textbooks, journals and articles within the area under study; governmental material from law enforcement, intelligence and policy communities, and non-governmental sources like reputable global cyber security vendors, consultancy companies and academia or research institutes (secondary sources were reported using the triangulation process). The retrieved data from books, journals and newspapers were analyzed using content analysis.

Keywords: Cybercrime; National Development; Malware; Hacking; Phishing.

Introduction

Human civilization has advanced through the ages to its current position due to human drive and desire to utilize God giving intellect towards creating a better living. The efforts of man have yielded good fruits in various ways part of which is the breakthrough in information technology which has provided wide access to information. This unfettered access to information and ease of

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

communication has transformed the world to the point that it is justifiable to say it is a global village, because nations of the world more than ever before are now so connected. However, there are downsides to unhindered access to the internet, as it has introduced diverse changes to human life, one of which is the surge in criminality.

Cyberspace has become a haven for crimes and criminality with the advent of technological breakthroughs. While its benefits in improving communication and other spheres remain veritable, it has become a tool in the hands of evil plotters especially when tech users fail to take the most basic protective measures and where tech products lack defences (Chong, 2013; Akinyetun, 2021). The spate of cybercrime in Nigeria has experienced cataclysmic eruption with many youngsters using, misusing and abusing the access gained to the internet network. Various range of criminal activities have now arisen ranging from cyber stalking, cyber extortion, cyber bullying, phishing, etc. the socioeconomic affairs of the country are greatly affected and until something is done to avert the dangers arising from cybercrime, it is likely to crumble a nation's peace and security as well as sabotage the economy (Bhawna, 2016).

The internet came into Nigeria in 1996 and between then and now, Nigeria has over 108 million internet users according to demography and it is expected to rise by 60 per cent in 2026 (Johnson, 2021). The internet creates unlimited opportunities for commercial, social and educational activities. There is a noticeable change in socioeconomic sphere and development such as banking, insurance, stock market, low production, service etc. which have consequences such as email scam, identity theft, child pornography, organized crime and solicitation for prostitution, fake lotteries and scam text messages as well as cyber-piracy. It has introduced its own peculiar risk that poses danger to the economic, social and political life of countries and the world at large including Nigeria. The dangers could affect many sectors of society and put the development of the country in peril. Nigeria is a very youthful country, with the vast majority of its population comprising of young people who are doing everything possible to make ends meet. With this teaming population comprising of majorly youths, makes cybercrime an epidemic which needs to be contained. Sorunke (2011) maintained that Nigeria in the cyber-space is under threats with such vulnerability, many loopholes in our system and issues bothering our payment networks. If urgent steps are not taken by businesses and governmental organization deploying web-based platforms for their operation and with the rate of cyber security in Nigeria, companies might soon be faced with a high incidence of hacking leading to loss of data critical to business life and revenue.

Hence, this work looks at the implication of cybercrime on national development in order to examine the menace this has caused to national development and proffer plausible ways of combatting internet crimes. The research will make recommendations that can be adopted by governments and other institutions towards quelling this menace both locally and internationally.

Conceptual Clarification

Cybercrime is defined as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause psychical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the internet (chat rooms, emails, notice boards and groups) and mobile phones (Debarkaton and Jaishankar, 2011).

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

Phishing or "web spoofing" is a type of social engineering method in which an attacker attempts to acquire PII through a fraudulent method of emailing bulk messages to victims (Brody *et al*., 2007). A common factor that many users face is the use of the same username and password for multiple sites, and then the imposter sends a link asking the victims to verify.

Malware is the use of malicious software to obtain the desired information directly from the user's computer. They can also be designed to intercept communications or log keyboard strokes by recording every entry made by a user and this information can be sifted electronically for passwords and related information.

Business Email Compromise [BEC] is the act of sending an email from a spoofed or compromised account to the victim company's financial institution requesting a wire transfer. Once the transfer is sent, the payment details are intercepted by the criminals and changed (Akinyetun, 2021).

Hacking involves breaking into a person's computer to compromise information, this is often perpetuated from a remote location and takes advantage of loopholes in the victim's computer program (Adepegba, 2021).

The Wave of Cybercrimes among Nigerian Youths

Society is evolving and new things sprout up daily with the advancement in technology and globalization, it cannot be said that they are known or predetermined, but we learn to describe them and attribute meanings to them. Cybercrime means different things to different people depending on the lenses from which it is viewed. To be able to guide our thoughts in this research, we will consider some scholarly definitions already proffered as it has been defined in a variety of ways by scholars and researchers. While there is no blanket or one-size-fits-all definition, the basic elements of the definition reflect in all definitions. For Moore, Cybercrime refers to any crime that involves a computer and a network (Moore, 2005). It is a fast-growing expanse of crime whereby the internet has been used to commit a variety of criminal actions that knows no borders either physical or cybernetic (Interpol). According to Folashade and Okeshola (2013), the information technology revolution associated with the internet has brought about two edge functions: that is, on one hand, it has contributed positive values to the world. While on the other hand, it has produced so many maladies that threaten the order of the society and also producing new wave of crimes in the world (Folashade and Okeshola 2013). Shinder (2002) opines that cybercrime is any criminal offenses committed using the internet or another computer network as a component of the crime.

Cybercrimes come in different ways depending on the way and manner the internet is utilized to orchestrate them (Jane, 2013). It cannot be said that mankind has seen all the types of crimes affiliated with the use of the internet, as criminals will always struggle to break new grounds and foment different types of criminal activity using the internet as a tool. There are diverse types of cybercrime part including Website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mail, cyber laundering, wiretapping and virus/worm/Trojans. According to Ribadu (2007), the most common form of cybercrime in Nigeria are cloning of websites, false representation, internet purchases and other e-commerce kinds of fraud. While these lists may not even exhaustively accommodate the known types of cybercrime, the unknown is a plethora and the ones to come if the uses of computers, the internet and other electronic

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

devices are not tailored to suit societal needs and development cannot be quantified (Jaja and Jude, 2013). With the spate of terrorism, efforts to disrupt the security and financial health of nations cannot be explained.

The transformation of information and communication technology in Nigeria has resulted in an inevitable spike in criminality. Albert Einstein's remark that technological progress is like an axe in the hands of a pathological criminal comes to mind (Folsing, 1997). Activities of people in Nigeria today are knit to technology in virtually all spheres. Information is now digitized with an attendant consequence of people seeking more rapid, open and global access to information. In Nigeria, cybercrimes are not age restricted as they can be by people of all ages, both old and young alike. Although it is more common with the younger generation because hacking tools have become more accessible. With the increase in computer usage and internet access as well as access to other electronic devices and the convenience, more young people are prone to be commissioned into crimes on the internet (Jonathan *et al*., 2004). In recent times there is a surge in the activities of cybercrime by young people, with trends of ritualistic activities connected to it, and even leading to the murder of victims of such rituals.

Its Implication on National Development

The term National Development is all-encompassing as it relates to the overall wellbeing of the nation and individuals therein. National development is geared towards the improvement of the standard of living of citizens. The term national development is very comprehensive; it includes all aspects of the life of an individual and the nation. It is a process of reconstruction and development in various dimensions of a nation and the development of individuals. National Development is also the gradual manifestation of positive changes in the economic, industrial, political, social, cultural and administrative life of a country (Ogai, 2007). It is an all-round and balanced development of different aspects and facets of the nation *viz* political, economic, social, cultural, scientific and material.

National Development is hinged on several factors and is greatly influenced by the participation of every member of the nation. The activities of members have an impact on the affairs and running of the nation (Kamini, 2011). On the international plane, the world is grumbling with various menaces ranging from insecurity, and data violation to economic sabotage, these are issues that hamper development. It is even more worrisome when these are left for an individual state to deal with personally. While the world is glory in the gains of technology and its consequent developments in virtually all spheres of human life, there is more than ever before, a need to take a reflective posture towards the ills that these advancements are clouded with. We celebrate the access to the internet and how in milliseconds we get things done and can access information, but we need to examine how the information is being misused and abused.

While it is a good thing to have the internet, it can cause severe damage when left in the hands of bad people. The effect cybercrime has on the image of the country and its effect on restricted business opportunities and social interaction should also be emphasized. The gains of access to the internet have brought upon us, the debilitating effect of cybercrime. It is dealing a heavy blow on the nations of the world. In fact, a report by International Monetary Fund ranks cybercrime as 3rd in dollar value as a global scourge (Maurer, 2021). A Cyber security venture, a company providing

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

research into threats opined that damage from cybercrime activity is expected to cost the global economy $ 10.5 trillion a year by 2025. The effect on security in a world heavily hit by issues of insecurity is immeasurable. Jonathan (2004) said that cybercrime may threaten a nation's security and financial health. In Nigeria, the common negative effects Cybercrime has generally been revenue losses, disruption of business, profit pilferage, and welfare losses. In most cases, affected stakeholders do not have records of losses encountered or let's say the concealed losses information, projecting losses based on assumptions. Meanwhile, Financial Derivatives Company FDC (2020) reports that the estimated annual financial loss in Nigeria due to cybercrime was N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018.

More so, as a result of identity theft and unauthorized access to data, it has led to international reputational mistrust. Folashade and Okeshola (2013) corroborated this by opining that cybercrime can "destroy image home and abroad, insecurity of life and properties, fear of doing business with Nigeria citizens. Recently, any social interaction with a foreigner over the internet as a Nigerian has become a problem in itself, as you are faced with the challenge of trying to explain how you are not a potential scammer or related to one. This is large because according to a 69-page document released by the United States District Court in February 2021, it was alleged that Abass (Cyber fraudster, famously known as Billionaire Gucci Master Hushpuppi) paid $20,600 to Abba Kyari (Nigeria Police Officer and leader of the Intelligence Response Team) to unlawfully detain and torture Kelly Vincent over a disagreement. The police officer was allegedly involved in an international scheme to defraud a Qatari businessman the sum of $1.1m. Abass was arrested by the Dubai police on June 10, 2020, alongside 12 other accomplices in connection with multiple fraud charges amounting to $35million. He and his major accomplice Olalekan Jacob Ponle (Woodberry) were accused of committing crimes outside the UAE, including hacking, money laundering, banking fraud, cyber-fraud, criminal impersonation, and identity theft. The Dubai CID claimed incriminating documents were found of planned frauds worth a total of $435 Million. Also seized in the arrest were $40.9 million in cash, 21 laptop computers, 12 luxury cars valued at $6.8 million, 47 Smartphones, five hard disks, and 15 memory sticks, all containing 119,580 fraud files as well as addresses of 1,926,400 victims. Cybercrime decimates the reputation of a country, making the business environment unconducive for Small and Medium-Sized Enterprises (SMEs) and start-ups, while discouraging investment in the economy by foreign companies. This is worrisome considering that after the arrest of Abass, six Nigerians were placed on the FBI's most-wanted list, alongside 73 others from different countries. The six Nigerians Alex Ogunshakin, Richard Uzuh, Abiola Kayode, Micheal Olorunyomi, Nnamdi Benson, and Felix Okpoh were accused of perpetrating Business Emails Compromise and romance scams to the tune of $6.3m in losses by Americans (Akinkuotu, 2021).

A major implication of cybercrime for national development in Nigeria is communal and sectarian violence. They affirm that social media is being used to spread hate speech and divisive contents which often give rise to tension among various groups in the country. For example, social media has been used to frame the prevailing farmer-herder conflict in the country as an ethno-religious crusade. In addition to using cyberspace to incite violence, cybercriminals are beginning to commit acts of terrorism via computer networks. Cyber terrorism, cyber espionage, insurgency financing, and recruitment are gradually becoming the norm. Indeed, cyberspace is now being used to solicit funds, increase the membership of terrorist organizations, drive ideological indoctrination, and

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

promote radicalization. The Boko Haram insurgency group in Nigeria is beginning to have a cyber-presence. The Boko Haram sect hacked the servers of the Department of State Security on August 30, 2013, and leaked the details of over 60 officials including their addresses and names of family members. This is a big threat to the lives of the officials and their family members, and of course, a strain on national security (Akinyetun, 2021).

In addition, another implication of cybercrime is its effect on the educational system. The advent of social media has easily spread the awareness of cybercrime among the youth in Nigeria. This has drastically increased the quest for participation in cybercrime, having seen the lavish lifestyle fluent on social media, clubs, and other social gatherings not knowing the danger behind this wealth. Some youths go as far as withdrawing from school to join the pyramid of cybercriminals which is motivated by the influx of youth to the urban city where it is lucrative to be established. They also travel out of Nigeria to other countries to hide and carry out their activities without an easy trace (Ogunjobi, 2020). Meanwhile, victims of cyber-attacks usually suffer from emotional trauma, they feel that they are to be blamed for the attack, they prefer not to involve anyone, or preferably handle the situation themselves which results in isolation, depression and suicide, and drug abuse.

Legal Regime/Mechanism for Combating Cybercrime

The spate of cybercrime in the world and Nigeria, in particular, is at an alarming high thus, there must be in place a legal mechanism to combat cybercrime. The import of this cannot be overemphasized because the more simplified the access to the internet is, the more the need to strengthen the legal system to be able to contain it because new crimes related to the internet will sprout daily.

In Nigeria, the laws on cybercrime have been harmonized in the Cybercrime (Prohibition and Prevention) Act 2015, which is geared towards mitigating and prosecuting cybercrime. The act is the shield of cyberspace even though it cannot be said to be comprehensive enough to perform the task of prohibiting, detecting, prosecuting and punishing cyber offenders. It is an institutional framework to safeguard the legal right of the users of the internet and oversee the distribution of software, information, online security and e-commerce through the internet (Ogunjobi, 2020). It also helps to give legal validation to documents.

However, pertinent to note are the areas that need improvement or adjustment that the law did not take cognizance of. Firstly, it does not provide for a very common form of cybercrime in Nigeria which is email spam. Section 15 of the Act only referred to the crime of sending messages that are offensive, indecent, obscene, and false or messages meant to annoy or harm another. The act is not comprehensive enough compared to what is obtainable in other foreign jurisdictions as it does not provide for compensatory damages to victims of cybercrime (Ogunjobi, 2020). It does not allow victims who suffer damages as a result of violations of the Act to institute civil actions against the violators for injunctive or equitable reliefs. Section 31 only makes provision for forfeiture to the federal government by neglecting the interest of the victims.

Section 24 (3) of the Act allows law enforcement, security and intelligence agencies to undergo training programmes. While this is plausible, adding the judges who will adjudicate on these issues to the list would have been advantageous because the cases coming before them will require their

(ISSN: 2006-2826 – Print / ISSN: 2682-6356 - Online)

ability to determine and establish the occurrence of these crimes. Section 8 and 9 also prevents the modification of computer data and computer system through malicious codes such as viruses they do not prevent the creation and distribution of computer viruses among people (Ogunjobi, 2020).

Recommendations

I. The pace at which most Nigerian youths are eager to make quick-money is alarming, this greed has led them into all sorts of crimes. There is therefore an urgent need to sensitize and reorient youths on the dangers of cybercrime and the effect it has on the individual, image and national security of Nigeria.
II. Cyber security should be made an interdisciplinary and compulsory course of study in Nigerian schools.
III. Cyber Forensics Department should be created to analyze and keep track of cyber activities and investigate any suspected acts of cybercrime.
IV. The government should partner with the Nigerian Police and set up Anti-Scam Reporting Channels across the thirty-six states of the federation, so that people can easily report suspected cybercriminals.
V. Modernization of current processes, such as the Mutual Legal Assistance Treaty (MLAT), which allows governments to enlist the help of other governments in cybercrime investigations and evidence collection.

Conclusion

From the preceding discourse, Cybercrime is a great threat to the Nigerian economy and even to its national peace and security. The study has shown that the abuse of computer technology threatens national security, public safety and even devastates the lives of affected individuals. However, Nigeria like most African countries has a weak legal framework and weak legal enforcement to effectively combat cybercrime. As shown in the research work, the legal framework regulating cybercrime in Nigeria is not as comprehensive as other developed jurisdictions particularly in reference to the US jurisdiction. Therefore, regulating the abusive usage of the internet, and social media just like china, Japan, and other world power will go a long way to check the excesses of cyber risk.

References

Akinkuotu, E. (2021). "$6.3m fraud: Six Nigerians placed on the FBI's most-wanted list." online:<https://punchng.com/6-3m-fraud-six-nigerians-placed-on-fbi-most-wantedlist/>.

Akinyetun, T.S. (2021). "Poverty, Cybercrime and National Security in Nigeria" *Journal of Contemporary Sociological Issues*, Volume 1, Issue 2, pp. 1-23. DOI: 10.19184/csi.v1i2.24188

Adepegba, A. (2021). "Hushpuppi: Kyari risks dismissal, criminal prosecution" Punch News https://punchng.com/hushpuppi-kyari-risks-dismissal-criminal-prosecution-says-psc/

Bhawna, B. (2016). National Development: Meaning and Problem" Web. 7 January. http://www.yourarticlelibrary.com/society/national-development-meaning-andproblems/7682

Brody, R.G. Mulig, E. and Kimball, V. (2007). "Phishing, pharming and identity theft" *Academy of Accounting and Financial Studies Journal*, 11(3), 43–56C

Financial Derivatives Company FDC (2020) Annual Report. https://fdcng.com/

Folashade, B.O. and Abimbola, K.A., (2013). "The Nature Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria- Kaduna State, Nigeria" *American International Journal of Contemporary Research* Vol. 3 No 9 pg. 98-114 at www.aijcrnet.com

Holder, D. and Jaishankar K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations* (Hershey, PA, USA: IGI Global 2011), ISBN 978-1-60960-830-9

Jackson, J. (2006). "Cybercrime and the Challenges of Socio-Economic Development in Nigeria": *JORIND* 14 (2) www.transcampus.org/journal

Jaja, N. and Jude, O. (2013). "Security and National Development in Nigeria: The Threat of Boko Haram": *International Journal of Humanities and Social Science* Vol. 3 No 4

Jane, C. (2013). *Why Is Our Cyber Security So Insecure?*', Cyber Trust and Cybercrime Prevention Project

Kamini D. (2011). "Cybercrime in the Society: Problems and Preventions": *Journal of Alternative Perspectives in the Social Sciences* Vol. 3(11). pp. 240-259

Maurer, T. and Nelson, A. (2021). "The Global Cyber Threat" IMF: Finance and Development": https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-system-manurer.pdf

Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime,* Cleverland, Anderson Publishing

Ogai, J.O. (2007). "An Analysis of the Concepts of Development and Underdevelopment" in O. Uwakwe, *Communication National Development*, (2nd edition), London, Cecta Books Publishers, 25-31.

Ogunjobi, O., (2020) "The Impact of Cybercrime on Nigerian Youths" *Research Gate Publication*. https://www.researchgate.net/publication/347436728

Okechukwu, O.A. (2012). "Religion and National Development" *American Academic and Scholarly Research Journal* Vol. 4 No. 4. www.aasrc.org/aesrj

Ribadu, E. (2007). "Cyber Crime and Commercial Fraud: A Nigerian Perspective". A Paper Presented at Conference of *the Modern Law for Global Commerce, Vienna 9th – 12th July,*

Shinder, D.L. (2002). *Scene of the Cyber Crime: Computer Forensic Handbook*, USA Syngress Publishing Inc.

Ume, T.A. (1987). "Towards a More Restricted Definition of Development" in F.C. Okafor, E.C. Okeen and J. Mereni (eds.) *Foundation of Adult Education a Book of Readings* Anambra: Pacific Publishers. pp. 86-100

www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf accessed 20th February, 2022.

www.interpol.int/crime-areas/cybercrime/cybercrime accessed 20th February, 2022.