journals.unizik.edu.ng/index-php/jcpl ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW

Examining the Effect of the Elevated Rate of Cybercrime on the Growth and Sustainable development of Nigeria's Economy

Onwugbenu Ezinne Olivia*

Abstract:
The cyberspace has provided an internet platform which has enabled geometric growth, productivity, efficiency and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by corporate organizations across the globe. It goes without saying that Nigeria's economy in recent times have had advancements in Information and Communications Technology which can be seen in every facet of its industries. This growth has also attracted innumerable crimes which has directly and otherwise affected the growth and sustainable development of Nigeria's economy, especially in the form of Cybercrime. Nigerians have become cyber-creatures, spending significant amount of time online. As the digital world expands, so does cybercrime in Nigeria. While the escalation of cybercrime could not be curtailed adequately by crime prevention agencies, the effects continue to bite hard on our economy, both locally and internationally. The necessity to combat these seemingly uncontrollable phenomena gave rise to Cyber Laws in Nigeria. This paper has attempted to provide an overview of cybercrime, it will also analyze the effect of cybercrime on the growth and sustainable development of Nigeria's economy. This paper has also furnished preventive measures to be put in place to curb cybercrimes in Nigeria. This article recommends that the Nigerian government must become proactive and focused in the continuous fight to curb the menace and mitigate its effect on the citizenry. Furthermore, Cyber laws should be made more effective in acting as a shield over cyberspace, preventing cybercrime from occurring.

Keywords: Cybercrime, Cyberspace, Internet security and Nigeria's economic growth and development

1.0 Introduction

The proliferation of the internet in Nigeria has indeed come with unintended consequences, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. The Cybercrimes (Prohibition and Prevention) Act 2015 has a significant impact on cyber law in Nigeria. This Act creates a comprehensive legal, regulatory and institutional framework in Nigeria to prohibit, prevent, detect, prosecute and punish cybercrime.[1] This Act also encourages cyber security and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights as well as the protection of important national information infrastructure.

*__Onwugbenu Ezinne Olivia__ LL.B, BL, LLM, Lecturer II, Department of International Law and Jurisprudence, Faculty of Law, NnamdiAzikiwe University, Awka Nigeria. Email: eo.onwugbenu@unizik.edu.ng; oliviaonwugbenu@gmail.com+2348066647575, +2348093430945

[1]Cybercrimes(Prohibition and Prevention) Act 2015

The internet has become an invaluable tool for governments, businesses, military, associations and individuals. Cyberspace is constantly evolving, so too is the threat of cybercrime on national security, prosperity and quality of life of the citizenry and the world as a global village. Just like governments of all sovereign nations, the government of Nigeria is committed to protecting Nigerians from the threat of cybercrime.[2]

The internet's rapid diffusion and digitization of economic activities have led to the emergence of new breed of criminals. In recent years, economic, political and social impacts of these cyber criminals' activities have received considerable attention. Individuals, businesses and government rightfully worry about their systems, network and IT infrastructure. The crimes have brought about a huge negative impact on our economic development.

Considering the pattern of cybercrime, it is apparent that many underlying assumptions are flawed, unrealistic and implausible to explain with this novel form of criminality. The empirical record regarding cybercrime patterns and strategy to avoid and fight the crimes run counter to the functioning of the cyber world.[3]

There are various ways to gain access to information in cyberspace. Attackers can exploit vulnerabilities in software and hardware. They can exploit security vulnerabilities by tricking people into opening infected emails or visiting corrupt websites that infect their computers with malicious software. They can take advantage of people who fail to follow basic cyber security practices, such as changing their passwords frequently, updating their antivirus protection on a regular basis, and using only protected wireless networks. At the turn of the 21st century, Nigerian internet penetration levels took a running jump. Whereas the number used to be less than 5% in 2002 – 2003, it stood at over 40% by the end of 2015 and the growth is only poised to accelerate. The advent of mobile telephones on the Nigerian market played a major role and continues to be a key driver in economic advancement.[4]The VSAT deployments that were once the only source of dependable internet connectivity has since been rendered quaint and antediluvian, compared to the untapped capacity of the undersea broadband cable that have been brought to the coast of Nigeria since 2009.[5] As time wears on, competition and market forces continue to act on the industry, constantly nudging quality up and costs down for the average consumer.

However, the rise of the internet in Nigeria has come with an unintended consequence – global notoriety as a haven of cybercrime. Back in the 90s, fraud in the Nigerian society was popularly called "419" in reference to the criminal code that framed the criminal justice system in Nigeria. At the time, persons who were arrested in connection to that law were labelled '419'. Enforcement and a ponderous criminal justice system meant that the rampant practice of 419 was already a constant source of grief. Then along came the internet, shortly after which a number of tech-savvy cons successfully "exported" the 419 concept. While the popular 419 reference has

[2]C. Shafic, Adamu, "Cybercrimes and the Nigeria Academic Institution Networks Cybercrime, its impact on government, society and the prosecutor". (2011)

[3] Dartmouth Business Journal: Posted by Ethan Portnoy '14 on Wednesday, (May 30, 2012)

[4]*W. Edwards Deming* (1990). Sample Design in Business Research. John Wiley and Sons, 1990, p. 31. ISBN 0-471-52370-4.

[5]C. *Dupasquier*, P.Osakwe,(2005) Foreign Direct Investment in Africa: Performance, Challenges and Responsibilities. African Trade Policy Center. Work in Progress No.21 Economic Commission for Africa.

since been extended to include cyber criminals, in Nigeria the name "Yahoo-Yahoo" is the most familiar informal usage that is employed to speak of people who perpetrate scams online.

2.0 Definition and Nature of Cybercrime

The word 'cybercrime' derives it definition from the word 'cyber' which has its origins from 'cybernetics', and refers to the science of communication that deals with the study of automatic control systems (much like the human nervous system/ workings of the brain) as well as the mechanical &electrical communication systems. Cyber is therefore a derivative of cybernetics used to describe interactions that relate to, or involve computers or networks.

'Crime' refers to the specific actions or inactions due to negligence that is injurious to public welfare or morals, and one that is legally prohibited. Cybercrime (e-crime or hi-tech crime) is a global phenomenon which takes place in the cyberspace i.e. in the world of computers and on the internet. Cybercrime involves using specialized applications in computers with the internet by technically skilled individuals to commit crime.

In the past, the former descriptions of cybercrime were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Since the internet was invented, other new terms, like "cybercrime" and "net" crime became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental.[6]We therefore come to terms with a conclusion on the meaning that cybercrime is an evil having its origin in the growing dependence on computers in modern life.[7] A simple yet sturdy definition of cybercrime would be unlawful acts wherein the computer is either a tool or a target or both". Defining cybercrimes as illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime in a broader sense computer-related crime: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. Cyber Crime refers to all activities done with criminal intent in cyberspace. Cybercrimes in Nigeria fall into three categories: (a) Crimes against persons. (b) Crimes against Business and Non-business organizations. (c) Crimes against the government.

The aftermath of such crimes may threaten a nation's security architecture and financial health.[8]

2.1 Types of Cybercrimes

In the past, little was known about cybercrime, but as the internet grew worldwide, the unintended consequences of computerization manifested in global notoriety. It is a worldwide problem that costs countries, businesses and individuals billions of dollars. The first reported

[6]N. Ribadu, "Cybercrime and Commercial Fraud: A Nigerian Perspective Modern Law for Global Commerce Congress" to celebrate the fortieth annual session of UNCITRAL Vienna, 9-12 July (2007)

[7]A. Azeez, O. Osunade, "Towards ameliorating cybercrime and Cyber security", *(IJCSIS) International Journal of Computer Science and Information Security", Vol. 3,* No. 1, (2009)

[8]*Saul H.* (2007): Social network launches worldwide spam campaign New York Times.

cybercrime was committed by employees of a company in the 1960s and involved the company's mainframe computer.[9]

There are several ways we can categorize the various cybercrimes. We can divide them into two very broad categories: (1) those crimes committed by violent or potentially violent criminals, and (2) non-violent crimes. Types of violent or potentially violent cybercrime include: Cyber terrorism; Assault by threat; Cyber stalking and child pornography.[10]

Cybercrimes include three main offending patterns.[11] The focus of the offending can either be the integrity of the system (hacking) or the computer can be used to commit an offence, else the content of the computer itself can be the object of the offending.

- Child exploitation: In 2005, the Virtual Global Task Force defined child sexual abuse online as the sharing and downloading of images of children being physically and sexually abused and approaching children online with the aim of developing asexual relationship in the 'real world', also known as 'grooming'.[12]Child exploitation is not an invention of the internet age by any means. However, the Internet has become the new playground for consumers of child pornography and a market place for those who provide it.

- Harassment**:** The term is normally used to refer to the use of the Internet, e-mail, or other electronic communications devices to harass another person.[13](Black and Kenneth, 2010).

- Digital Piracy: The development of the personal computer has led to wide spread use of the Internet, which allows for an exchange of information and the production of behaviours that include crime. One form of crime on the Internet is digital piracy.[14]Some researchers defined digital piracy as the act of copying digital goods that include software, documents, audio (including music and voice), and video for any reason other than to back up without explicit permission from and compensation to the copyright holder using computer technology.

- Hacking**:** Unauthorized access may occur both on individuals' personal computers, as well as in the workplace. 'One major form of unauthorized access is known as hacking.

[9]O. Maitanmi., S. Ogunlere & S. Ayinde (2013): Impact of Cyber Crimes on Nigerian Economy, The International Journal of Engineering and Science (IJES, vol. 2(4) 45–51).

[10]*M. Chawki*, (2005) "*Cybercrime in France: An Overview"*[Online] available from<http://www.crime research.org/articles/cybercrime-in-france-overview/> [February 28, 2011].

[11]*Wall, S. David* (2005) The Internet as a conduit for criminal activity, In A. Pattavina (Ed.), Information technology and the criminal justice system (pp.78-94) Thousand Oaks, CA: Sage..

[12]E. *Martellozzo, D. Nehring,H. Taylor* (2010) *Online child sexual abuse by female offenders- An Exploratory study*, International Journal of cyber criminology Vol 4 Iss 1and2, pp 592–609 [Online] available from<http://www.cybercrimejournal.com/elenaetal2010ijcc.pdf/> [September 15,2005].

[13]*G. Black, Hawk & R. Kenneth* (2010) "Computer and Internet crimes", San Francisco, California [Online] available from <http://www.fd.org/pdf_lib/WS2010/WS2010_Computer_Crimes.pdf> [March 29, 2011]

[14]*W. Gunter, G. Higgins &R. Gealt* (2010) *Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents*, International Journalof Cyber criminology Vol 4 Iss. 1and2, pp 657–671 [Online] available from<http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/> [September 14, 2005] .

Hacking is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access.[15]

- Intentional Damage**:** The enterprise's communications networks can be harmed through zapping, the process of damaging or erasing data and information, causing problems for both the enterprise and the customer.[16]
- Spam**:** Email spam could be one of the most prevalent crimes in the sense that almost every email user probably has received at least a few unsolicited commercials.

3.0 Causes of Cybercrime in Nigeria

The root causes of cybercrimes are not far-fetched. One only has to take a quick glance around the society to observe illicit wealth acquisition and its display. This is coupled with the fact that, the perpetrators are highly exalted. The problem is made worse by the high youth unemployment, the absence of enforceable prohibitive laws and the general laissez faire attitude of individuals and businesses regarding cyber security.[17] Evidence has also shown that, a significant proportion of these crimes are perpetrated by people in their youthful age. It is however worth noting that some of these crimes are also perpetrated within organizations. Many internet users are easily lured by unknown mails and website addresses, falling victim to spyware and phishing. Hassan et al. identified urbanization, high unemployment, quest for wealth, poor implementation of cybercrime laws, inadequately equipped law enforcement agencies, and negative role models as some of the causes of proliferated cybercrimes in Nigeria. In a study, the relationships among unemployment, poverty and insecurity in Nigeria was examined. They found that unemployment causes poverty, and that a positive causal relationship exists between the latter and insecurity.[18] Other causes of cybercrime according to them are: corruption, gullibility/greed, proliferation of cyber cafes and the vulnerable nature of the internet.

The main causes of cyber-crimes in Nigeria are briefly discussed below.

(a) **Urbanization:** Rapid urbanization in Nigeria which manifests mainly through the fast population growth is a challenging issue for policy makers. Urban population grows at an annual rate of 4.3% (WDI, 2016). This is much higher than the Sub-Saharan Africa average and continues to put pressure on available resources in Nigerian cities. For instance, only 32.8% of urban population had access to improved sanitation facilities in 2015, and about 68.5% of urban population had access to potable water supply within the period (WDI, 2016). Urbanization is beneficial only to the extent of availability of good jobs that have been created in cities, amidst high population growth rate.[19] The study held that urbanization is one of the major reasons that

[15]*M. Kunz, &P. Wilson,* (2004) "Computer Crime and Computer Fraud", University of Maryland Department of Criminology and Criminal Justice [Online] available from <http://www.montgomerycountymd.gov/content/CJCC/pdf/computer_crime_study.pdf> [March 29, 2011].

[16]*Wienclaw, A. Ruth* (2008) *Internet Security -- Research Starters Business* [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=

[17] B. Hassan, D. Lass & J. Makinde (2012) "Cybercrime in Nigeria: Causes, Effects and the Way Out", ARPN Journal of Science and s, vol. 2(7), 626 –631.

[18]F. Akwara, J. Enwuchola, & M. Adekunle (2013): Unemployment and Poverty: Implications for National Security and Good Governance in Nigeria. International Journal of Public Administration and Management Research (IJPAMR), Vol. 2, no. 1.

[19]E. Meke (2012): Urbanization and Cyber Crime in Nigeria: Causes and consequences.

led to increases in cybercrimes in Nigeria. He also noted that urbanization and crime move in tandem.

(b)**Unemployment:** Unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. Youth unemployment rate is currently above 47%. High unemployment in Nigeria comes with socioeconomic, political and psychological consequences.[20] This phenomenon encourages the development of street youths and urban urchins ("area boys") that grow up in a culture that encourages criminal behavior.

(c)**Poor Implementation of Cybercrime Laws and Inadequately Equipped Law Enforcement Agencies:** African countries have received intense criticism for inadequately handling cybercrimes, this is due to inadequate infrastructure and competence of assigned law enforcement agencies.[21] The private sector also lags behind in protecting itself from cyber savvy criminals, Nigeria inclusive. There is no sophisticated hardware to forensically track down cyber criminals. In some instances, the laws regarding cybercrimes are circumvented by criminals. It is worth noting that law enforcement agencies in Nigeria such as the EFCC and ICPC have successfully prosecuted cybercrime offenders over the years. Nevertheless, much improvement can still be made.

(d)**Corruption:** Nigeria has continued to occupy despicable position in the global ranking for corruption. In 2018, Nigeria was ranked the 144th most corrupt nation in the world out of 176 countries surveyed by the Transparency International.[22] People celebrate wealth without questioning the source of such wealth. It is common to hear of people with questionable character and wealth being celebrated in society. This misguided disposition towards wealth encourages the "get rich quick" mind-set that can be pursued through cybercrime.

(e)**Poverty:** Poverty refers to the inability to afford decent food, shelter, clothing and recreational activities.[23] Hence, poverty is the absence of basic life essentials for survival and comfort of mankind. A poverty-stricken person may unwittingly turn to crime for survival. About 50% of Nigerians live in extreme poverty as at 2018.[24]

4.0 The Effect of Cybercrime on the Growth and Sustainable Development of Nigeria's Economy

Advancement in ICT no doubt brought with it unlimited opportunities (particularly internet and financial software) for banking institutions in Nigeria. It facilitated ease of transactions and reduced cost for both depositors and the banking institutions. However, it also introduced its own peculiar risks through cybercrimes which have negatively impacted the industry and the economy in no small measure. Some researchers identified reduction in competitive edge of organizations, time wastage and slow financial growth, slow production time and increase in overhead cost, as well as defamation of the image of a nation as some effects of cybercrime.

[20]E. Okafor (2011): "Youth Unemployment and Implications for Stability of Democracy in Nigeria", Journal of Sustainable Development in Africa Vol.13, No. 1.
[21]A. Laura (2011): Cyber Crime and National Security: The Role of the Penal and Procedural Law.
[22] See https://www.transparency.org/news/feature/corruption_perceptions_index_2016
[23]A. Jolaosho. (1996): Some Popular Perceptions of Poverty in Nigeria, quoted in UNDP Human Development Report on Nigeria. Lagos: UNDP.
[24] Ibid UNDP

Other major effects include monetary losses and loss of privacy. The threats are enormous to citizens of any nation. Some of the impacts of cybercrime on the Nigerian economy are:

(i) **Reduction in Competitive Edge**: An organization can lose its competitive advantage and suffer losses when a hacker steals its confidential information and future plans and sells it to a competitor. The time spent by IT personnel on rectifying harmful incidents caused by computer criminals could have been used to earn profit for the organization.

(ii) **Productivity Losses and Rising Cost (Inflation)**: Cybercrime also reduces the productivity of an organization, as businesses take measures to prevent it by securing their network. This is time consuming and also affects productivity. In addition, to control viruses and malware, organizations buy security software to reduce the chances of attacks. Computer crime therefore increases overhead cost and reduces profit margins. Other effects include the consumption of computer and network resources, and the cost in human time and attention of deleting unwanted messages.

(iii) **Monetary Losses**: The financial costs to economies and businesses from cyber-attacks include the loss of intellectual property, financial fraud, and damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity etc.) make up a proportion of the reported cost of cyber-attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. Businesses face greater damage from financial fraud and intellectual property theft over the Internet. Thus, where cybercrime is rife (especially relating to businesses and financial institutions) there are bound to be untold financial consequences. According to a research, the cost of cybercrime in six countries (U.S.A, Japan, Germany, U.K, Brazil and Australia) in 2016 ranged from USD$4.3 million to USD$17.3 million annually. The study used a sample of 237 companies in the six countries.[25]

(iv)**Destroys Country's Image**: One key negative effect of cybercrime is that it tarnishes a country's image. Once a country is labelled as a harbor for cybercrime activities, potential investors are cautious in investing in such countries. This has some dire implications for the nation's macroeconomic stability. Cybercrime is no doubt providing a dent on Nigeria's image which remains a crucial source of national embarrassment for the country. The fear of cybercrime has made several persons to avoid the use of ICT. This has a negative impact on the welfare of the citizenry and investors. Confidence in a nation's financial system could be eroded by activities of cyber criminals. Potential investors and tourists are equally scared and the image of citizens is tainted.

(v) **Retards Financial Inclusion:** Proliferation of cybercrime in a particular country discourages financial inclusion, due to the fear of being a victim of cyber-attack. The perceived loss of confidence may also affect the country's developmental progress, as foreign investments find it difficult to flow into the economy. This gives the nation an economic pariah status. The lack of confidence in the banking sector as a result of cybercrime can also be devastating on the economy.

Furthermore, the citizens face reputational risk in today's global economy, a nation cannot afford to have its reputation and that of its financial system tarnished by being associated with

[25]A research study byPonemon Institute (2016)

cybercrime. It becomes a problem for a citizen to engage in meaningful social interaction with the rest of the world when every citizen is perceived as a potential scammer.

5.0 The Legal Framework of Cybercrimes in Nigeria

The Cybercrimes (Prohibition and Prevention) ACT 2015 "provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria". The Act needs to be constantly reviewed to align with the dynamic nature of the cyber environment to accommodate more crimes and address more cyber-related issues that are unique. The Nigeria Data Protection Regulation 2019 is also another regulation that is targeted at protecting both data in motion and at rest. Moreover, there are general laws that deal with financial crimes such as the Nigeria Criminal Code, Economic and Financial Crimes Commission (EFCC) Act 2004, and the Advance Fee Fraud and other Related Offences Act, 2006.

For legislation on cybercrime to be relatively effective and efficient, government needs to empower graduates through employment and the provision of intensive training for law enforcement agencies on ICT to enable them in tracking down cyber criminals.[26]

To reduce cybercrimes in Nigeria, there is the need to create job opportunities for the unemployed youths as well as the need for government, law enforcement, intelligence and security agencies to understand the technology and individuals engaged in the criminal acts in order to be able to curb their activities.[27]

The social impact of cybercrimes is so damming that various tiers of governments have come up with different programmes aimed at re-orientating the youth towards positive thinking.[28] Several initiatives directed at protecting the interests of Nigerians in the cyberspace have been put forward. Agencies, such as the National Information Technology Development Agency (NITDA), Nigerian Communication Commission (NCC), Economic and Financial Crimes Commission (EFCC) have all worked towards curbing the menace of cyber-crime in Nigeria. Other notable cybercrime control initiatives include the setting up of a National Cybercrime Working Group (NCWG) with

Stakeholders drawn from the law enforcement agencies, the financial sector and ICT professionals, and a pilot project of a Computer Emergency Response Team (CERT) center by NCWG and NITDA. Cybercrime can however take place regardless of borders, but legislations and jurisdictions are based on a country-specific framework.

The upgrade of the Nigeria Financial Intelligence Unit (NFIU) to a full-fledged Agency (NFIA) is also a great leap to strengthen the fight against cybercrime in the country. The countries affirm their willingness to cooperate within the existing through the relevant organizations and

[26]F. Okeshola. & A. Adeta (2013): The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions. American International Journal of Contemporary Research. Vol. 3, No. 9, pp 98-113.

[27]*F. Tushabe, & V. Baryamureeba,* (2007), "Implications of Cyber Crime on Social-Economic Development: International Journal of Computing and ICT Research, Vol. 1, No.1, pp. 47 – 57, June 2007.

[28]*J. Jackson & J. Jackson, "Cybercrime and the challenges of socio-economic development in Nigeria" (2016) 14:2 JORIND 42–49.*

institutions to provide assistance, especially capacity development for less inclined nations.[29] Notable amongst the areas of cooperation include:

i. Prevention and recovery from malicious cyber-activities with significant threat to individuals and critical infrastructure, and one that can lead to indiscriminate/systemic harm;

ii. Check activities which substantially result in damages in availability or integrity of the internet for the majority of people;

iii. Strengthen the collective capacity of all members to easily detect and trace any misalignment/ interference by foreign actors, especially as it relates to malicious cyber-attacks of country's electoral processes;

iv. Put measure in place to stall theft of intellectual property garnered in ICT environment and this includes trade secrets and other confidential business information. The aim is to encourage competitive advantages amongst companies or commercial sector;

v. Competence should be enhanced in the areas of preventing the proliferation of malicious ICT tools and practices to stall its damaging effects;

6.0 Necessary Preventive Measures from Cybercrimes

Preventing cyber-criminals activities is not an easy task. Tan (2002, p. 347 in Dion, M. 2010) said that cyber-criminals are often difficult to identify because of jurisdictional challenges[30]. Most times, the country in which they live and/or have their criminal activities does not have strong criminal laws against cyber-criminality. Despite of these challenges, some measures can be taken to account as the way of combating these cyber criminals' activities such as:

(a)User identification & Authentication

User identification typically includes the use of user names and passwords. However, these simple tools can be very easy for a cyber-criminal to break. Passwords can be made harder to break by various techniques including requiring longer character strings, the inclusion of numbers as well as letters, making them case sensitive, and requiring that they be changed at regular intervals (e.g., monthly, annually). Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge.[31] The use of smart cards is expected to increase in the future since it requires both the card and a personal identification number known only to the card holder. Access is impossible without both pieces.

(b)Using network scanning programs: For large to medium enterprises, the proven Virtual Private Network (VPN)technology over WLAN, which is a practical and scalable design can be

[29]C. Chigozie-Okwum, M. Daniel, & S. Ugboaja, "Computer forensics investigation: Implications for improved cybersecurity in Nigeria" (2017) 6:1 International Journal of Science and Technology 59–73.

[30]*D. Michael* (2010) "*Advance Fee Fraud Letters as Machiavellian/NarcissisticNarrative'*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp630–642 [Online] available from <http://www.cybercrimejournal.com/micheldion2010ijcc.pdf/> [September 14, 2011].

[31]*V. Kumaz* (2008) cybercrime prevention, detection [Online] http://www.cidap.gov.in/documents/Cyber%20Crime.pdf available from [February 17,2011].

used for the security. A VPN allows users on a public or un-trusted network, like the internet or WLAN to setup a secure connection to a private network. In a wired or wireless network, the user establishes a secure VPN tunnel to the VPN server when user authorization is successful. Then all the traffic sent through the tunnel is encrypted.[32]

(c)Using open source for security

Another way of preventing cybercrimes is through the use of open source software. Open source enables users to evaluate the security by themselves, or to hire a party of their choice to evaluate the security for them.[33] Open source even enables several different and independent teams of people to evaluate the security of the system, removing the dependence on a single party to decide in favor of or against a certain system.

(d)Special law Protecting Computer Users

The paper has shown that many countries do not have any special Act which has been established to combat computer crime activities. Though many countries have Communications Regulatory Authority (CRA), many of these regulatory authorities do not have any clear Act which protects computer users. For instance in Tanzania, "The Tanzania Communications Regulatory Authority" has come up with the Act known as "The Electronic and Postal Communications Act, 2010" (EPOCA), but it does not consider the protection of ICT users against cybercrimes.

Furthermore, the following are additional information for both stakeholders and Nigerian government if the rate of cybercrimes are actually going to be minimized:

- Insufficient funding for cybercrime law enforcement should be looked into
- Lack of trained cyber experts within law enforcement officials
- Lack of effective international cooperation and data sharing
- Lack of universality of laws against cybercrime
- Statutory minimums in cybercrime cases hamper effective enforcement
- The growing nature of mass unemployment in Nigeria is worrisome.

Conclusion

The issue of cybercrime and its antagonistic impact on the Nigerian economy is alarming and has increasingly become disheartening. To this extent, the government must become proactive and focused in the continuous fight to curb the menace and mitigate its effect on the citizenry.

For Nigeria to serve as a fertile ground for economic breakthrough, it must be built in a crime free society. But an ideal economy is virtually impossible. As technology upsurges, so also is

[32]Issac, Biji& Mohammed (2007) War Driving and WLAN Security Issues Attacks, Security Design and Remedies: The Journal of *Information Systems Management*, Vol. 24 Issue 4, p289-298, 10p, [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=7andhid=105andsid=d9b6cd7d-57dd-42f8-89f2-dcf2f83440ea%40sessionmgr110>[April 30, 2011].

[33]*Hoepman, Jaap-Henk& Jacobs (2007), "Increased security through open Source Communications of the ACM"*, (Jan2007), Vol. 50 Issue 1, p79-83, 5p [Online]available from?sid<http://web.ebscohost.com/ehost/pdfviewer /pdfviewer =7a28b26e-60d2-4ee8-a9ff-d0f7f9f6cdef%40sessionmgr104andvid=1andhid =105>[April 30, 2011].

cyber-crime rate on the rise. Cyber criminals will always keep at pace with any technological advancement. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications.

Nigeria's economy needs major private sector investments in almost all facets of the economy that can industrialize it as a whole. Therefore, Nigeria's foreign investment policies should gear towards attracting and encouraging inflow of foreign capital investments through stable economic programs. Recent studies published on the evolution of principal cyber threats in the security landscape. They present concerning scenarios, characterized by the constant growth of cybercrimes activities.

Finally, even though the level of awareness of cyber threats has increased, and law enforcement acts globally to combat them, illegal profits have reached amazing figures. The impact to society has become unsustainable, considering the global economic crisis. It's necessary to work together to avoid the costs the global community suffers, which we can no longer sustain. The risk of business collapse is concrete, due to the high cost for enterprises in mitigating counter measures, and the damage caused by countless attacks. The problem is to minimize the risks associated by so doing. If there is no technology, hopeful the cybercrimes would not be found anywhere. As it has been discussed in the paper, the preventive measures should be taken to prevent the society as well as the organizations from cybercrimes instead of avoiding the use of technology.

Recommendations

This paper recommends that:

a. Governments and cyber law enforcement organizations should prioritize raising awareness of these cybercrime issues in the near future. Cyber lawyers may advocate for their clients by approaching legislators to explain their position and request laws that benefit them. Cyber lawyers are involved in the continuous debate about what laws should be enacted in this area of law. The weak state of global legal protections against cybercrime suggests three kinds of action.

b. Firms should secure their networked information: Laws to enforce property rights works only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

c. Nigerian Government should ensure that their laws apply to cybercrimes: The Cybercrime (Prohibition and Prevention) Act 2015 remain the dominant authority for regulating criminal behavior in Nigeria. It is crucial that this law should be improved on

to other nations can copy this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals.

d. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security: To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cybercrimes in a similar manner. Those who are caught in cybercrime activities should be punished severely according to the regulations of Cyber security Act 2015 to deter other criminals from future occurrence.

e. Workshops and media advertisements should be regularized quarterly to enlighten the public, organizations, and governmental agencies on the workings of cybercrime and how to adopt measures for protection.

f. A databank for internet users and mobile phones should be created to enable the identification of suspicious calls and transactions in order for criminals to be apprehended immediately upon initiating an attack.