CYBERCRIMES AND THE CHALLENGES OF ECONOMIC DEVELOPMENT IN NIGERIA

Charles Arinze Obiora (Ph.D)
Department of Political Science, Chukwuemeka Odumegwu Ojukwu University
Email: arinzeobiora2002@yahoo.com

James Ebipere Jacob Tiebiri
Department of Business Administration
Niger Delta University, Wilberforce Island, Bayelsa State
Email: jamestiebiri207@gmail.com

Onwunyi Ugochukwu Mmaduabuchi
Department of Political Science, Chukwuemeka Odumegwu Ojukwu University
Email: ugochukwu.onwunyi@gmail.com

Abstract

The effects of cyber crimes on the economic development of any nation cannot be overemphasized. Various crimes are perpetrated by criminals with the use of information and communication technology which Nigeria welcomed with great enthusiasm in order to adapt to changes in the world. Millions of naira is lost on daily basis since the inception of cyber crimes and the economy suffers most, cases of money laundering with the use of internet. Data for this study was gotten from the secondary source where information from the textbooks, internets, journal articles etc, while the Ulrich Beck’s risk society theory was adopted as the tool for analysis. Findings show that the economic situation of Nigeria is adversely affected by cyber crimes. The paper therefore recommends that there is the need for government to provide jobs for the teeming youths so as to take their minds off social vices cyber crimes inclusive that will simply derail the economic development of the nation. Also, laws should be made to ensure strict compliance of government agencies and private organizations that are dependent on the network for its operations in securing their own Network, Information and computer systems promptly.

Keywords: Cybercrimes, Development, Economy, Development, Democracy, Nigeria

Introduction

Antecedent to cyber crime can be traced to a few disgruntled employees causing physical damage to the computers they worked with, with the aim to get back at their superiors. As the ability to have personal computers at home became more accessible and popular, cyber criminals began to focus their efforts on home user. The history of cybercrime was further established with the first published report of cybercrime which occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment, allowed them to access into mainframe computers, and then refers to as computer crime rather than cybercrime. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because availability of Internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime (Guillane and Fortinet, 2009).
In fact, the former descriptions 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 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 (Mbaseki, 2008). According to crime-research.org (2003), the United States was already leading the world in percentage of cyber attacks at 35.4 percent, followed by South Korea at 12.8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cyber crime. As a result, many hackers and other cyber criminals can flourish in countries with few Internet crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as such internet has no geographical demarcation (Guillane and Fortinet, 2009).

In Nigeria, cyber crimes are perform by people of all ages ranging from young to old, but in most instances the young. Several youth engage in cyber crime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many. Mbaseki (2008) holds that secret agents of the UPS (United Parcel Service) smashed a record scam with a face value of $2.1 billion (about N252 billion) in Lagos. The interception was done within three months. Some of the instruments uncovered by the UPS were documents like Wal-Mart Money orders, Bank of America cheques, U.S postal service cheques and American Express traveler’s cheques. This record scam is made possible as a result of the large number of young people who now see Cybercrimes or internet fraud as a source of livelihood (Saulawa and Abubakar, 2014). These have over the years had devastating effects on the economic growth and development of the nation and as such this paper seeks to find the answers to certain questions asked as to extent of problems caused to the economic development of the nation by Cyber crimes and related internet scams that have ravaged the nation and the society in general.

**Conceptual Clarifications**

**Cyber Crime**

Cyber crime is one of the words frequently used by individuals in our contemporary Society. To understand the true meaning of cybercrime, there is the need to understand the slit meaning of cyber and crime. The term “Cyber” is a prefix used to describe an idea as part of the computer and Information age and “Crime” Can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. Cyber crime can simply be explained as crimes carried out with the aid of a computer system. The internet has offered a lot of platform for useful research purposes; However, cyber crime is a worldwide problem that's costing countries billions of dollars (Halder and Jaishankar, 2011). A cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet. Cyber crime has been increasing in complexity and financial costs since corporations, government and individual or society at large started utilizing computers in the course of doing business. As technology increases between governments, corporate organizations and individuals that are involved in international and local businesses; criminals have realized that this is a cost effective method to make money.

Shehu, (2014), posits that cybercrime involves the use of computers and the internet to defraud unsuspecting victims ranging from identity theft, credit card theft (in which victims credit cards or bank account numbers are stolen by computer scanners and used to pay for goods and services) to money laundering by terrorists, and organized crime syndicates. Halder and Jaishankar (2011), views cybercrime as offences committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, by using modern telecommunication networks such as internet (chat rooms, e-mails, notice board and groups) and mobile phones.

This definition limits cybercrime as internet aided illicit activities targeted at individuals and groups. On his part, Kamini (2011), sees cybercrime as crimes committed on the internet or unlawful acts using the computer as either a tool (e.g. 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 (e.g. unauthorized access to computers networks, electronic information theft, denial of service attacks, malware, malicious codes, e-mail bombing, data didling, salami attacks, logic bombs, web jacking, internet time theft, Trojan attacks etc). Cyber crime is a continuum ranging from crime which is almost
entirely technological in nature and crime which is really, at its core, entirely human-related or driven. For example, a fraud carried out via e-mail where the user is directly and simply asked to send money to a particular physical address in return for some service which never materializes. Elementarily, this fraud would work via regular paper mail or telephone. Thus, as argued by Gordon and Ford (2008:12), it is not a technological issue, but a human one, though the perpetrator can use attributes of technology to his advantage.

Economic Development

Development itself is the capacity of a national economy, whose initial economic development has been more or less static for a long time, to generate and sustain an annual increase in its Gross National Product (GNP) at rates perhaps 5% to 7% or more (Tornado and Smith, 2003 cited in Obi and Nwanegbo, 2006). Economic development is therefore the development of economic wealth of countries, regions or communities for the well-being of their inhabitants. From a policy perspective, economic development can be defined as efforts that seek to improve the economic well-being and quality of life for a community by creating and/or retaining jobs and supporting or growing incomes and the tax base (Shalom, 1995). Sen (1999), considers economic development to be the strengthening of autonomy and substantive freedoms, which allow individuals to fully participate in economic life. Hence, economic development occurs when individual agents have the opportunity to develop the capacities that allow them to actively engage and contribute to the economy.

Economic development is measured by rising real per capita income, coefficients and other measures of the distribution of income and wealth as well as indicators of quality of life, that range from life expectancy to crime statistics to environmental quality. From this standpoint, economic development differs from growth in terms of a focus on a broader set of metrics. Schumpeter (1999), sees economic development as a fundamental transformation of an economy. This includes altering the industrial structure, the educational and occupational characteristics of the population, and indeed the entire social and institutional fabric. While growth is measured by putting more people to work within an existing economic framework, economic development is aimed at changing that framework so that people work more productively, and the economy shifts toward higher-value activities. Thus, while economic growth can be measured quarterly, realizing gains in economic development may take decades or generations.

Porter (1998:19-20), holds that, “economic development seeks to achieve long-term sustainable development in a nation’s standard of living, adjusted for purchasing power parity.” The term sustainable, as defined by Economic development is the expansion of capacities that contribute to the advancement of society through the realization of individual, firm and community potential. Economic development is measured by a sustained increase in prosperity and quality of life through innovation, lowered transaction costs, and the utilization of capabilities towards the responsible production and diffusion of goods and services. Economic development requires effective institutions grounded in norms of openness, tolerance for risk, appreciation for diversity, and confidence in the realization of mutual gain for the public and the private sector. Economic development is therefore essential to creating the conditions for economic growth and ensuring our economic future. (Porter,1998).

According to Howell (2007), economic development encompasses the following;

1) Policies that governments undertake to meet broad economic objectives such as price stability, high employment, expanded tax base, and sustainable growth. Such efforts include monetary and fiscal policies, regulation of financial institutions, trade, and tax policies.

2) Policies and programs to provide infrastructure and services such as highways, parks, affordable housing, crime prevention, and educational programs and projects.

3) Policies and programs explicitly directed at job creation and retention through specific efforts in business finance, marketing, neighborhood development, small business start-up and development, business retention and expansion, technology transfer, workforce training and real estate development. This third category is a primary focus of economic development professionals.
Theoretical Nexus

This paper is anchored on the theory of the German Sociologist, Ulrich Beck’s risk society theory. The theory holds that there is a movement away from traditional and industrial society and towards a new modern “risk society” which is individual, global and self-confrontational (reflexive). Beck (1992:21), defines the risk society as “a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself”. The nature of modern societies is such that risks multiply with the increasing “complexities” of societal systems of production, consumption, governance and technological control and as Jonathan, Nick and George (2004), posits that high modernity is characterized by the production and distribution of risks from an increasingly complex techno-scientific system. Similarly, Bell (1998 cited in King and McCarty, 2009), describes risk society as “a society in which the central political conflicts are not class struggles over the distribution of money and resources but instead non-class-based struggles over the distribution of technological risk”. Hence, the risk society is one where every citizen is exposed, to some degree, to technological dangers such as radioactivity, airborne and waterborne pollution, and hazards from mass transportation such as airline, automobile or train crashes, including cybercrimes.

This implies that paradoxically scientific and technological advancement produces new forms unintended risks and does portend severe consequences for society. Beck (1992), rightly demonstrated this when he asserts that in late modern society risk is increasing due to technology and science rather than being abated by technological progress and it is not a world which is less prone to risk, but it is “world risk society” with magnitude of risk so great, that transcends both time and place, by becoming global in scope, the control of risk across is both impossible and meaningless. This is so apt with the advent of the internet revolution and mobile telephony technology which has aided instant messaging, communications, electronic business transactions, banking, and electronic learning anywhere in the world just by the click of a mouse. The globalization process is fast tracked with the information communication technology as hitherto distance and space barriers between countries are no more with the world shrinking into one global community.

Hence, the positive role of the internet technology revolution on the development of the society cannot be overemphasized, however like every other technological innovation it came with it unintended risks which includes cybercrime. The internet hosts billions of computers with billions of people behind those computers and one is unaware of the risk that can occur with a single click of mouse as hacking, fraud and online schemes are some of the risks to which internet users are exposed to. The information society we live in today thus creates unintended risks such as property theft, money laundering, terrorism and so on that are mostly virtual, invisible and most likely irreversible thereby exhibiting a “Risk Society” for individuals, organizations and governments with severe implications for technological and socio-economic development.

Nature, Types and Causes of Cyber Crimes in Nigeria

The usage of the internet is growing daily in Nigeria and as Folashade and Abimbola (2013), suggests this surge is associated with the increasing availability of broadband connections due to the advent of mobile telecommunications and decrease in subscription fee. Recently, most Nigerians and their business are registered on several social networking platforms. The assimilation of the internet into every sphere of our socio-economic lives ranging from electronic banking, electronic commerce, and electronic education to electronic governance has come with it new forms of cybercrimes as cyber technology evolve. Cybercrime activities are prevalent in Nigeria and according to the Daily Trust, (2010 cited in Maitanmi et al 2013; Folashade and Abimbola 2013), by the Internet Crime Complaint Centre, which is a partnership between the Federal Bureau of Investigation (FBI) and America’s National White Collar Crime Centre, revealed that Nigeria is ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9.9%).

According to Ribadu (2007), Nigeria is also ranked first in the African region as the target and origin of malicious cyber activities; and this is spreading across the West African sub-region. Similarly, the American national Fraud Information Centre ranked Nigeria cybercrime impact per capita as being exceptionally high while reporting Nigerian money offers as the fastest online scam, up to 90% in 2001( Saulawa and Abubakar, 2014). The nature of cybercrime in Nigeria is continually evolving with the emergence of new technologies. Kamini (2010), posits that most cybercrimes in Nigeria are tool cybercrimes in nature. This implies that cyber criminals in Nigeria mostly use the computer and internet as a tool to defraud and harm others instead of targeting the computers. He argues that this is so because Nigerians are yet to develop their technical knowledge to accommodate and perpetrate target cybercrimes. Relatedly, Saulawa and Abubakar (2014),
argues that generally cybercrimes in Nigeria are targeted at individuals and not directly to computer systems hence requiring less technical expertise on the part of the criminals.

These kinds of tool cybercrimes prevalent in Nigeria are perpetrated using different kinds of computer and telecommunication tools operational in the country. Ribadu (2007), on his part suggests that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other e-commerce kinds of fraud. Moreso, Olugbodi (2010), identified website cloning, financial fraud also popularly known as Yahoo-Yahoo, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus worms/Trojans. Also, Ibikunle (2005), and Olumoye (2013), suggests that the advent of electronic commerce and electronic banking in Nigeria is accompanied by attended rise in fraud due to the new degree of complexities and vulnerabilities associated with electronic commerce which the fraudsters exploits. Furthermore, Longe et al (2007), and Olumoye (2013), opined aside the conventional financial crimes, that an emerging worrisome dimension in the Nigerian cyberspace is pornography and prostitution aided by technology-induced anonymity on the internet.

Cybercrimes in Nigeria are largely perpetrated by young men popularly called yahoo-boys or yahoo-zee millionaires. Most of these lads are undergraduates of Nigerian universities and young graduates (Folashade and Abimbola, 2013), involved in hacking, cloning and defrauding unsuspecting victims using tools such as password cracker, key loggers, network sniffers, port scanners, vulnerability scanners, exploits and so on. As an underworld criminal activity, cyber criminals in Nigeria plan their executions in some details, as their perpetrations are deliberate with their victim-system or network pre-chosen and identified deliberately and not randomly. Their targets are usually the gullible, greedy, and inexperienced and those desperate for quick money or love and relationships.

There are various types of crimes committed with the use of computer, some of these are;

**Cyber Terrorism**

A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. Parker (1983), defines cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or government bodies using computer and internet is generally referred to as cyber terrorism. Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service (Anah et al, 2012).

**Fraud -Identity Theft**

Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone. For instance, making a false bank webpage to retrieve information of account of someone. The concept is simple; someone gains access to your personal information and uses it for his own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to automated tele-machines (ATM) and using such people can make themselves a lot of money with personal information. In Nigeria people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes (Anah et al, 2012).

**Drug Trafficking Deals**

Another type of cyber crime is drug trafficking; it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to -face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs. ([www.wikipedia.com](http://www.wikipedia.com)).
Malware

Malware refers to viruses, trojans, worms and other software that gets onto your computer without you being aware it’s there. Back in the early part of the century, most such software’s primary aim was thrill. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. In some cases a piece of malware will pretend to be a legitimate piece of software. When such software is downloaded, it infects the computer system and destroys valuable information. The Trojan horse is also a technique for creating an automated form of computer abuse called the “salami attack”, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time.

Cyber Stalking

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking, a term that essentially refers to using the Internet to stalk (to illegally follow and watch somebody), (Justin, 2010). Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. (www.wikipedia.com)

Spam

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site (Saul, 2007). Spammers remain economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer (Gyongyi, 2005).

Logic Bombs

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display “I gotcha” on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it, this is a sure-fire way to get back at the company if he is fired. The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn’t find the employee’s name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes (Anah, Funmi, Makinde., 2012).

Password Sniffing

Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are
programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password as required when using certain common internet services like FTP (which is used to transfer files from one machine to another) or telnet (which lets the user log in remotely to another machine) the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces (e.g., the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994 as many as 100,000 sites were affected by sniffer attacks. (David et al, 1995). There are always immediate and causative effects of most social vices in the society in recent times, the causes of cyber crimes cannot be over emphasized as cyber crimes has been identified as a canker worm that is steadily eating deep into the fabrics of the economy, this is because of the growing need for global trend in virtually all aspects of human existence. The causes of Cyber crimes according to Anah, ; Funmi, ; Makinde, (2012) are;

Urbanization

Urbanization is one of the causes of Cyber crime in Nigeria; it is the massive movement of people from rural settlement to Cites. According to Wikipedia urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for a better life. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called “Yahoo Boys”. Meke (2012), reiterated that urbanization is one of the major causes of cyber crime in Nigeria and that urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, in his article, he emphasized that urbanization without crime is really impossible. As such the elites amongst them find it lucrative to invest in the cyber crime because it is a business that requires less capital (Anah et al, 2012).

Unemployment

Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system. According to the Nigerian National Bureau of Statistics (2016), Nigeria is saddled with almost 20 million unemployed people, with about 2 million new entrants into the dispirited realm of the unemployed each year. This clearly reveals that a lot of youths are not employed. There is an adage that says “an idle mind is the devil’s workshop”, as such most of our youth will use their time and knowledge as a platform for their criminal activity, in order to improve their livelihood and to make ends meet (Anah et al, 2012).

Primitive accumulation

Another cause of cyber crime in Nigeria is quest for wealth, there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most cyber criminals require less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage of that (Anah et al, 2012).

Weak Legal framework:

The Nigerian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they have committed because cyber crimes reduces the nation’s competitive edge, failure to prosecute, cyber criminals, can take advantage of the weak gaps in the existing penal proceedings. Weak /fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as armed robbers are treated with maximum penalties. Unfortunate the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012), states that “African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime’’ Nigeria is not an exception to this rule. Furthermore, it is therefore paramount that the nation’s legislation should ensure proper implementation of their laws against cyber crime Anah, Funmi, Makinde, (2012).
Bad Leadership

Youths are mirrors of the society, but it is quite unfortunate how parents neglect their rightful duties. Meke (2012), remarked that today many parents transmit crime values to their wards, via socialization as if it a socio-cultural values which ought to be transmitted to the younger generation. Imagine a situation where the child supplies the mother with vital information to wreck individual’s banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations most of them will see no wrong in cyber crime practices Anah, Funmi, Makinde, 2012).

Cyber Crime and Challenges of Economic Development in Nigeria

The era of globalization has made the information communication technology (ICT) a sine qua non for any developmental agenda. This is because virtually every aspect of life requires the use of information technology to be able to effectively and favourably remain relevant in a global world. Internet relevance in the development of a nation’s economy has well been established. Ehimen and Bola (2009), argues that the internet has been able create a geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. Owing to the unquantifiable merits and advantages associated with the ear of information and communication technology which is evident in the vast use of the internet, one can easily subscribe to the fact that it is an important tool for national development in a developing country like Nigeria. However, the internet based cybercrime has become a huge menace threatening the socio-economic and technological advancement of Nigeria.

Oni (2013), maintains that in as much as the escalation of cyber crime could not be curtailed adequately by crime prevention agencies, the effects continue to bite hard on our economy, both locally and internationally. Aside from the social menace it is creating in our entire systems to a large extent, cyber crime has thrown up a large number of advanced fee fraud perpetrators in our economic system. Very easily people are able to commit economic crime through the internet by duping one another of large sum of money locally and internationally. Corporate internet fraud has been on the increase as even unscrupulous banking officials are conniving with outsiders to steal depositor’s funds. Aside from local economic sabotage and fraud, a large number of Nigerians particularly the youths are also engaged in perpetrating internet fraud by duping individuals and corporate institutions abroad through spurious economic deals. Fraudulent practices through cyber crime has thrown up emergency millionaires, even billionaires in our economic system which is injurious to our economic growth as most of such funds acquired, illegally are not been used productively to promote the economy. Such funds could not be easily traced by law enforcement agencies. In deed economic sabotage resulting from cyber crime cannot be over-emphasized (Oni, 2013).

More so, cyber crimes reduces the competitive edge of organizations. Computer crimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cyber crime, there has being loss of billions of dollars annually globally speaking, such crimes may threaten a nation’s security and financial health, a company can suffers losses due to computer crime when a hacker steals confidential information and future plans of the company. And he simply sells the information to a competitor company; this will automatically reduce the competitive strength of the company (Anah; Funmi and Makinde, 2012).

Shehu (2014), posits that in the social perspective, cybercrime activities such as cyber stalking, harassment, blackmail and cyber terrorism are a menace to individual’s right to privacy and fundamental freedom. Similarly, cybercrimes like pornography, child predation, online gambling, online prostitution and so on undermines morality in society and puts the society at risks of breakdown of social norms and values. Cyber-crime has thrown up emergency millionaires or billionaires in Nigeria which is injurious to the socio-economic development of the country as most of such funds acquired illegally are not been used productively to promote the economy of the nation. The crime has diverted the attention of so many Nigerian youth from undertaking productive activities such as manufacturing, construction as well as large scale farming that would have grown the economy to such criminal activities because of the flamboyant life chances and life styles that it presents (Folashade and Abimbola, 2013).

The prevalence of cybercrime has also created a bad image for Nigeria amongst the committee of nations as one of the most corrupt nations in the world. This tarnished national image affects the way Nigerians are treated abroad with suspicion and extreme caution as Nigerians are stereotyped to be 419ers (conmen) and hence not to be trusted. Private companies
around the world are beginning to take steps geared towards blocking e-mail originating from the country and financial instrument are accepted with extreme caution. Foreign investors are scared of the country, considering it as risky and unattractive business zone (Honwell, 2007). Cybercrime also has an implication in the socio-economic advancement of the country as information flowing from the country is been characterized as questionable because of the criminal element that make it unreliable, inaccurate and untrustworthy, (Iwarimie-Jaja 2010).

Indeed one cannot overemphasize the economic sabotage resulting from cybercrime in Nigeria. According to Saulawa and Abubakar, (2014), in 2012, an estimated $1 trillion was lost to cyber-related frauds globally although only $390 billion was reported for obvious reasons; and only recently a report by the South African based Institute of Digital Communication indicates that Nigeria is losing about $ 80 million dollars yearly to software piracy alone. Similarly, Sesan, Soremi and Oluwafemi (2012), reports that in 2012 alone, an estimated customer loss of N2, 146,666,345,014.75($13,547,910,034.80) was incurred to cybercrime in Nigeria.

Folashade and Abimbola (2013), while commenting on the dangerous consequences of cyber crime to the economy posits that cybercrime hinders the socio-economic development of the country as it engenders lack of trust and confidence in profitable transactions, promotes denial of innocent Nigerians opportunities abroad and causes loss of employment and revenue loss. Maitanmi et al (2013), found out in a study that cybercrime impedes socio-economic development in Nigeria as it scares away foreign investors due to the low level of confidence it has created for the Nigerian economy. The findings also show that cybercrime has aided other illicit activities in Nigeria such as intellectual plagiarism, disruption of public services, drug trafficking, and terrorism.

i. Widespread cybercrime has tarnished the image of Nigeria in the international community thereby making the country unsafe for foreign investors;
ii. Cybercrime has negatively impacted on confidence Nigerians have on the digital economy thus inhibiting economic growth;
iii. Cyber-attacks against businesses and organizations has the ability to damage organizational reputation and result in a loss of customers and revenue;
iv. The need to develop measures to combat and respond to cyber-attacks imposes significant costs on businesses and organizations;
v. Financial losses accrued by consumers and businesses resulting from the theft of information and money, or extortion impedes economic growth;
vi. Nigeria’s critical infrastructure may be targeted by cyber-attacks and this can lead to immediate and long term economic losses
vii. Cybercrime has the potentials to fuel other criminal activities and increases cost in time and resources for law enforcement agencies.
viii. It can lead to loss of business assets and cost of government agencies and business in re-establishing credits histories, accounts and identities.
ix. Loss of personal financial resources and the subsequent emotional damage (Maitanmi et al, 2013).

Other effects of cyber crime on the economic development of Nigeria according to Anah et al,( 2012), they are;

**Time Wastage and slow financial growth**

Wastage of time is another problem because many information (IT) personals may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information.
**Slows production time and add to overhead cost**

Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercrime, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks.

**Defamation of Image**

With high level of cyber crime in the nation, the image of the generality of Nigerians and everything it stands to represent will be tarnished and global community will perceive Nigeria generally as a corrupt and crime incensed country. Other effects include the consumption of computer and network resources and the cost in human time and attention of dismissing unwanted messages (Anah; Funmi and Makinde, 2012).

**What should be done?**

Cyber crimes cannot be totally wiped out from Nigeria, though it has devastating effect on the economic development of the country. However, if the suggested measures are strictly adhered to, it may help tame cyber crime and thereby enhancing economic development in Nigeria. These are;

1. Laws should be made to ensure strict compliance of government agencies and private organizations that are dependent on the network for its operations in securing their own Network, Information and computer systems promptly.
2. Governments should assure that their laws apply to cyber crimes. African countries are bedeviled by various socio-economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cybercrime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. The government must ensure laws are formulated and strictly adhered to.
3. Individuals should observe simple rules Individuals on their part should ensure proper anti-malware protection on their computer systems, individuals should be encouraged to avoid pirated software, never to share their Personal Identification Number(PIN), bank account, email access code to unknown persons, never disclose any confidential information to anybody as none of these networks were design to be ultimately secure. Ignore any e-mail requiring any financial information. Report particularly evil spam to the appropriate authorities as suggested by Justin (2010). Mbesekei (2008), suggested that telecommunication regulatory agencies should enhance security on internet service providers’ server in other to detect and trace cybercrimes and creation of job opportunities for the teeming unemployed youths will go a long way in minimizing the menace.
4. Government should ensure that there are jobs for the teeming youths so as to take their minds off social vices that will simply derail the economic strength of the nation. It is often said that an idle mind is the devil’s workshop, this therefore means that the provision of employment opportunities will in no small measure distract the youths who may ordinarily wish to engage in cyber crimes and other social vices that will be to the detriment of Nigeria in particular and the society generally.
5. There an urgent need to include entrepreneurship education as well as technical education in the school curriculums so ensure that the youths does not get frustrated in the search of non-existing white collar jobs which the inability to secure one definitely leads to crimes of all sorts which cyber crime is the most prone because of the era of globalization occasioned by the invention of Information and communication technology and the adverse use of mobile phones.
6. Provision of cyber security for all users of internets and a periodic maintenance and upgrade to reduce to its barest minimum the incidences of system hacking and stalling.
7. There is the need for appropriate equipment of the agents and agencies that are charged with the responsibility of fighting cyber crimes and cognizance should be put on the personalities employed for such a purpose to ensure prudence in the discharge of their duties.
References


Justin, P. (2010). “Top five computer crime and how to protect yourself from them”, Publication of Justin plot.


Rights, and Regulations. USA: IGI Global.


