academicJournals

Vol. 6(3), pp. 116-125, March, 2014
DOI: 10.5897/IJSA2013.0510
ISSN 2006- 988x © 2014 Academic Journals
http://www.academicjournals.org/IJSA

International Journal of Sociology and Anthropology

Full Length Research Paper

A socio-technological analysis of cybercrime and cyber security in Nigeria

Odumesi John Olayemi

E-Learning Department, Civil Defence Academy, Abuja, FCT Nigeria.

Accepted 15 January, 2014

The Global Information Infrastructure creates unlimited opportunities for commercial, social and other human activities. However, it is increasingly under attack by cybercriminals; as the number, cost, and sophistication of attacks are increasing at an alarming rate. This study sets out to examine the sociological and technological factors that impact cybercrime and cybersecurity and thereby articulates the relevant circumstances and threats of cybercrime in Nigeria. The study approached the issue of cybercrime from theoretical and investigative points of views. Structured interviews with law enforcement agencies and governmental institution for cyber security were also conducted. Data obtained through these research instruments were subjected to descriptive analysis and frequency counts in order to explain the activities of Nigerian cybercriminals based on existing theories of crime, and to understand their intents, purposes and methods. Four theories of crime, namely, Structural Functionalism Theory, Marxian Theory, Routine Activity Theory and Technology Enabled Crime Theory were all found to be relevant to Nigerian cybercrime. At the level of existing laws, the study established that there are no existing laws in the Nigerian statues that directly address cybercrime.

Key words: Cybercrime, cybersecurity, cyberlaw, Nigeria, Global Information Infrastructure.

INTRODUCTION

The development of the internet and the widened access to computer technology has created new opportunities for work and business activities, as well as those who engage in illegal activities. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activities, but has also resulted in the emergence of what appears to be a new variety of criminal activities. Both the increase in the incidence of criminal activities and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement (Brenner, 2007).

While technological advancements have produced radical shifts in the ability to reproduce, distribute, control, and publish information, the internet in particular has radically changed the economics and ease of reproduction (Longe and Chiemeke, 2008). Computer networks have also radically changed the economics of distribution. With transmission speeds approaching a billion characters per second, networks enable the sending of information products worldwide, cheaply and almost instantaneously.

For Nigeria, a nation in the process of saving her face regarding cybercrimes, efforts are now being directed at the sources and channels through which cybercrimes are perpetuated. The task of re-stigmatizing cybercrime and re-dignifying honest is not as easy as that of institutionalising a deterrence mechanism like code of conduct bureau, Independent Corrupt Practice Commission (ICPC), Economic and financial crime commission

E-mail: olayemijohn@yahoo.com.

(EFCC) and many more. This is after many years at the bottom of the ladder of the corrupt nations of the world, which is based on some index set by the Transparency International (TI), an anti-corruption crusader group.

Problem statement

The internet creates unlimited opportunities for commercial, social and other human activities. But with cybercrime the Internet introduces its own peculiar risks. What are the menace cybercrime and cybersecurity threats poses to Nigeria?

Waziri (2009) spoke about the dreadful level of corruption as being a threat to Vision 20:2020. Cybercrime is an obstacle that may shut the door of progress against the nation. This was why Aluko (2004) gave seventeen (17) ways of stopping financial corruption in Nigeria. One of these crimes according to him has to do with cybercrimes. The global village currently records an increasing criminal behaviour. News of cybercriminal activities continue to fill the pages of the newspaper, it is central to world news and has become a global problem. There is hardly a place where computers and internet facilities are found that cases of crime are not recorded. New modes of operation are developing as the Global System for Mobile-telecommunication (GSM) is now used for browsing. A lot of young people are common among the perpetrators of these criminal activities. They spend hours browsing and sometimes stay awake all night to carry out their nefarious activities. The people involved are mostly found within the ages of fifteen to thirty years.

According to Erhabor (2008), cybercrimes are described as one of the fastest growing criminal activities on the planet. He repeated the fact that it covers a large range of illegal activity including financial scams, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred. In recent time, young students in the tertiary engage in forgery of all kinds ranging from false admission paper to school fees receipts, certificates racketeering and examination malpractice that is, accessing useful information during examinations through the handset and other electronic devices. Ajao (2008) said Nigeria, Ghana and South Africa top cybercrime in Africa. Nigeria is not spared from the heartache caused by cybercrimes.

The findings above are worrisome and it is in order to curb and proffer solution to the above that the study intends to look at the sociological and technological factors influencing cybercrime and cyber security in Nigeria.

Research objectives

The general objective is to provide information and analysis which lawmakers, policy makers and law enforcement agencies in Nigeria can use in order to create legal definitions which are meaningful from sociological and technological perspectives of cybercrime and cybersecurity.

The specific objectives are as follows:

1. To identify informal, sociological and technological causes of cybercrime and cybersecurity in Nigeria.
2. To analyse the approaches adopted by Nigerian law enforcement agencies and cybersecurity stakeholders in combating cybercrime and ensuring cybersecurity.

Research questions

This research study aims to assess the vulnerability of the Nigerian society is to crime and abuse on computer networks and the Global Information Infrastructure at large.

The study then attempts to answer the following questions:

1. How are Nigeria anti-graft agencies tackling cybercrime and cyber security threats?
2. How effective and efficient are the efforts of the security agencies in combating cybercrime and ensuring cybersecurity in Nigeria?
3. What can be done to improve the state of cybercrime and cybersecurity in Nigeria?

METHODOLOGY

A mixed research approach is needed for adequate insight and knowledge into solving and achieving the research problem and objectives. The study will approach the issue of cybercrime from theoretical and investigative points of views. This study will use a combination of existing literature studies, direct in-depth primary research and secondary materials from the Internet. The study population for this study includes: law enforcement agencies and cybersecurity governmental agencies

LITERATURE REVIEW

Cybercrime: Definition and conceptualization

A primarily problem for the analysis of cybercrime is the lack of a consistent and statutory definition for the activities that may constitute cybercrime (PJCACC, 2004; Yar, 2005). According to Smith et al. (2004), defining cybercrime raises conceptual complexities. Varied definitions of cybercrime do exist. In addition to the difficult of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004), Internet crime (Wall, 2001), virtual crime (Lastowka and Hunter, 2004; Grabosky, 2001), e-crime (AIC, 2006) and net crime (Mann and Sutton, 1998). Cybercrime could reasonably include a wide variety of criminal offenses and activities.

At the Tenth United Nations Congress on the Prevention of

Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was divided into two categories and defined thus:

1. Cybercrime in a narrow sense is any illegal behaviour directed by means of electronic operations that targets the security of computers systems and the data processed by them.
2. Cybercrime in a broader sense is 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.

In the Council of Europe's Convention on Cybercrime (2001), cybercrime is used as an umbrella term to refer to an array of criminal activities including offenses against computer data and systems, computer-related offenses, content offenses, and copyright offenses (AIC, 2006). The convention covers cybercrime in four main categories:

1. Offenses against the confidentiality, integrity, and availability of computer data and systems such as illegal access, illegal interception, data or system interference, and illegal devices.
2. Computer related offenses like computer-related forgery and computer-related fraud
3. Content-related offenses (e.g. child pornography).
4. Offenses related to infringements of copyright and related rights.

A working definition along these lines is offered by Thomas and Loader (2000), who conceptualised cybercrime as those "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks". The working definition for cybercrime by the Canadian Police College has increasingly been accepted by Canadian law enforcement agencies; as a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence (Statistics Canada, 2002). Maat (2004), proposed a definition for cybercrime which encompasses all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of computer, computer systems, information network or data. It is significant to note that there is no consistent and statutory definition for cybercrime.

Cybersecurity in Perspective

Cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threat" is rather vague and implies the malicious use of information and communication technology (ICT) either as a target or as a tool by a wide range of malevolent actors. Cybersecurity is often confused with national security while national security, according to the co-ordinator of NCWG, Udotai (2002) in Odumesi (2006) may often be implicated in some cases of cybersecurity. Cybersecurity as a term refers only to security of networks and systems- computers, electronics and ancillary devices. Typical cybersecurity issues, according to Udotai (2002) in Odumesi (2006) include: confidentiality of information; and integrity of systems and survivability of networks (CIS). Major objective of cybersecurity includes: protection of system/networks against unauthorised access and data alteration from within; and defense against intrusion from without. As commonly used, the term "cybersecurity" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and software devices, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associate field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Cybersecurity is thus more than just information security or data security, but is closely related to those two fields, because information security lies at the heart of the matter. Information security refers to all aspects of protecting information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information. Confidentiality" refers to the protection of information from disclosure to unauthenticated parties, while "integrity" refers to the protection of information from unauthorised changes. "Availability" means the information should be available to authorised parties when requested. Sometimes, "accountability" the requirement that the actions of an entity be uniquely traceable to that entity is added to the list.

The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice and particularly in the face of denial-of-service attacks.

The dominance of network topologies has implications for the shape of the protection policies and, subsequently, in determining appropriate protection efforts, goals, strategies, and instruments for problem solution:

1. Cybersecurity as an Information Technology issue: Cybersecurity can be approached as an IT security or information assurance issue, with a strong focus on Internet security. Policies are thus aimed at countering threats to the information infrastructure by technical means such as firewalls, anti-virus software, or intrusion detection software. The main threats perceived range from accident, system failures, bad programming, and human failures to hacker attacks.
2. Cybersecurity as an economic issue: Cybersecurity is relevant to the business continuity, and especially to e- business, which requires permanent access to ICT infrastructures and permanently available business processes to ensure satisfactory business performance. The main actors are representatives of the private sector. The main threats are viruses and worms, human failures, but also hacker attacks of all sorts, and acts of cybercrime.
3. Cybersecurity as a law enforcement issue: Cybersecurity is seen as relevant to cybercrime. Cybercrime is a very broad term with various meanings, and definition can include everything from technology-enabled crimes to crimes committed against individual computers. The main actors are law enforcers. The main threats are acts of computer criminality, but also cyber terrorism.
4. Cybersecurity is a national security issue: Society as a whole and its core values are endangered, due to their dependence on ICT. Action against the threat is aimed at several levels (the technical, legislative, organisational, or international levels). The main actors are security specialists. The main threats are terrorists, but also information warfare threats from other states.

Theoretical framework

According to Khan (1999), theoretical framework of the study is a structure that can hold or support a theory of a research work. It presents the theory which explains why the problem under study exists. Thus, the theoretical framework is but a theory that serves

as a basis for conducting research. A theoretical framework guides your research, determining what things you will measure, and what statistical relationships you will look for.

The researcher will be adopting the following for this study: Structural-Functionalism Theory, Marxian Theory, Routine Activity Theory, and the Theory of Technology-enabled Crime.

Structural Functionalism Theory

The key insight of the structural-functional theory is that crime and deviance is a necessary part of social organisation. It maintained that society is an organism, a system of parts, all of which serve a function together for the overall effectiveness and efficiency of society. Structural-functionalism is a consensus theory which sees society as built upon order, interrelation, and balance among parts as a means of maintaining the smooth functioning of the whole. The theory views shared norms and values as the basis of society, focuses on social order based on tacit agreements between groups and organizations, and views social change as occurring in a slow and orderly fashion.

Writing in the mid-1930s, Merton understood crime and deviance to be a response to the inability to achieve social goals. This is referred to as "anomie theory" of crime, since Merton highlights a tension or strain between:

1. The cultural goals of a society, and
2. The legitimate or institutionalized means to achieve these goals.

The relevance of this theory to this study is that, it provides us insight understanding that crime and deviance is not a matter of a few "bad apples"; it is a necessary condition of "good" social living. The theory maintains that to control crime, the government should enact laws and build institutional frameworks to enforce law, order and cybersecurity in Nigeria.

Marxian Theory

The key insight into the theory is that, crime is a natural outgrowth of capitalism and view society as constantly changing in response to social inequality and social conflict. Capitalism as an economy system is based on the private ownership of property with personal gain rather than collective well-being is encouraged. The theory argued that capitalism is itself a crime and it further causes crime. It is based on oppression and economic exploitation of the majority, and creates a competitive world in which greed, violence and corruption flourish.

Bonger (1916) in Giddens (2001) provided a very early inter-pretation of Marxian ideas on crime and deviance. Bonger shared with Marx himself a belief that, by nature, humanity is altruistic and not competitive. Bonger suggests that capitalism itself, as a form of economic organisation, makes humanity greedy and selfish.

Quinney (1973, 1977) in Giddens (2001), in line with Bonger's argument, argues that under capitalism the law is used to oppress the working class. He suggests that what we now regard as 'criminal' will disappear only once capitalism itself has disappeared. He contends that there will be no greed and profit-seeking under socialism; also, the ruling class will not exist to use the law as a weapon to define as deviant or criminal those working class activities they do not wish to allow.

The Marxian theory is relevant to this study because it provides significant understanding to why people especially unemployed youths engage in crime. Given the level political and economic instability as well as corruption in Nigeria, it is no surprise that cybercrime is rampant. Due to the oppression, exploitation and alienation of the majority for the benefits of the elites; a segment disadvantaged citizens who are in the majority have taken to alternative means to survive. Such alternative means includes prostitution, armed robbery, amongst others. It can be seen that crimes in Nigeria have been influenced by monumental poverty, relative social deprivation, rampant corruption, excessive greed and materialism, amongst others.

Routine Activity Theory

The Routine Activity Theory was proposed by Cohen and Felson 1979 in (Miller, 2006). They contended that for a crime to take place three requirements needed to be present; a motivated offender, a suitable target, and absence of capable guardians.

The theory argues that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. Crime does not need hardened offenders, super-predators, convicted felons or wicked people. Crime just needs an opportunity. It states that for a crime to occur, three elements must be present at the same time and in the same space when any crime is committed:

1. A suitable target is available
2. There is the lack of a suitable guardian to prevent the crime from happening
3. A likely and motivated offender is present.

The theory is relevant to this study in the sense that it provides significant understanding to why people engage in cybercrime. Cybercrime has more to do with the effectiveness of indirect guardianship; as such, a motivation for such crime to take place. Also, the Global Information Infrastructure (GII) is open and immoderate, and the mechanisms of the Internet are designed to transfer data, not to examine the data.

The Theory of Technology-Enabled Crime

The key insight into the theory is that, it combines several categories of criminological theories to help society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and difficult forms of crime to prevent, investigate and control. McQuade (1998) reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there is continual competition between the criminals and law enforcement for technological advantage. As criminals do something new and innovative, law enforcement must catch up in order to avert, control, deter, and prevent new forms of crime.

McQuade (2006) argues that, technology-enable crime theory encompasses:

1. Crimes committed directly against computers and computer systems.
2. Activities which fall under this category are often referred to as high tech crime, computer crimes or cybercrimes.
3. The use of technology to commit or facilitate the commission of traditional crimes.
4. Crimes such as fraud, scams, and harassment can be facilitated using technology which brings unique challenges to old crimes.

The theory provides a framework for understanding all forms of criminality and especially those that are evolving with computing and telecommunications technology inventions and innovations. The theory is pertinent for understanding contemporary threats

posed by emerging forms of cybercrime, transnational crime and terrorism networks that defy traditional methods criminal justice and security measures for preventing and controlling crime.

The theory is relevant to this study because it provide us insight understanding of the new tools and techniques use by cyber-criminals; that is, a shift from the simple crime committed using simple tools to complex crime committed using complex tools. It also helps in understanding the new forms of deviance, social abuse or crime committed through innovative use of technology.

Research design

The study is descriptive and survey research method was adopted. The survey research method was adopted because of its usefulness in establishing existing or prevailing conditions of a given point in time (Travers, 1978). It gives valid and reliable information if well designed. Aina (2002) stated that research design consists of two essential processes; research methods and data collection instrument.

According to Travers (1978) a survey research design often focuses on the characteristics of a population. Those include certain phenomena of interest in a population. Its result can be analysed easily for quick action or necessary intervention.

Study sample

The population for this study includes:

1. Two law enforcement agencies
2. One cybersecurity governmental agency

Sampling techniques

This study made use of non-probability sample. The non-probabilistic sampling technique that was used for this study is purposive sampling. This technique was chosen because the researcher is interested in a particular information-rich subset of stakeholders in cyber activities.

Sample size

The following sample sizes were chosen for each category of the research population:

Law Enforcement Agencies

The unit of analysis is organisation hence the data collected from the Head of the organization best represent the organisations, which are the Economic and Financial Crime Commission (EFCC) and the Nigeria Police Force (NPF).

Cybersecurity Governmental Agency

The unit of analysis is organisation hence the data collected from the Head of the organisation represent the information needed from the organisation, which is National Information Technology Development Agency (NITDA).

Data collection and data collection methods

Law Enforcement Agencies and Governmental Cybersecurity Agency

The following questions were asked during the interview section the EFCC, NPF, and NITDA in order to understand the approaches adopted by Nigerian law enforcement agencies and cybersecurity stakeholders in combating cybercrime and ensuring cybersecurity:

1. How do Nigerian law enforcement agencies identify cybercrime activities?
2. How do Nigerian law enforcement agencies get evidences to ensure conviction?
3. What legal provisions or instruments are available in the Nigeria Criminal Law to address cybercrime?
4. How does your organisation ensure cybersecurity?
5. What challenges have your organization encountered in its efforts to combat cybercrime
6. Do you perceive positive result against cybercrime?
7. Are there any recent cybercrime cases in Nigeria, which demonstrates the importance of having laws against cybercrime?
8. What is your perception of the general awareness about cybercrime and cybersecurity in Nigeria?

PRESENTATION OF RESULTS

Interview with Law Enforcement Agencies

Based on the data collected, we discovered that the Economic and Financial Crime Commission (EFCC) as well as the Nigerian Police Force (NPF) become aware of cybercrime activities through complaints and reports by victims of cybercrime, online surveillance, and frequent assessment of cybercafés. They generally get evidences to ensure conviction through forensic analysis of suspects' computer systems and devices used to perpetuate the crime. Apart from these means, oral testimony of victims, mails exchanged between the suspects and the victims and Internet Protocol address results from Internet Service Providers (ISPs) are also part of the evidences used to ensure conviction of those who might be guilt.

The Advance Fee Fraud Act of 2006, the Money Laundering Act of 2004 section 12(1) (c) - (d), the Economic and Financial Crime Commission Act of 2005, and the Evidence Act of 1948 are the only available provisions in the Nigeria criminal law that may be used to convict perpetrators of cybercrime. These security agencies ensure cybersecurity through registration of all prospective cyber cafes and through public enlightenment. Some of the challenges encountered in the course of their duties of ensuring cybersecurity include: lack of adequate provisions for cybercrime in the criminal code, non-registration of SIM cards and Internet modems, non-cooperation of Internet Service Providers (ISPs) and telecoms service providers, insufficiently trained personnel and inadequate number of trained personnel as well as lack of opportunities for regular training. Also of

relevance is the inadequate knowledge of cybercrime issues and technicalities by Nigerian Judges, and the duplication of duties and responsibilities among law enforcement agencies toward cybercrime activities.

The Economic and Financial Crime Commission (EFCC) reports positive results in the fight against cybercrime due to regular raids of public Internet café, arrests and prosecution of suspects; the Nigerian Police Force (NPF) did not report positive results and they attribute this ineffectiveness to lack of adequate Information Technology skills, lack of adequate funding, and lack of necessary motivation to adequately engage cybercriminals.

The most recent cybercrime case that demonstrates the importance of having a cybercrime law is the case of Akeem Adejumo VS the National Aeronautic and Space Agency of the United States. The law enforcement agencies perceive a low level of general awareness of cybercrime and cybersecurity among the Internet-using Nigerian public and they attribute this to the low penetration of Internet access, mass illiteracy, and the inability on Internet users to take precautionary measures.

Interview with Governmental Cybersecurity Agency

The National Information Technology Development Agency (NITDA) suggests that the major problem towards identifying cybercrime activities is Section 14 of the Nigerian Constitution, which states that "no person shall be punished for a crime unless such crime is prohibited by written law and specific penalties are provided for the violation". As such; there is no cybercrime in Nigeria because there is no written law prohibiting any activities on the Internet. The agency reports that, the law enforcement agencies get evidences to ensure conviction through any other means apart from electronic evidence because there are no legal provisions or instruments available in the Nigerian Criminal Law that address cybercrime directly.

The agency contributes to efforts towards cybersecurity through capacity building workshops on cybercrime, public enlightenment programme, and interactive session with the Bankers' Committee and law enforcement agencies. They also sponsored the cybercrime bill, worked with the Law Reform Commission in updating the evidence act, and partners with private sector in setting network security rules. Some of the challenges they face in the course of their duties include the fact that they are not a law enforcement agency. They also have the challenge that the general awareness of the general populace, the law enforcement agencies and policy makers towards cybercrime is rather low. For instance, Nigeria banks will not provide information to law enforcement agencies on cyber-security threats they receive. Also, organisations lack institutional memory, as people who might have acquired cybercrime training are sometimes placed in positions where the knowledge they have acquired may not be useful to the organisation. Another challenge is the inadequacy of funding which makes it difficult for them to set up a forensic laboratory, equip and train personnel.

The agency recognises the modest successes of the various law enforcement agencies but remarks that the Nigerian government often react based on the exigencies at the time. For instance, when corruption became a major issue, ICPC was set up; when hard drug became an issue, we set up NDLEA; when fake drugs became an issue, we set up NAFDAC; etc.

The agency reports that, there are several cases of attempt to tender electronic evidences but they are not acceptable at the law courts. A typical example is the celebrated case of Femi Fani-Kayode, where the court rejected the printout statement of account because the Evidence Act says you have to produce ledger and right now no banks uses ledger anymore. The perception of the agency on the general awareness of cybercrime and cybersecurity in Nigeria is that, most people link them with only "Yahoo Yahoo Boys"; whereas there are other equally fundamental dimensions of the problem.

DISCUSSION OF FINDINGS

Approaches Adopted By Law Enforcement Agencies to Combat Cybercrime in Nigeria

The available enabling criminal laws used by the law enforcement agencies which are the Advance Fee Fraud Act of 2006, the Money Laundering Act of 2004 section 12(1) (c) - (d), the Economic and Financial Crime Commission Act of 2005, and the Evidence Act of 1948; are not sufficient enough to address the menace of cybercrime directly. As such, an appropriate cyberlaw is required urgently to tackle the activities of cybercrime and ensure cybersecurity.

Aside from legislation, adequate resources must be provided to law enforcement agencies so that they can acquire the tools, equipment, and know-how necessary for the successful defense of network systems from cyber-attacks. Laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary to even operate a computer. Judges must be well trained as well.

Approaches adopted by governmental cybersecurity agency in ensuring cybersecurity in Nigeria

The government cybersecurity agency ensures cybersecurity through capacity building, workshops on cyber-

crime, public enlightenment programme, interactive session with the Bankers' Committee and law enforcement agencies, sponsored the cybercrime bill, working with the Law Reform Commission in updating the evidence act, and partnering with private sector in setting network security rules. However, these are not sufficient enough; as proactive measures are required to ensure cyber safety on the Internet. A typical example is the deployment of the International Telecommunication Union (ITU) toolkit in ensuring cybersecurity. The International Telecommunication Union (ITU) toolkit is a practical instrument that countries can use for the elaboration of a cybersecurity legal framework and related laws.

In addition, consultation, coordination and cooperation between and among governments and the private sector are important, in order to harmonize as completely as possible measures, practices, and procedures that will be utilized in combating this problem. Harmonization of laws at the international, regional and national levels is necessary to meet the challenges of a worldwide technology and its accompanying problems.

However, the Nigeria law enforcement agencies and cybersecurity governmental agency differ in respect to forensic laboratory. Both the Economic and Financial Crime Commission (EFCC) and the Nigerian Police Force (NPF) claim to get evidences to ensure conviction through forensic analysis of suspects' computer systems and devices used to perpetuate the crime. Whereas, The National Information Technology Development Agency (NITDA) affirmed that, the law enforcement agencies get evidences to ensure conviction through any other means apart from electronic evidence because of the non-availability of forensic laboratory.

Problems confronting law enforcement agencies and governmental cybersecurity agencies in combating cybercrime in Nigeria

According to Odumesi (2006), the problems hindering the performance of law enforcement agencies in combating cybercrime in Nigeria are as follows:

1. There is no existing law to adequately address challenges of technology with regards to security breaches and online crime. Thus, absence of laws (legislation) to address online criminality makes it impossible to prosecute offenders.
2. The absence of a national Internet gateway for Nigeria had made it difficult to isolate and determine the real criminal activity that could be ascribed to Nigeria on the Internet.
3. Lack of national framework and infrastructure for the protection and management of electronic payment fraud and other cybercrimes. Therefore, no single law enforcement agency in Nigeria can bear the cost of system infrastructure.
4. There is no adequate data on the level and extent of cybercrime damages in the country.
5. The Nigerian law enforcement agencies are not computer literate and lack of computer forensic laboratory within any branch of the Nigerian Police or other law enforcement agencies to investigate and analyse cybercrime related issues.
6. Nigeria law enforcement agencies does not have a centralised government body that collects and publish cybercrime statistical report.

Theories of crime in relation To Nigeria cybercrime

The researcher adopted four theories of crime in order to understand Nigerian cybercrime. The followings are the findings;

1. The structural-functionalism theory maintains that to control crime, government should enact laws and build institutional frameworks to enforce such laws. In relation to Nigeria, government requires the enactment of a cyberlaw to address the dynamic nature of cybercrime and cyber security threats.
2. The Marxian theory takes the position that what are regarded as crime are merely activities against the interest of the elite and that crime will disappear once capitalism itself disappears. Many of the criminals take the position towards cybercrime. They see it as a means of livelihood within a tough economic environment, whose repercussions affect mainly foreigners. Although, Nigeria is not a pure capitalist economy; the theory still provides some insight into the causes of cybercrime and cybersecurity threats in Nigeria based on the disposition of criminals. The study reveals that criminals engage in cybercrime majorly as a result of unemployment, deprivation and a need to aspire to the higher socio-economic statuses of some others they see with no readily visible income generating activities to justify such affluence.
3. The routine activity theory argues that crime will only be committed if a likely offender thinks that a target is suitable and a capable guardian is absent. It is their assessment of a situation that determines whether a crime will take place. In relation to Nigeria, the theory is relevant because cybercrime activities have more to do with the ineffectiveness of indirect guardianship; as such, a motivation for such crime to take place. Also, the Global Information Infrastructure (GII) is open and immoderate, and the mechanisms of the Internet are designed primarily to transfer data, not to examine the data. As such, the obvious lack of cyberlaw and cyber policing in Nigeria will continue to promote the activities of Nigerian cybercriminals.
4. The theory of technology-enabled crime provides a

framework for understanding all forms of criminality and especially those that are evolving with Information Communication Technology (ICT). In relation to Nigeria, the theory provides us insightful understanding of the new tools and techniques used in perpetrating cybercrime activities. With the changes arising from globalisation of business and the emergence of new economies; developments in digitisation of information; the widespread use of broadband services and mobile and wireless technologies; the evolution of electronic payment systems; and changes in the use governments make of technology to allow members of the public to conduct transactions with government agencies. These and other developments create not only benefits but also risks. Therefore, it is no surprise that online Advance Fee Fraud, identity theft, financial/investment scam, phishing, employment scam and amongst others arise as opportunities for illegality within Nigeria Global Information Infrastructure.

Conclusion

Undoubtedly, the liberalization of telecoms and Internet penetration policies of government have yielded unprecedented growth in Information and Communication Technology (ICT), leading to increased dependence on technology for the delivery of basic as well as critical services in Nigeria amongst citizens, businesses and governments. A cybersecurity framework is therefore inevitable to compliment these great strides by government, secure and protect the underlying ICT infrastructures and boost consumers' confidence as well as the general public.

Cybersecurity is a reality that has to be dealt with now as it would determine how we are conceived in a global village. Today's world is in an important evolution such that physical transactions in all spheres of everyday life will be done online from bank transactions to controlling our hybrid power generating plants, and so on. Thus, there is a need for a cyber-activities regulation that safeguards Nigerians within and foreigners interested in investing in Nigeria.

Cybercrime with its complexities has proven difficult to combat due to its nature. Extending the rule of law into the cyberspace is a critical step towards creating a trustworthy environment for people and businesses. Since the provision of such laws to effectively deter cybercrime is still a work in progress, it becomes necessary for individuals, organisations and government to fashion out ways of providing security for their systems and data. To provide this self-protection, individuals, organizations and government should focus on implementing cybersecurity plans addressing people, process and technology issues, more resources should be put in to educate and create awareness on security practices.

Therefore, there is no one measure that will cure the menace of cybercrime and ensure cybersecurity. But it is the combination of measures together with the sincerity and rigour with which they are implemented and administered that will serve to reduce risks most effectively and efficiently. Also, the fight against cybercrime and cybersecurity threats in Nigeria requires not just knowledge of Information Technology but Information Technology intelligence on the part of all citizens.

RECOMMENDATIONS

Based on the findings of this study, cybercrime is definitely a threat to the economy of a nation, peace and security. Therefore, there is need for a holistic approach to combat this crime and ensure cybersecurity in all ramifications. To this end, the researcher suggests the following as mechanisms to combat cybercrime and ensure cybersecurity in Nigeria;

1. First and foremost is to review existing criminal laws and enact Nigeria cyberlaw to address the dynamic nature of cyber security threats.
2. Forensic laboratories should be established with all investigating units of law enforcement agencies.
3. Ensure progressive capacity building programmes for the law enforcement agencies on cybercrime and cybersecurity.
4. There should be a symbiotic relationship between the firms (Most especially, Internet Service Providers), government and civil society to strengthen legal frameworks for cyber-security.
5. Develop a national cyber security technology framework that specifies cyber security requirement controls and baseline for individual network user.
6. Develop, foster and maintain a national culture of security standardise and coordinate cybersecurity awareness and education programme at all levels of education-primary, secondary and tertiary.
7. Finally, it is important to note that cybercrime cannot be divorced from the widespread corruption, harsh economic climate and abject poverty. To fight crime, Nigerian government must attack the cause and attacking the cause in this context comes by the way of good governance, transparent electoral processes and accountability in government all of which translates into food on the table, more good jobs, better schools, a fairer investment climate and ultimately a reduction in the tendency of our citizens to want to go into cybercrime.

In addition to the recommendations of the researcher; Ehimen and Bola (2009) proposed the following recommendations in addressing cybercrime in Nigeria:

1. The government should establish cyber police who are

to be trained specially to handle cybercrimes in Nigeria. The police should have a Central Computer Crime Response Unit to act as an agency to advise the state and other law enforcement agencies to guide and coordinate computer crime investigation.
2. The government should set up National Computer Crime Resource Centre, which should comprise experts and professionals to establish rules, regulations and standards for network security protocols.

Ayofe and Oluwaseyifunmitan (2009) suggested (both in form of security, education and legislation) following the weak nature of global legal protection against cybercrime:

1. Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions; such as the Council of Europe's Convention on Cybercrime.
2. Establishment of a framework for implementation of information assurance in critical sectors of the economy such as public utilities, telecommunications, transport, tourism, financial services, public sector, manufacturing and agriculture and developing a framework for managing information security risks at all levels.
3. Establishment of an institutional framework that will be responsible for the monitoring of the information security situation, dissemination of advisories on latest information security alerts and management of information security risks including the reporting of information security breaches and incidents.
4. Firms should secure their network information. When organization provides security for their networks, it becomes possible to enforce property rights laws and punishment for whoever interferes with their property.
5. Improving awareness and competence in information security and sharing of best practices through the development of a culture of Cybersecurity at all levels.
6. Promote secure e-commerce and e-government services.
7. Safeguarding the privacy rights of individuals when using electronic communications
8. Formalize the coordination and prioritization of cyber security research and development activities; disseminate vulnerability advisories and threat warnings in a timely manner.
9. Implement an evaluation/certification programme for cyber security product and systems.

United Nations (2005) outlined the following recommendations to be considered by countries in fighting cybercrime:

1. A broad, inclusive focus is necessary to address problems of cybercrime, going beyond criminal law, penal procedures and law enforcement. The focus should include requirements for the secure functioning of a cyber-economy optimizing business confidence and individual privacy, as well as strategies to promote and protect the innovation and wealth-creating potential and opportunities of information and computing technologies, including early warning and response mechanisms in case of cyber-attacks. Behind the prevention and prosecution of computer-related crime looms the larger challenge of creating a global culture of cybersecurity, addressing the needs of all societies, including developing countries, with their emerging and still vulnerable information technology structures.
2. International cooperation at all levels should be developed further. Because of its universal character, the United Nations system, with improved internal coordination mechanisms called for by the General Assembly, should have the leading role in intergovernmental activities to ensure the functioning and protection of cyberspace so that it is not abused or exploited by criminals or terrorists. In particular, the United Nations system should be instrumental in advancing global approaches to combating cybercrime and procedures for international cooperation, with a view to averting and mitigating the negative impact of cybercrime on critical infrastructure, sustainable development, and protection of privacy, e-commerce, banking and trade.
3. All States should be encouraged to update their criminal laws as soon as possible, in order to address the particular nature of cybercrime. With respect to traditional forms of crime committed through the use of new technologies, this updating may be done by clarifying or abolishing provisions that are no longer completely adequate, such as statutes unable to address destruction or theft of intangibles, or by creating new provisions for new crimes, such as unauthorized access to computers or computer networks. Such updating should also include procedural laws (for tracing communications, for example) and agreements or arrangements on mutual legal assistance (for rapid preservation of data, for example). In determining the strength of new legislation, States should be encouraged to be inspired by the provisions of the Council of Europe Convention on Cybercrime.
4. Governments, the private sector and non-governmental organizations should work together to bridge the digital divide, to raise public awareness about the risks of cybercrime and introduce appropriate countermeasures and to enhance the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. For this purpose, national judicial administrations and institutions of legal learning should include comprehensive curricula on computer related crime in their teaching schedules.
5. Cybercrime policy should be evidence-based and subject to rigorous evaluation to ensure efficiency and effectiveness. Therefore, concerted and coordinated efforts at the international level should be made to establish funding mechanisms to facilitate practical

research and curb many types of newly emerging cybercrime. It is, however, equally important to ensure that research be internationally coordinated and that research results be made widely available.

Future research

The researcher was unable to gain access to the arrested cybercriminals within the Special Fraud Unit of The Nigeria Police Force (NPF) and the Advance Fee Fraud Unit of Economic and Financial Crime Commission (EFCC), due to the magnitude of their cybercrime offences, which exit a million naira (N1,000,000:00). Therefore, further study will be required in understanding the demographic and sociological characteristics of the cybercriminals.

Lastly, the researcher recommends a further study into the demographic and sociological characteristics of cybercriminals in Nigeria in order to identify the factors that influence their perpetuating in cybercrime activities.

REFERENCES

Aina LO (2002). Research in Information Sciences: An African Perspective. Ibadan: Stirling-Horden. pp.1-31.

Ayofe AN, Oluwaseyifunmitan O (2009). Approach To Solving Cybercrime And Cybersecurity. Int. J. Comput. Sci. Inform. Security Vol. 3, No. 1.

Aluko M (2004). 17 ways of stopping financial corruption in Nigeria. www.comcast.net. April 5, 2010.

Awe J (2004). Nigeria, South Africa, Ghana top Cybercrime in Africa. www.davidajao.com. 25th June 2010.

Brenner S (2007). Law in an Era of Smart Technology, Oxford: Oxford University Press p.374.

Cohen LE, Felson M (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. Am. Sociol. Rev. 44(2):588-605.

Ehimen OR, Bola A (2010). Cybercrime in Nigeria. Bus. Intell. J. 3(1):26.

Erhabor IM (2008). Cybercrime and the Youths (PGDE Thesis), Department of Education, Ambrose Alli University, Ekpoma, Nigeria, p.37.

Giddens A (2001). Sociology. Uk: Blackwell Publishers pp.306-501.

Grabosky PN (2001). Virtual criminality: Old wine in new bottles. Social and Legal Studies 10(2):243-249.

Khan ER (1999). Developing the Theoretical and Conceptual Framework. Retrieved from: http:// journclasses.pbworks.com/f/ theoretical+framewor.ppt.

Lastowka FG, Hunter D (2004). Virtual Crimes. New York Law School Law Rev. 49:293-316.

Longe OB, Chiemeke SC (2008). Cybercrime and criminality in Nigeria – What roles are internet access points in playing? Eur. J. Soc. Sci. 6(4):133-139.

Maat S (2004). Cybercrime: A Comparative Law Analysis (Doctoral thesis), University of South Africa, Pretoria, South Africa p.239.

Mann D, Sutton M (1998). NETCRIME:More Change in the Organization of Thieving. Br. J. Criminol. 38(2):201-229.

McQuade S (1998). Towards a theory of technology enabled crime. Unpublished manuscript. George Mason University, Fairfax, Virginia.

McQuade S (2006). Understanding and Managing Cybercrime, Boston: Allyn & Bacon.

Odumesi JO (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja, Nigeria p.45.

Smith RG, Grabosky P, Urbas G (2004). Cyber Criminals on Trial. Cambridge (UK):Cambridge UP.

Statistics Canada (2002). Canadian Community Health Survey Cycle 1.2: Mental Health and Well-being. 2002.

Thomas D, Loader B (2000). Cybercrime: law enforcement, security and surveillance in the information age. Routledge, London, J. Soc. Policy 30(1):300.

United Nations (2005). UN recommendations on fighting cybercrime. http://www.crime-research.org/news/13.05.2005/1225/ 25th November 2013.

Wall DS (2001). Maintaining order and law on the internet. In: Wall DS (Ed.), Crime and the internet. London: Routledge pp.167-183.

Waziri F (2009). Antigraft campaign: The war, the worries. The Punch, 1st March 2009, p.1.

Yar M (2005). The novelty of cybercrime: An assessment in light of routine activity theory. Eur. J. Criminol. 2(4):407-427.