# AN APPRAISAL OF THE PROSPECTS AND CHALLENGES OF CYBER CRIME INVESTIGATION AND PROSECUTION IN NIGERIA.

**Idris, Jaleelah Fehintola**[1]

**Abstract:**

*Cyber-crime is the term, used to describe the series of criminal activities that occur in cyber space; it embodies the organized crime that undermines cyber security. Cybercrime is any illegal activity that uses a computer as its primary means of operation and for the storage of evidence, unlawful acts perpetrated by using the computer as either a tool or a target or both. With the advancement in information accessibility and use of the internet, it has become imperative to assess and appraise the existing criminal laws for its effectiveness in combating cybercrime. This article aims to focus on the existing legislations on cybercrime in Nigeria, in order to bring out the challenges in enforcement and ways to harmonize these laws in combating cybercrime. It explains the concept of cybercrime, identifies the loopholes in the law, and addresses the challenges of investigating cybercrime. The recommendations that follow are to proffer ways to the effective use of existing legislations in Nigeria to bring incidences of cybercrime to the barest minimum.*

.

## INTRODUCTION

The growth of technology has both facilitated and impeded the investigation of crime, especially those crimes involving the use of computers and telecommunications. This is what is described as cybercrime. On the one hand, computers have made it possible for vast amounts of data to be searched and analyzed quickly and permitted documents and files to be scanned and transmitted across the globe within seconds. On the other hand, the sheer quantity of information creates considerable problems for investigators who sometimes have to examine gigabytes of data and break encryption codes before the material they are interested in can be discovered. [2]

[1] Barr. (Mrs) IDRIS Jaleelah Fehintola LL.B (Ife), PGD, in Development, Law and Social Justice (the Hague, Netherlands), BL(Abuja) LL.M(Ibadan) is a lecturer at the Bola Ajibola College of Law, Crescent University Abeokuta, Ogun State.

[2]Dr. Russell G. Smith 'Investigating Cybercrime: Barriers and Solutions, Association of Certified Fraud Examiners, Pacific Rim Fraud Conference. Sydney. Retrieved from 2003-09-cybercrime.Pdf-reader.

Cybercrime is one area of crime that is fast growing. The rate at which criminals are exploiting the speed, ease and most importantly the anonymity of the Internet to perpetrate a diverse range of criminal activities is alarming. These criminal activities know no borders. The network of cybercriminals consists of criminal organizations working with criminally minded technology professionals. Highly sophisticated, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organizations are turning increasingly to the Internet to facilitate their activities and maximize their takings in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, and sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging and because the Internet offers near-total anonymity, it is difficult to discern the identity, the motives, and the location of an intruder. The global connectivity of the internet makes it much easier for the criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing criminal organization to use more sophisticated techniques to support and develop networks for their activities and thus creating the challenge for investigators and prosecutors.

**Nature of Cybercrime**

The development of the Internet and the proliferation of computer technology have created new opportunities for those who would engage in illegal activities. The rise of technology and online communication has not only produced a dramatic increase in the incidence of crime, it has also resulted in the emergence of what appear to be some new varieties of criminal activities. These phenomenon pose challenges for legal systems, as well as for law enforcement.[3] The growth of information technology has changed the dimension of crimes and categories of criminals who engage in these crimes. The kinds of crimes instigated across the cyberspace are indeed many and varied. Some of the most common would include the following: computer network break ins- these involve hackers breaking into computer systems and networks to steal data or undertake acts of sabotage such as planting viruses, capturing intelligence as a result of software piracy so as to undermine national security.

[3]Brenner Susan W 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law'(2001) Murdoch University Electronic Journal of Law(Mur.UEJL) Vol 8, No2 available at www.austlii.edu.au/au/journals/Mur.UEJL/2001/8.html (ascessed on 26th July 2016)

Cyber-crime refers to criminal activity done using computers and the Internet. Such criminal activities would include vandalisation of, and intrusion into computer networks by dissemination of viruses, hacking, fraud, pervasive pornography, child pornography, pedophile rings, drug trafficking, extortion, copyright infringement, plagiarism, child grooming, cyber terrorism, cyber stalking, cyber squatting and all other computer based variations of known and existing crimes. It also includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts and non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. The most common form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. A very comprehensive definition of cybercrime was given as:

> A criminal activity involving an information technology infrastructure. Activity which includes illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud"[4]

The growth of electronic commerce offers rich picking for criminals who are prepared to undertake fraudulent activities such as identity theft, misrepresented cyberspace business opportunities and franchises, work at home schemes and credit card swindles. Apart from commerce related crimes, the internet is also used for such serious crimes as kidnapping, child pornography and terrorism. A cyber criminal is therefore, any person who knowingly or intentionally and without permission access or caused to be accessed any computer, computer system or network. [5]The Nigeria Cybercrime Act[6] listed cyber offences as follows: offences against critical infrastructures; unlawful access to a computer; system interference; intercepting electronic messages; mails and money transfers; computer related forgery; computer related fraud; theft of electronic devices; unauthorized modification of computer system, network and data; cyber terrorism; identity theft and impersonation; child pornography and related offences, cyberstalking, cybersquatting, racist and xenophobic offences,

---

[4]Laura, A. 'Cyber Crime and National Security: The Role of the Penal and Procedural Law', (1995): Research Fellow, Nigerian Institute of Advanced Legal Studies., Retrieved from on 3rd July 2016http://nials-nigeria.org/pub/lauraani.pdf(ascessed )

[5] India, Information Technology Act 2000, cited in Gupta, S. and Agrawal, B *'Cyber Laws: Law Relating to Information Technology, Hacking, Intellectual Property Rights, Trade Marks, E-Commerce, Computers, Computer Software, Internet and Cybercrimes'* Allahabad India, Premier Publishing Co. (2009)

[6] Cybercrime (Prohibition, Prevention etc.) Act 2015, Part III

manipulation of ATMs/POS terminal, phishing and spamming, spreading of computer virus, electronic cards related frauds. All these offences can be grouped under the following heads:[7]

Cybercrimes against the person are those that directly target the person. Crimes against the person can be sexual and non-sexual. Non-sexual crimes against persons include, inter alia, homicide, identity theft, cyber stalking (includes but not limited to harassing threatening behaviors), blackmail. Sexual crimes against persons include child pornography and pedophilia. Although, homicide, blackmail and threats are not part of the offences listed in the Act, they can be grouped as part of system interference done through hacking. It is taking of life unlawfully, can be committed by hacking into the computer system of a hospital and altering the records establishing the type and dosage of medication a patient is to receive so that the patient actually receives a lethal dose of medication.

Crimes against property such as hacking (includes but not limited to unauthorized modification of computer system, network and data), theft, fraud (includes but not limited to manipulation of ATMs/POS terminal, spamming, credit card frauds like, the fraudulent use of credit cards and accounts, theft of money from actual conversion to transfer of accounts, telecommunication fraud- individuals using cellular phones and then electronically billing charges to other customer), system interference; intercepting electronic messages; mails and money transfers. Hacking is the unauthorized access to computer programs, systems or data. Theft can be actual theft of computer components or using the computer as a tool to steal-theft of intellectual property, pricing data or customer lists; theft of electronic devices etc.

Another category of Cybercrime is that against morality where the computer is used as a tool to commit immorality such as the dissemination of obscene materials, prostitution and pornography (including but not limited to child pornography and pedophillia). Cybercriminals can direct their activities against the state; crime against the state would include acts specifically directed at destroying the viability of the state such as, offences against critical infrastructures( including but not limited to treason and sabotage; acts undertaken to weaken the effectiveness of the state such as, espionage, the internal dissemination of misinformation and propaganda, dissemination of hate mails against a religion or an ethnic group, acts targeting various state infrastructures such as., terrorism directed at transportation systems, economic systems, public utilities, medical systems, etc., and acts taken to undermine the state's fiscal stability such as, counterfeiting)

[7] See note 3 at pg 2. classifying cybercrimes in this way was carried out by Dr. Susan Brenner. There are other forms of classification such as based on content, on victims and on role computer.

Crime against the administration of justice is another area in which the computer can be used as a tool to commit already-established crimes, but at least two new kinds of computer-facilitated activity that can undermine the administration of justice have emerged. Computer technology can be used to obstruct justice in a number of traditional ways: generating false evidence or destroying electronic evidence; altering or deleting court records to erase criminal convictions or charges; threatening law enforcement officers and judges; filing false reports of crimes; and shutting down crime-reporting system. In addition, someone can use it to impersonate a law enforcement officer or public official. All the above mentioned category of crimes are made up of offenses, the general contours of which have been clearly established, which means computer technology will become at most a tool used to commit these crimes. Crimes that target the computer includes the theft of computer parts, unlawful retrieval of information from the computer so as to undermine the proper functioning of that computer or the causing of damage to information contained in the computer.

Hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system. The hacker gains entry by bypassing the security systems like passwords and carry out some activities making slight changes to the web page, complete destruction of the site or stealing of passwords and other personal data or re- routing or denial of service to the original owner. The criminal uses the computer to target his/her victims. Computers are incidental to the commission of cybercrimes because the computer and the internet make it easy for criminals to access and contact their victims.

Destruction of digital information: Logic bombs and computer infections such as viruses and Trojan horses are sent to destroy digital information. Logic bombs are written in order to destroy or worse, to subtly change the contents of an organization's computer system. Computer viruses do not begin acting until signaled to do so.[8] A computer virus is the computer machine codes that copies its code into another executable program called a host when that program is run. When the infected program is run, the infection spread to other files and some viruses can replicate themselves.

**Investigating and Prosecuting Cyber Crime**

The major point of argument in this article is that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offenses and laws for use in prosecuting cybercriminals

[8] The viruses start to act as soon as they are signaled either by opening a file or otherwise. If they are not signaled, a cancelling signal may come within a given period, which will cancel the virus and render it ineffective.

and procedural rules governing evidence gathering and investigation. Because cybercrime is often transnational in character, offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes.[9] Inadequacies in penal and procedural law can create a loop- hole through which cybercriminals can evade culpability. In order to examine the prospects and the challenges in the investigation and prosecution of cybercrimes in Nigeria, this article will focus on The Administration of criminal Justice Act 2015[10] , the Cyber Crime (Prohibition and Prevention etc) Act 2015 [11] and the Evidence Act 2011[12].

**Essential Ingredients of Cybercrime**

It is the general principle of criminal law that a person would not be convicted of a crime unless the prosecution has proved the ingredients of the crime beyond reasonable doubt. The general ingredients of any crime that the prosecution is expected to prove beyond reasonable doubt are that- (1) The defendant has caused or is responsible for the existence of a certain state of affairs that the criminal law forbids. This means that he has actively participated in the causing of an illegal act, which has been described by the relevant laws of the land as a criminal offense. (2) He had a defined state of mind in relation to the causing of the event or the existence of the state of affairs. This means that his state of mind is that which supports the causing of that state of affairs

Thus, by the ingredients stated above, a crime essentially consist of two elements, *actus reus* and *mens rea*. The actus reus is made up generally but not always, of conduct and sometimes its consequences and also the circumstances in which the conduct takes place, or which constitute the state of affairs, in so far as they are relevant. Sometimes a particular state of mind on the part of the victim is required by the definition of the crime.

[9] Brenner Susan W. 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' 2001 Vol 8 *Murdoch University Electronic Journal of Law(Mur.UEJL*) retrieved from www.austlii.edu.au/au/journals/Mur.UEJL/2001/8.html (ascessed on 26th July 2016)

[10] The Administration of Criminal Justice Act (ACJA)was signed into law in May 2015 which purpose as stated in its S.1 is to ensure that the system of administration of criminal justice in Nigeria promotes efficient management of criminal justice institutions, speedy dispensation of justice, protection of society from crime and the protection of the rights and interest of the suspect, the defendant and the victim. It repeals the CPA and the CPC.

[11] Cybercrimes (Prohibition, Prevention etc.)Act 2015 signed into law on 15th May 2015, its purpose as stated in the explanatory memorandum is to provide an effective, unified and comprehensive legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria. This Act also ensures the computer systems and networks, electronic communications data and computer programs intellectual property and privacy rights.

[12] CAP E14 LFN 2004.

If so, that state of mind is a part of the actus reus. The actus reus is essentially the physical act of the defendant which brings the offense into existence. Mens Rea on the other hand, is the defined state of mind which may comprise of a number of different mental attitudes including intention, recklessness and negligence.[13]

In the case of crime in cyberspace which involves the use of the computer, the actus reus is established when (i) a person is trying to make a computer function (ii) trying to access data stored on a computer or from a computer which had access to data stored outside. If the criminal uses the internet to attempt to gain access, signals pass through various computers and, each of these computers is made to perform a function on the instruction, which the person gave to the first computer in the chain. Each such function can be said to constitute actus reus.

The essential ingredient in determining the mens rea in cybercrime on the part of the offender is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized. There must be, on the part of the hacker, intention to secure access, though this intention can be directed at any computer and not a particular computer. Thus, the hacker needs not be aware of which computer exactly he or she was attacking. Further, this intention to secure access also need not be directed at any particular, or particular kind of program or data, it is enough that the hacker intended to secure unauthorized access to programs or data per se. Thus the intention of the criminal to commit the crime in this case will be established where it is shown that: (a) the access to be secured is unauthorized and (b) the criminal knows and is aware of the same at the time he or she tried to secure the access.

The culpability of a defendant in committing an offence will be established where it is shown that the action of bringing the act that constitutes the offence is backed by the requisite intention and state of mind.

**Stages of Execution in Cybercrime.**

Generally, in any penal law, there are four stages for the commission of an offence. These are the intention, preparation, attempt and commission. The intention is the criminal mindset and the determination to commit the offense, preparation is the preliminary steps taken by the offender towards the execution of the offence while the attempt and commission are the first and the last stage of bringing the offence to fruition. Dr. K P C. Ghandi in

[13]C. Gringas, 'The law of the Internet' page 221 cited in Gupta, S. and Agrawal, B *'Cyber Laws: Law Relating to Information Technology, Hacking, Intellectual Property Rights, Trade Marks, E-Commerce, Computers, Computer Software, Internet and Cybercrimes'* Allahabad India, Premier Publishing Co. (2009)

his article "An Introduction to Computer Related Crimes" [14]classified the stages of execution of cybercrime as Planning, execution, concealment and conversion.

A cyber criminal plans over extensive period. For this purpose, the criminal acquires relevant information such as data entry practices, program listing, systems documentation, location of the systems data and other system details in addition to learning the controls on system access and system security procedures. The information acquired at the planning stage will facilitate the next stage of execution. In execution, cybercrimes differs from other crimes in that the presence of the perpetrator is not necessary. The criminal and the scene of crime may be as apart as several countries away. A cybercriminal can execute his/her illegal act in different ways. The use of terminals or communication channels to gain access, modifying application programs or operating system, entering extra or modified transaction to an input file, physical removal of programs or data, accessing controlled information and copying the same and manipulating the action of programs or people are some methods of execution employed by the cybercriminal. The concept of remote offenders comes to play in the execution of cybercrime because an offender, while in one country can execute the offence effectively in another country without been physically present.

After committing the crime, a cybercriminal will take steps to remove all traces of the crime to conceal himself and his act from the law. A cybercriminal can hide his crimes by (1) representing the crime as an error or omission in an otherwise normal run, (2) representing a fraudulent transaction as a normal transaction being executed, (3) modifying an individual account but manipulating the systems totals to reflect normal results, (4) misrepresenting a criminal activity as an error or flaw within a system and (5) performing the illegal act in conjunction with an authorized activity.[15] These acts of concealment which can be so effectively done as to hide the identity of the criminal is one area that poses a great challenge to investigators and prosecutors in cyber offences. The criminal also in a bid to evade the law will convert the proceeds of his crime such as sale or destruction of data acquired without authority.

**Prospects and Challenges**

There are several challenges faced by law enforcement agencies and other stake holders in combating the menace of cybercrime. The challenges are visible at every stage of prosecuting a cyber offender. From the very first stage of investigating the crime, to the identification of the offender, to the arrest and finally to the effective prosecution of the offender, the challenges

[14] See note 10
[15] See note 10

and obstacles are daunting. In Nigeria, the existing penal laws and the procedural laws cannot adequately help in curtailing the problem. Cybercrime Act 2015 is crafted in such a way that it covers extensively the offenses, the punishment for the offenses and the required international cooperation to bring the offenses to light. The Act however falls short in prosecution and cannot adequately assist a prosecutor of cyber offender. Some of the general challenges identified in this case are the inadequacy of penal laws and the lack of cyber-specific procedural law. Procedural laws in existence are those that were crafted to deal with criminal conduct occurring in the real, physical world, not in or by means of the virtual world of cyberspace. Other challenges are the lack of international agreements on cybercrimes, the incompatibility and the often conflicting requirements of local procedural laws of different nations; the difficulty of ascertaining which nation(s) has/have jurisdiction to prosecute a cybercriminal and, once this determination has been made, of asserting jurisdiction over that person; the difficulty of determining how many offenses have been committed, against whom and the damage resulting from those offenses.[16] To some extent, the Cybercrime Act 2015 has taken care of lack of Cybercrime specific Law in the country. Even though the Act is cybercrime specific, it is not adequate in combating cybercrimes effectively in Nigeria. There are several international agreements on Cybercrime, which are crafted as bilateral and multilateral agreements among nations[17]. International agreements like the cybercrime Treaty[18] is vital if the growing threat of global cybercrime is to be curtailed.[19] International conventions however needs to be domesticated and incorporated into local laws for its effective use in local jurisdiction[20]. There are no national borders in cyberspace; therefore, international cooperation is required for effective prosecution of cyber offenders by any nation.

## Jurisdiction

Jurisdiction is vital in any legal prosecution. This Article is primarily (although not exclusively) concerned with crimes that take place across jurisdictional borders, particularly those that involve offenders and victims

[16] See, Philipplines' Laws Complicate Virus Case, USA Today (June 7, 2000), retrieved from http://www.usatoday.com/life/cyber/tech/cth879.htm:

[17] Budapest Convention on Cybercrime 2004. Crafted by the Council of Europe is the first international Treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyrights, computer related fraud, child pornography and violations of network security. its main objective as set out in its preamble is to pursue a common policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Retrieved from www.coe.int>conventions>fulllist , https://en.wikipedia.org./wiki/conventions_on_cybercrime. on 6/8/2016

[18] ibid

[19] Robel, Dan 'International Cybercrime Treaty: looking beyond ratification' SANS Institute 2007. Retrieved from www.sans.org/international_treaty_ratification_175. on 5/8/2016

[20] Constitution of the Federal Republic of Nigeria(CFRN) 1999(As amended)Cap C Laws of the Federation of Nigeria 2004, s 12

(and other parties) located in different countries. This provides a link with the title of "cybercrime" or crime committed in "cyberspace" – which is simply a shorthand expression for the globally networked computers that may be used for criminal purposes. Cyber criminals will often be international Electronic- criminals therefore, the law must guard against the possibility that the criminal might exploit the international nature of their crime to their legal advantage. Where offences are committed in various countries or where the offender and victim are located in different places, questions arise as to which court should deal with the matter. If the offender in question can be charged in the country in which the offender is located then problems of extradition will be avoided, but if the offender must be charged in the country in which the victim is located or where the effect of the conduct occurred, then the offender will need to be extradited to that country.

Another problem of jurisdiction in cases involving cyber offenders is one that is called 'negative international jurisdiction'- that is, cases that are not investigated because they could be prosecuted in one of many countries, but none of these countries want to take action. There is also the reverse problem of too many countries wanting to prosecute a particularly noteworthy case. What one may need to deal with this situation is the creation of an international protocol along the lines of the United Nations protocol on negotiating jurisdiction, setting out how jurisdiction is best determined in these cases. Generally, the rule is that if a country refuses to extradite an offender and if it has power to take action, then it should be obliged to do so. In some jurisdictions in the world,[21] it was stated that before a country can claim domestic jurisdiction in cases of cyber offenders, a significant link must be established with the home country. The question arising from that is, what constitute significant link? A significant link is established where (1) the accused committed the offence while in the home country and (2) any computer containing a program or data to which the accused secured or intended to secure unauthorized access by doing that act was in the home country at the time concerned. Jurisdiction would therefore be established if, at the time of the offence, either the offender or the computer with which he was perpetrating the criminal act was in the home country. The Nigerian Cybercrime Act did not directly provide for such significant link but this can be deduced from its S 50[22]. The major bottleneck that may arise is the exclusivity of jurisdiction

[21] India, Information Technology Act, culled from Gupta, S. and Agrawal, B " Cyber Laws: Law relating to Information Technology, Hacking, Intellectual Property Rights, Trade Marks, E- Commerce, Computers, Computer Software, Internet and Cybercrimes" Allahabad India, Premier Publishing Co, 2009

[22] . Section 50 provides for jurisdiction and international co-operation, stating that the Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to try offences under this Act, if the offence is committed in Nigeria, by a resident or citizen of Nigeria, in a ship or aircraft registered in Nigeria, the victim of the offence is a citizen or resident of Nigeria and if the alleged

on the federal High court-this may lead to over congestion of the court, which will in turn affect speedy dispensation of these cases.

**Investigating Cybercrimes.**

An investigator is required to gather information about the subject of his/her investigation. A person who is required to investigate a criminal act must gather information about the act, determine the validity of such information, identify and locate the offender and provide evidence to support the prosecution of such an offender. In case of physical criminal offences, the methods of investigation employed by law enforcement agencies usually includes visits to scene of crime, following up on information to interrogate suspect and take down the statements of such suspects. In case of cybercrimes, the scene of crime may be non existing as those crimes are perpetrated in cyberspace. To an investigator of cybercrime, the computer is a vital tool. The computer itself may even be defined, as the scene of crime therefore the information on the computer used for the crime is essential. A cybercrime investigation will start by checking computer system documentation, system logs, background and personnel. If a suspect is identified, the investigator will find out the equipment used and the depth of the expertise of such person. The most important thing to know in this is that a person investigating cybercrimes or any criminal act for that matter must do it in such a way that no evidence recovered by the investigation will be thrown out on prosecution- that is, he must follow the relevant rules of evidence on admissibility.On the average, in Nigeria, there is a dearth of expertise to effectively investigate cyber crime. There is also a lack of proper understanding of the internet and the varying technologies at all levels. It is difficult to determine where a crime has been planned and /or committed- investigation will thus be conducted at a much slower speed. It is often difficult to investigate in another country due to language problems, different laws and practice in place, problems of logistics that create practical barriers while conducting investigations across national borders. Often, for example, investigators have to contact people on the other side of the globe at inconvenient times. These problems will result in delaying matters and increasing general cost of investigation. Teleconferences are difficult to arrange at times suitable for all concerned, translating documents can cost considerable sums and again delay investigations. Witnesses from non-English speaking countries may

---

offender is in Nigeria and has not been extradited to another country for prosecution. In addition the Court shall give all matters brought before it by the Council accelerated hearing. Furthermore, subject to the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of all criminal matters brought under this Act shall not be entertained until judgment is delivered. This provision as it isexpects a substantial link to Nigeria.

need the assistance of interpreters, which can also be expensive and slow down investigations. Finally, countries have different priorities in terms of the importance of cybercrime investigations. Therefore, if there is a conflict between countries on priority, this may affect cooperation in identifying suspects.

Another problem that confronts the investigation of cybercrime is the identification of suspects. Occasionally, this can lead to considerable problems when the wrong person is arrested. There is a range of techniques, software programs and websites available on or accessible over the internet, which allow individual users to hide either who or where they are. It is also possible to assume legitimate user identity and behave as if they were they- spoofing[23]. Remailers and remote storage are also methods usually employed. Remailers are computers located about the internet, which allow a user to send mail to another anonymously, by routing their mail via the computer, where the sender's identity is stripped out- usually employed by persons who send racial or hate material. Remote storage is where a user can store their data elsewhere other than their own computer; this way it is easy to set up and store data on a computer in another part of the world.

It is extremely important to ensure that the right mix of staff, both police and civilian, are employed utilizing assistance from all the relevant experts and specialists in the different computer and network disciplines. There is a need for additional skill to access, analyse and draw evidence from the various network that form the internet. There is a need to train investigating officers to understand, trace and find out offenders at the early stage of commission of crime.

**Liability of Internet Service Providers (ISPs)**

The execution of a significant number of cybercrimes in Nigeria is carried out in cyber café. The Cybercrime Act examines this fact as it states that from the commencement of the Act, all cyber café operators must register as a business concern with "Computer Professionals Registration Council" in addition to a business name registration with the Corporate Affairs Commission. The Act also mandates them to maintain a register of users through a sign in register, which they must make available to law enforcement personnel when needed.[24] This provision will make it easy to track perpetrators of online fraud, as the register serves as a database of all persons who have used the internet service provided by the Internet Service Provider in question in any given cyber café. In the same vein, the Act also provides that, a service provider must retain and preserve information on the

[23] Assuming the identity of a legitimate user of a computer system in order to gain access
[24] Section 7(1) (a) (b)

users of service[25]. While this may be seen as taking due diligence, it can also be seen as invading the privacy of users.

The Act further provides that where there is reasonable grounds to believe that the content of an electronic communication is required for criminal investigation or proceeding, a judge has the power to make an order, on the basis of information on oath, permitting a service provider to use technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data/traffic data associated with electronic communication, or communications transmitted by means of a computer system.[26] The provision of section 53 will necessitate the procurement by either the service provider or other competent authorities, such as a law enforcement officer, of a court order prior to legal interception of an electronic communication. Cyber café are bound by the provision of the Act to either, at the request of any law enforcement agency or on its own initiative provide assistance towards; the identification, apprehension, and prosecution of offenders; the identification, tracking and tracing of proceeds of any offence, or any property, equipment, or device used in the commission of any offence; freezing, removal, erasure or cancellation of the services of the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.[27]

**Prosecution of Cybercriminals**

Once an offender is identified and arrested, he can be made to face the consequences of his actions through prosecution. Investigation is important in establishing the guilt or otherwise of a defendant facing trial for cybercrime. Essential rules guiding prosecution of any offender in Nigeria are determined by the procedural law, which is expected to take care of evidence gathering and arrest of offenders. Apart from the challenges posed by the determination of jurisdiction, inadequate procedural laws in Nigeria are also a bottleneck in the prosecution of cybercriminals as there is no cyber specific procedural law in Nigeria. Cybercrime permeates national boundaries such that a single crime can actually involves several countries where procedural laws are quite different. According to a publication[28], in

[25] Section 38
[26] S. 39
[27] S 40 Cyber crime Act.
Brenner Susan W. 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' 2001 Vol 8 *Murdoch University Electronic Journal of Law(Mur.UEJL*) retrieved from www.austlii.edu.au/au/journals/Mur.UEJL/2001/8.html (ascessed on 26th July 2016)

early May of 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. According to one report, the virus, which was designed to disseminate itself and to destroy various kinds of files on a victim's computer, "infected at least 270,000 computers in the first hours" after it was released.[29] The "love bug" forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company, as well as the computer system at the House of Lords.[30]

After security experts determined that the virus had come from the Philippines, investigators from the Philippines and from the United States set about tracking down the person(s) who created and disseminated it. They were frustrated in this effort by the Philippines' lack of computer crime laws. For one thing, it took days for investigators to obtain a warrant to search the home of their primary suspect; local prosecutors had to comb through Philippines statutes to find laws that might apply to the dissemination of the virus, and then had to persuade a judge to issue a search warrant on the basis of one possibility. For another, when a suspect-Onel de Guzman-was eventually apprehended, there were no laws criminalizing what he had done.[31] The Philippines had no statutes making it a crime to break into a computer system, to disseminate a virus or other harmful software or to use a computer in an attempt to commit theft. Lacking the ability to charge de Guzman with precisely what he had done. Cybercrime is not a phenomenon that we can deal with only at the national level; as the "love bug" episode illustrates, with the emergence of cybercrimes we witness the correlate development of "remote offenders," perpetrators who can, while physically located in one country, easily wreak havoc in other nations.[32]International cooperation is required to deal with the cybercrime as a transnational phenomenon, e.g., with the offender who, working from a computer in Country A, embezzles funds from a bank in Country B or steals trade secrets from a corporation in County C. Section 45 of the Cybercrime Act allows for the support of the law in evidence gathering where there is a reasonable suspicion that a cybercrime had been committed, sections 52 and 56 of the same Act allows for the cooperation of Nigeria with relevant foreign authorities in apprehending and prosecution of cybercriminals. The Cybercrime Act of 2015 was

[29] Fast-spreading Virus Hits U.S., Asia, Europe, USAToday (June 7, 2000), retrieved from http://www.usatoday.com/life/cyber/tech/cth837.htm. cited in Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law" Susan W. Brenner Murdoch University Electronic Journal of Law(Mur.UEJL) Vol 8, No 2, June 2001.retrieved from www.austlii.edu.au/au/journals/Mur.UEJL/2001/8.html

[30] Corporate Systems Hard-Hit by Virus, USA Today (June 7, 2000) retrieved from http://www.usatoday.com/life/cyber/tech/cth839.htm.

[31] Philipplines' Laws Complicate Virus Case, USAToday (June 7, 2000), retrieved from http://www.usatoday.com/life/cyber/tech/cth879.htm

[32]Lynn Burke, Love bug Case Dead in Manila, Wired News (August 21, 2000), retrieved from http://www.wired.com/news/print/0,1294,38342,00.html

promulgated to deal with varieties of illegal activities in cyberspace. S 52 states:

> The Attorney--General of the Federation may request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences under this Act and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.
> (2) the joint investigation or cooperation referred to in subsection (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country

Section 53 provides for the procedure in authenticating evidence gathered pursuant to requests made under section 52, it state that:

> 'all such evidence shall be authenticated by either ; certification by a judge, magistrate or notary public of the foreign state; sworn to under oath or affirmation of a witness or sealed with an official or public seal; or if it emanates from a ministry or department of the Government of the foreign state, or from a person administering the government of a foreign territory, protectorate, or colony'.

In prosecuting, the rules of evidence will come into play regarding the admissibility of the evidence gathered by the investigating officer. In Nigeria, the relevant statute as per rules of evidence is the Evidence Act 2011. In Nigeria, the omnibus statute regulating the admissibility of evidence in criminal trials is the Evidence Act, 2011. Considering the virtual and intangible nature of evidence that is likely to emerge in a cybercrime, can we make use of the Evidence Act as it is? The answer is no. Although the Evidence Act gives provision for the admissibility of electronically generated evidence such that evidence received from a computer is admissible. [33]. S. 84(1) states:

> 'in any proceedings a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in sub-section (2) of this section are satisfied in relation to the statement and computer in question'

The conditions referred to in sub-section (1) are provided in s 84(2) as follows:

[33] S 84(1-5) Evidence Act 2011.

'…

*(a) That the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by an individual;*

*(b) That over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information is derived:*

*(c) That throughout the material part of that period the computer was operating properly, if not, that in any respect in which it was not operating properly or was out of operation during that period was not such as to affect the production of the document or the accuracy of its contents; and*

*(d) That the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.'*

The above provision of the Evidence Act does not envisage software and data like the virus that are written for purposes of criminal activities, it does not also envisage information retrieved through hacking and other such criminal activities in cyberspace. It covered only those documents that are produced and stored in the computer in the regular and ordinary usage of that computer, it states ' *…was used regularly to store or process information for the purposes of any activities regularly carried on over that period,…'* we can say that the provision covers criminal proceedings when it says… '*in any proceedings*…'

Subsection 3 of that section further states:

*'Where over a period the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2) ) (a) of this section was regularly performed by computers, whether:(a by a combination of computers operating over that period; or (b) by different computers operating in succession over that period; or (c) by different combinations of computers operating in succession over that period; or (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer shall be construed Accordingly'*

And subsection 4:

*'In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say:(a) identifying the document containing the statement and describing the manner in which it was produced; (b) giving such*

*particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer; (c) dealing with any of the matters to which the conditions mentioned in subsection (2) above relate and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities, as the case may be, shall be evidence of the matter stated in the certificate, and for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.'*

Subsection 3 provides for the inclusion of information over the internet and intranet of a combination of computers while subsection 4 provides for the laying of proper foundation and authentication. However, s. 53 of the Cybercrime Act states on admissibility of evidence as follows:

> (1) 'Any evidence gathered pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign state, if authenticate, shall be prima facie admissible in any proceedings to which this Act applies'.

The provision of S. 53 of the cybercrime Act envisages the transnational nature of cybercrimes. Cybercrime actually consists of a variety of discrete conduct, some of which we can reach under traditional penal law, some of which requires the modification of traditional penal law and some of which does; indeed, require the adoption of new penal laws. Rather than being a new phenomenon, cybercrime is simply the exploitation of a new technology to commit old crimes in new ways and, to engage in a limited variety of "new" types of criminal activity.[34].

**The Administration of Criminal Justice Act (2015)**

The Administration of Criminal Justice Act 2015(ACJA) applies to criminal trials for offences established by an Act of the National Assembly[35] and other offences punishable in the Federal Capital Territory, Abuja, This provision made the ACJA a federal Law. If the ACJA is a federal Law then it applies to offences under the Cybercrime Act 2015. The provision of this law on evidence gathering poses a problem for investigators of cybercrime because it provides only for the authorization to search and seize tangible evidence whereas the prosecution of cybercrimes usually requires collecting and analyzing intangible evidence, this omission

[34] Susan W. Brenner, "Is There Such a Thing as Virtual Crime?", ___ California Criminal Law Review ____ (2001), retrieved from http://boalt.org/CCLR/. On 6/8/16

[35] S.2(1) ACJA

can be a serious problem for investigators and which can in turn affect prosecution of criminals under the Act. ACJA provides for the venue of trial of offences on the basis of jurisdiction that:

> *' An offence shall ordinarily be inquired into and tried by a court within the local limits of whose jurisdiction: (a) the offence was wholly or in part committed, or some act forming part of the offence was done; (b) the consequence of the offence has ensued; (c) an offence was committed by reference to which the offence is denied; or (d) a person against whom, or property in respect of which, the offence was committed is found, having been transported there by the suspect or by a person knowing of the offence.' [36].*

The Act further states that an offence committed at sea or outside the territory of Nigeria, may be tried or inquired into at any place in Nigeria to which the suspect is first brought, or to which he may be taken thereafter[37]. This provision takes care of offences committed outside of the country but it also emphasizes a connection to the country before any court in Nigeria can assume jurisdiction. Therefore the choice of the locus of trial of cybercrimes, going by the combination of this provision of the ACJA and s 50 of the Cybercrime Act is the Federal High court closest to the place where the offence was committed if the offender resides in Nigeria.

The striking feature of crime on the Internet is that somebody with a computer in a jurisdiction where there are no cybercrime laws can get on and wreak havoc around the rest of the world. Therefore, Section 52 of the Cybercrime Act reproduced above allows for international cooperation in evidence gathering which in effect will aid in prosecution. The Act[38] further state that such evidence if authenticated shall be admissible in any proceedings to which the Act relates[39].

The court in the case of *Sanusi v UBA*[40] allows for the accommodation of foreign cases where there is no sufficient provision in the law- this, the court stated is to avoid an injustice. In that case, the court laid it down in matters concerning phantom withdrawals from ATM that even though the provision of the Evidence Act is that the onus of proof is on the claimant[41], the burden can shift to the defendant in a case where all the necessary documents are in the custody of the defendant.[42] The learned trial judge stated as follows;

---

[36] S. 93(1)(a-d)ACJA
[37] S 94 ACJA
[38] Cyber crime Act 2015
[39] S53 of Cybercrime Act.
[40]( 2014) 2 OGLR 156
[41] S131 of Evidence Act 2011
[42] S 133(1), (2); 136(1)(2), 140 and 167 Evidence Act 2011

> ‘ the provision of sections 133(2), 136(1) and (2) and 140 show that the burden thus shifts to the defendant bank who has all the logs, statements, records in its possession or able to procure such documents or record there from the interswitch operators as it is the banks that keep the records including the mode and the ATM point where such money was collected and records and data from its numerous video cameras which will show the identity of the perpetrators of the act…’ [43]

**Recommendations/Conclusion**

The most important issue that is raised in this article is the fact that cybercriminals can exploit gaps in a nation's penal and procedural laws to effectively perpetrate their act and evade prosecution. The permeability of national boundaries resulting from the Internet allows an offender situated in one country to perpetrate crimes in other countries; the remote offender may be able to operate with impunity, especially if the country in which he is located does not have penal laws, which can cover his conduct. This lack of adequate penal laws will prevent the offender's being prosecuted in his own country (assuming he did, in fact, commit offenses there as well), will prevent his being extradited to the countries he has victimized and can hamper law enforcement's ability to investigate and apprehend him.[44] It is therefore recommended as follows:

1. The relevant laws in the country must be made to adequately provide for the investigation and prosecution of cybercriminals. The necessary amendments must be made in the procedural law or a more cyber specific procedural law be enacted to accommodate prosecution of cybercriminals.
2. The nation still needs to explore the advantages of international cooperation by signing and ratifying International Conventions on cybercrime such that it will enhance the effectiveness of the machinery of justice in combating cybercrime. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale. U.S.-China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime.
3. Adequate sensitization and awareness program should be made available to the citizens and law enforcement agencies on the realities of cybercrimes.
4. Security and law enforcement agents should be trained in the effective use of computer surveillance like keyboard monitoring electronic monitoring and line monitoring and other necessary technological expertise to aid them in investigating cybercrime.

[43] Justice Ogunfowora J in the case of *Sanusi v UBA& Anor (2014)2 OGLR 156 at*

[44] Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law” Susan W. Brenner Murdoch University Electronic Journal of Law(Mur.UEJL) Vol 8, No 2, June 2001.retrieved from www.austlii.edu.au/au/journals/Mur.UEJL/2001/8.html

In order to achieve global cyber security and to bring to the barest minimum the incidence of cybercrime, all countries must adopt appropriate and necessary legislation against the utilization of Information and Communication Technology (ICT), for criminal purposes. It will always be a losing battle if security professionals are way behind the cyber criminals in terms of technological knowledge[45]. It is not just about computing skills, but IT Security expertise. Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system. The threat posed by breaches in our cyber-security is advancing faster than we can keep up with it. It is not possible to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This leads us to conclude that we have to attack cyber security breaches as a whole.[46] And to properly combat cybercrimes, we need effective legislations, expertise for investigation and realistic legal procedures for enforcement which infrascture will suggest to current and prospective cybercriminal that Nigeria is not a safe haven for them and their criminal activities.

[46] Dr. Ibikunle Frank and Dr. Eweniyi Odunayo "Approach to Cyber Security in Nigeria: Challenges and Solution" International Journal of Cognitive research in Science, Engineering and Education. Vol 1 No 1 (2013).