7

CYBER CRIME AND NATIONAL SECURITY: THE ROLE OF THE PENAL AND PROCEDURAL LAW

By

Laura Ani*

Abstract

With the advent of the computer age, legislatures have been struggling to redefine the law to fit crimes perpetuated by computer criminals. This crime is amongst the newest and most constantly evolving areas of the law in many jurisdictions. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appears to be some new varieties of criminal activity. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement. This article argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. Further, a comparative and critical review of Jurisdictions such as the USA, UK, India and Nigeria have been analyzed to address if the existing laws in place are adequate to combat cyber crime and consequently if amendments need to be put in place.

Introduction

What is Cybercrime? The History of Definitions

As technology has developed so have also the definitions of computer crimes or cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or the use of computer technology.

---

*. Research Fellow, Nigerian Institute of Advanced Legal Studies, LLB,BL, LLM.

The OECD Recommendations of 1986[1] included a working definition as a basis for the study:

> Computer related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

The Council of Europe Recommendations of 1987[2] adopted a functional approach and computer- related crime was simply described as the offences enumerated and defined in the proposed guidelines or recommendations for national legislators.

In the council of Europe Recommendations of 1995[3] on Criminal Procedural Law, the term *"offences connected with Information Technology"* (IT offences or IT crimes) is used. In this recommendation, IT offences are described as:

> encompassing a criminal offence, in the investigation of which investigating authorities must obtain access to information being possessed or transmitted in computer systems, or electronic data processing systems.

1. Computer Related Criminality: Analysis of Legal Politics in the OECD Area (1986).
2. Recommendations No.R (89) 9, approved by the European Committee of Ministers of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See *http:// cm.coe.int/ta/rec/1989/89r9.htm.*
3. Recommendations No.R (95) 13, approved by the European Committee on Crime Problems (CDPC) at its 44th plenary session May29-June 2, 1995: Concerning problems of criminal procedural law connected with information technology: See *http://www.cm.coe.int/.*

In a communication from the commission of the European Union in 2001 a single definition is once again introduced. In this communication, "computer –related crime is addressed in the broad sense as:

> Any crime that in some way or the other involves the use of information technology.[4]

The Council of Europe Convention on Cyber-crime of 2001[5] defines cybercrime in the Articles 2-10 on substantive criminal law in four different categories: (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer- related offences, (3) content-related offences; (4) offences related to infringements of copyright and related rights. This is a minimum consensus list not excluding extensions in domestic law.

Content-related offences such as copyright infringements, racism, xenophobia, and child pornography may by many observers normally not be understood as cybercrimes. Copyright infringements are based upon civil agreements and contracts and are not traditionally criminal offences in many countries. Copyright infringements will very often be enforced thru civil remedies due to many of the complicated issues. Child pornography has always been a criminal offence in the paper based version.

Cyber crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as

4. The European Parliament, the Economic and Social Committee and the Committee of the Regions, January 26. 2001.*http://www.europa.eu.int.*
5. See *http://www. conventions.coe.int.Treaty.*

the USA. Terrorists are using 512 –bit encryption which is next to impossible to decrypt. An example may be cited as the Osama Bin Laden's 9/11 attack, the LTTE attack on America's army deployment system during the Iraq war.[6] Various kinds of cyber crimes are emerging in the world today, hacking, bombing, diddling, viruses, spoofing and salami attacks are all capable of breaching the security in the information systems of vital installations.

One of the most important purposes in criminal legislation is the prevention of criminal offences, A potential perpetrator must also in cyberspace be given a clear warning with adequate forseability that certain offences are not tolerated, and when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes. These legal tools include an arsenal of well defined cybercrime offences for use in prosecuting cyber criminals and procedural rules governing evidence-gathering investigation. 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.

The Phenomenon of Cybercrime

Cybercrime is today one of the great legal frontiers, as at 2000 to 2010, the internet has expanded at an average rate of

6. See *www.terrorism.about.com*

444.8% on a global level, and currently an estimated 1.96 billion people are "on the Net."[7]

Hart in his work[8] "The concept of Law" has stated 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safe guard them against cyber crime.

Cyber crime is a criminal activity involving the information technology infrastructure, including illegal access, illegal interception (by technical means of non-public transmission of computers data to, from or within a computer system) , data interferences (unauthorised damaging deletion, deterioration, alteration or suppression of computer data), systems interferences (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting etc) forgery (ID theft) and electronic fraud. There is no dissimilarity between conventional crime and cyber crime. However on deep analysis there is an apparent differentiation between the conventional and cyber crime, which is considerable. This lies in the involvement of the medium in cases of cyber crime. The *sine qua non* for cyber crime is that there should be an involvement, at any stage, of the virtual medium.

Business, economic and white collar crimes have transformed rapidly as computers are used to propagate into the activities and environments in which these areas occur. It has also been recorded that cybercrime today is one of the

7. See World Internet Usage and Population Statistics, *http:// www.internetworldstats.com/stats.htm* (June, 2008).
8. Lacey, Nicola: (2007) H.L.A. Hart's Rule of Law; The Limits of Philosophy in historical Perspective. 36. pp 1203-1224. *www.eprints.lse.ac.uk/pdf.*

greatest legal frontier which has stimulated a different form of crime and thus creating a source for new avenues of crime, such as identity theft, embezzlement, bribery, larceny, sabotage, espionage, burglary, conspiracy, extortion, distribution of pornography, violation of privacy, and offences as brutal as attempted murder, kidnapping and man slaughter. Almost all crimes that can be committed in person can now be committed through the use of computers. The reasons for this vulnerability of computers may be categorised as follows:

1. ***Capacity to Store Data in Comparatively Small Space-***
   The computer has a unique characteristic of storing data in a very small space. This affords the removal or derivation of information either through physical or virtual mediums easy.

2. ***Easy to Access-***
   The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewall which can be utilized to get past security systems.

3. ***Complex***
   The computers work on operating systems and those operating systems in turn are composed of millions of codes. The human mind is fallible and it is not possible that there might not be a lapse at any stage.

The cyber criminals take advantage of these lacunas and penetrate into the computer system.

4. *Negligence*

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be negligence, which in turn enables a cyber criminal to gain access and control over the computer system.

5. *Loss of Evidence*

Loss of evidence is very common and obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.[9]

The above listed could be referred to as basic factors and/or problems causing cyber crime but to get a clear picture of the extent of the problem it is necessary to take a pragmatic look at these factors. Some time in May 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. According to one report, the virus infected at least 270,000 computers in the first hours after it was released. This 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, also the Love bug destroyed files and impeded e-mail traffic in more than twenty countries, and some estimated that the virus caused $10 billion in damage.[10]

9. See. *www.justice.gov/criminal/cybercrime.*
10. See: *www.wsws.org ; www.bbc.co.uk.*

Security experts discovered that the virus had originated from the Philippines, investigators from the Philippines and the United States set about tracking down the persons who disseminated the virus. Their efforts were perturbed by the Philippines lack of computer crime laws: investigators had encountered drawbacks in trying to obtain search warrants, 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 s search warrant on the basis of one diminutive possibility. Also when the suspect Onel de Guzman was finally apprehended, there were still obvious lacunas in the law, as there were no laws criminalizing what he had done. 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. These charges were eventually dropped after the department of Justice determined that the "credit card law (did) not apply to computer hacking and that investigators did not present adequate evidence to support the theft charge".[11]

This incident impelled the Philippines to adopt cyber crime law that established fines and prison sentences for those who hacked into computer systems and/or disseminated viruses or other harmful programs, although the new law could not be applied retroactively against the individual suspected of disseminating the "love bug" virus, so the crime went uncharged.[12]

11. Onel de Guzman's thesis was a computer that was designed to steal passwords; the thesis was rejected because it was designed to commit theft).
12. Although the United States and the Philippines have an extradition treaty, Philippine law requires that laws exist in both countries recognizing a given offence.

The love bug clearly identified some of the problems this type of activity poses for law enforcement, i.e:

1. The lack of international agreements on cybercrimes which exacerbates the problems posed by lack/inadequacy of local penal law and the often conflicting requirements of local penal laws;
2. The lack of cybercrime-specific penal laws and/or the inadequacy of penal laws that were crafted to deal with criminal conduct occurring in the real/ physical world and not in or by means of the virtual world of cyberspace;
3. The difficulty of ascertaining which nation(s) has/have jurisdiction to prosecute a cyber criminal and, once this determination has been made, of ascertaining jurisdiction over that person;
4. The difficulty of determining how many offences have been committed, against whom and the damage resulting from those offences.[13]

Cybercrime is a problem that cannot be dealt with only at the national level as the love bug illustrates. We witness the parallel development of remote offenders and perpetrators who can while be physically located in one country can easily wreak irreparable damage in other nations, international cooperation is therefore required to deal with cybercrime as transnational crime. When it comes to dealing with cybercrime, no country is an island, instead, nations must cooperate to deal with the problem of cybercrime by

13. Scores of nations, especially in the developing world, lack laws governing cyberspace crimes and are woefully short on computer- savvy investigators and the technology required to go after sophisticated hackers.

ensuring that cybercriminals cannot exploit gaps and loopholes in procedural laws to evade capture and prosecution.

Countries also have an imperative to review their penal laws to ensure that their citizens are well protected from cybercriminals, as internal prosecutors have been known to fail for lack of applicable law. In the case of *United States v. Baker*[14] the U.S federal courts of appeals upheld dismissal of charges against a defendant who posted descriptions of his raping, torturing and killing of women online because provisions of federal criminal statute did not encompass his actions.

If a country reviews its penal laws and it indicates a lacuna which does not effectively deal with cyber crime, steps should immediately be taken to amend the deficiencies by adopting new cybercrime laws and amending existing laws. It is relevant to mention at this point that countries ignoring this grey area of the law will definitely be less able to compete in the new economy, reason being that cybercrime increasingly breaches national borders and nations perceived as havens run the risk of having their electronic messages blocked by the network.

Inadequacy of Legislation and Resources

The penal sanctions against trespass or breaking and entry cannot hold against an act of hacking into a computer network and unlawfully acquiring data. From sophisticated airline reservations systems, military early warning mechanisms to the ATM and the digital supermarket till, the

14. 1997 Fed. App. 0036P (Sixth Circuit Court of Appeals 1997) see: *www.laws.lp.findlaw.com.*

IT revolution has brought about a vast array of aides and conveniences that have indelibly influenced modern communication, travel, security and commerce. However the massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever present risk of abuse, insidious manipulation and sabotage of computer and computer networks.

This distinct, unitary phenomenon is a new class of anti-social activity that cannot be dealt with through the application of extant laws. Most countries lack appropriate legislation to deal with internet/computer related crimes. The core of this section gives a critical overview of countries that have adopted cybercrime specific penal laws and if such laws are adequate enough to target "high profile" cybercrimes such as virus dissemination, hacking, fraud and theft. Also for countries that lack cyber specific legislation, whether traditional penal laws are adequate to deal with problems posed by computer – generated crime. A comparative review of four jurisdictions; Nigeria, United Kingdom, United States and India would categorically provide a broad analysis of the cyber crime phenomenon and how it has been adequately dealt with in each of these jurisdictions.

The Nigerian Perspective

In Nigeria, the relevant legislations are the Economic and Financial Crimes Commission (establishment) Act[15] which is charged with the responsibility of investigating and prosecuting of all economic and financial crimes. Arguably

15. No 1 2004.

the closest offence is found in s.1 (1) Advance fee fraud Act[16] and other fraud related offences Act 2006 which was enacted to ease the proof of these crimes. The Economic and Financial Crimes Commission is now charged with the responsibility of enforcing the provisions of the 2006 Act. Other major Acts are the Criminal Code as applicable in the South and Penal Code operational in the north.[17]

The critical question is how do you apply the traditional provisions of the criminal code to offences related to cyber crime, for instance the offence of theft or stealing requires that tangible property be taken away with the intention of permanently depriving the victim of it. Applying traditional criminal concepts to acts involving intangible information can only mean that amendments to our criminal statutes are unavoidable. In order to strengthen this point a look at s.484 of the criminal code, s.321 of the penal code and s.348 of the Shari'ah Penal Code Law of Zamfara State[18], which deal with personating reflects the shortcomings of our criminal sanctions to effectively deal with cyber crime.

A cyber criminal can take over another's credit card/ ATM card account or steal his identity to create a new credit account, which is used to attack e-business, the criminal code provides:

> that every inanimate thing whatever which is the property of any person and which is moveable is capable of being stolen. [19]

16. No.18 of 1994.
17. Criminal Code Act, Cap 77, LFN 1990; Penal Code Act Cap 89, LFN 1963.
18. Shari'ah Penal Code Law, 2000.
19. Section 321.

Many Nigerian tourists abroad are reputed to open credit card accounts on line with another's identity, and shelf up thousands of dollars of charges within days of using the stolen identity. The closest definition of this type of offence just described is also contained in the criminal code which provides that:

> Any person who by any false pretence or by means of any other fraud obtains credit for himself or any other person in incurring any debt or liability; or by means of an entry in a debit and credit account between the person giving and the person receiving credit is guilty of an offence.[20]

Occurrences on the internet where people give false credit card details in order to access a merchant store to perpetuate fraud can give rise to some interpretation difficulties. For a fraud to be deemed to have occurred it is necessary that a person must be deceived. Where the machine was deceived to obtain a service no person as such was deceived. S.382 of the criminal code requires:

> that property (being an inanimate object) which is the property of any person, and which is moveable is the thing capable of being stolen.

Where information on a computer is manipulated, this may well be a matter for civil rather than criminal law. The

20. Section 419.

criminal element is perhaps at the stage where the credit card is used to purchase an item on line and the item is ultimately delivered.

Another perceptible problem law officer's face is the disseminating of evidence and admissibility of the materials generated by them. The evidential status and admissibility of a computer and other electronically generated documents such as e-mails and even statements of accounts have raised controversial issues in the law courts. The problem is the proof of its commission, because most of the steps are electronic in nature. Electronic records such as computer network logs, e-mails, word processing files will increasingly and invariably provide the prosecution with important and sometimes essential evidence in criminal cases, but how does the prosecutor analyse, understand and present electronic evidence stored in computers to prove beyond reasonable doubt to the understanding of the court that a crime not known to Nigerian law has indeed been committed.

On procedural laws, particularly the Evidence Act[21] which was enacted in the light of an agragarian and pedestrian society have become grossly inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes. In *Yesufu v. ACB*,[22] the issues as to whether "entries in books of account" as contemplated by the Evidence Act including computer generated statements or printouts became an issue of debate. The Supreme Court only expressed by way of obiter a willingness to interpret the section more literally in view of contemporary business practices and methods when it noted *inter alia:*

21. Evidence Act Cap 112, LFN 1990.
22. (1976) 4.S.C.1.

> the law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of computers. In modern times reproductions or inscriptions or ledgers or other documents by mechanical process are common place and s.37 cannot therefore only apply to books of account so bound and the pages not easily replaced.

The Evidence Act has become grossly inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes. There is a need to reconsider the prohibitive aspects of our laws. The inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most cyber crimes and their conventional network. Ngugi has stated that only a legislative structure that adequately captures emerging ethical notions that delineate minimum rights and liabilities of internet users, can properly lay the juridical foundation for a predisposition to IT driven national development.[23] As Professor Yemi Osibanjo (SAN) observed "one specific problem that have arisen from the use of electronic financial transactions is the manner and procedure for proving the forms of evidence generated by these means or simply proof of such transactions themselves".[24]

The Federal Government strengthened its commitment against cyber crime by approving a Computer Crime

23. M. Ngugi: Legalweek: Law on Cyber Crime Overdue, *www.crime-research.org* 2005.
24. *Law and Practice of Evidence in Nigeria* – Afe Babalola (SAN) pg 243

Prosecution Unit (CCPU) under the supervision of the Public Prosecution Department of the Federal Ministry of Justice; the department will work with agencies such as the EFCC and the telecoms and banking sector. Officers for the unit are to commence immediate training in basic cyber prosecutor's courses and electronic evidence handling amongst others, whilst other modalities for the effective take-off of the CCPU are currently been worked out.

It should be noted that in the absence of a good, interactive and responsive internet presence where offenders and offending websites and ISP's can be reported, this effort will be doomed to fail. There is a need for a site where victims can report all cases of fraud and know that his case will be given attention in a transparent manner.

United Kingdom

In the UK, the English courts concluded that their existing laws did not accommodate nor reflect the changes brought about by computer technology. In *R.V Gold*[25] the defendant was acquitted because there were no laws to prevent unlawful access to a computer, this led to the enactment of the Computer Misuse Act (CMA) 1990. However this Act was soon found to be ineffective in addressing cybercrime, thus the ageing Computer Misuse Act was amended and came into force in England and Wales on the 1st October 2008.

Modifications to the CMA were included in the Police and Justice Act[26] these changes were then themselves amended by the Serious Crime Act[27]. In order to avoid confusion the government decided to apply these changes all at once, through a (delayed) legislative order. Though the

25 . (1998) AC 1063.
26. (Commencement No.9) Order 2008.
27. (Commencement No.3) Order 2008.

Police and Justice Act deals mostly with policing reform, it also contains amendments to the Computer Misuse Act. There were widespread agreements that the UK's existing computer laws were outdated, as a result each of the changes has attracted criticism to a greater or lesser extent. The amendments cover three main provisions.

First the maximum penalty for unauthorised access to a computer system (the least serious of the three hacking offences covered in the original act) has been raised from six months to two years in prison, making the offence serious enough that an extradition request can be filled.[28] Denial of Service Attacks (DOS) previously something of a legal grey area are now clearly criminal with a maximum penalty of up to 10 years in prison.[29] Thirdly the amended Act makes it an offence to distribute hacking tools for criminal purposes.[30] Also the home office has recently announced a proposal to make it harder for child sex- offenders to meet children online.[31]

In the United Kingdom, the jurisdiction of the English court was considered inter *alia* in *R v Smith* (Wallace) No. 4,[32] the court of Appeal had to consider the following facts: the physical presence of the defendant within England, the fact that substantial criminal activities took place in England,

28. Section 35(3) (a)-(c) Police and Justice Act.
29. Section 36(1)-(6) Police and Justice Act.
30. S.37 (1)-(5) Police and Justice Act.
31. This is designed to stop child sex-offenders using social networking websites. Registered child sex offenders will now have to provide their e-mail addresses to the police or face five years in prison. The first UK social networking Guidance has also been published, which provides advice on how to stay safe online.
32. [2004] EWCA Crim 631. It should be noted that s.4 and 5 of the CMA also provide that the UK has jurisdiction to try the offender if the offence is significantly linked to the UK.

and whether or not it was necessary for the "last act" to be committed within its jurisdiction. The court found that the question of whether the English courts have jurisdiction or not depends on where the last act took place, and if it is established that a substantial part of the offence is within the jurisdiction of the United Kingdom then the English courts have jurisdiction to try the offender. The approach in England and Wales that allows prosecution in cases where an element of the offence occurred within the courts jurisdiction has little judicial support. This was relevant to fraud cases but could not be considered for cases of incitement to racial hatred, as part of the Public Order Act 1986

The UK has made praiseworthy efforts in trying to prevent cyber criminals, the amendments demonstrates the UK's tougher position in combating Cybercrime. Also innovative proposals aimed at child sex offences have been introduced by the Home office as well as the advent of the National Hi-tech Crime Unit.[33] This brings the police, the private sector and academics together to combat cyber crime which ultimately ensures the participation of all key parties in the fight against cybercrime.

United States

The National Information Infrastructure Protection Act of 1996 (hereinafter, the NIIPA or 'the 1996 Act') protects individuals against various crimes involving "protected

33. This is lynchpin in the Uk's coordinated response to cyber-crime in partnership with law enforcement, businesses and the IT world. It undertakes national proactive investigations of serious and organised crime using IT. It also provides consultation to local forces and other agencies; liase with government on policy issues and provides 24-hour point of contact.

computers".[34] Both the US Secret Service and the FBI have jurisdiction over offences committed under the NIIPA, the latter through the USA Patriot Act.[35] The Electronic Communications Privacy Act of 1986 (hereinafter the ECPA) is also aimed at non-traditional crimes such as hacking. It prohibits any obtaining, altering or preventing unauthorized access to electronic storage.[36] Major Federal offences include cyber stalking, identity theft, cyber fraud, spamming, making intentional false representations online, identity theft, the use of password sniffers, the decimation and creation of worms as well as the writing of viruses and Trojan horses, website defacements and web-spoofing.[37]

Many states have adopted legislation that targets procedural issues involved in prosecuting cybercrimes. Some have added definitional sections that augment cybercrime-specific statutes and/or general criminal statutes. Others have adopted statutes which set offense levels and penalties for cybercrime, establish time periods for commencing prosecution of cybercrimes and address possible defenses to cybercrime charges. It can be difficult to apply traditional

34. See s 1030 of Title 18 of the NIIPA. This includes a computer involved in interstate commerce or communications or any computer attached to the Internet. Offences include the prohibition of access to information without authorisation or computer hacking. See s 1030(a) regarding the types of offences and definition of electronic storage.
35. See s 1030 (d) of the NIIPA. It should be noted that the *Patriot Act* was introduced on 23 October 2001 to safeguard homeland security after the 9/11 attacks. Both the *Patriot Act* of 2001 and the *Cyber Security Act* of 2002 contain amendments to the NIIPA.
36. The ECPA was enacted to increase government's powers to wiretap so as to include the digital transmission of electronic data.
37. The sale of non-prescriptive drugs, firearms, explosives, cigarettes, alcohol and visas on the Internet is strictly monitored. The *No Electronic Theft Act* regulates copyright offences and copyright management offences, while the *Digital Millennium Copyright Act* addresses piracy.

jurisdictional predicates- such as committing all or part of a crime within a state or "causing harm" to someone in a state.

In the U.S. jurisdiction and applicable law has been determined on a case by case court analysis rather than applying strict written codified rules. The U.S approach has traditionally considered notions of "reasonableness" and "fundamental fairness" to both plaintiffs and defendants; the minimum contacts approach and the real and substantial connection with the forum. The U.S has a plethora of case law that has addressed the issue of jurisdiction in different areas of the regulation of the internet.[38]

As a general rule, a defendant in the US may be sued in the State where he resides, but when the defendant is not a resident of the state in which the suit is brought, a court may hear the case only when the court properly exercises personal jurisdiction over the defendant. However in Civil law jurisdictions, as a general rule, a defendant may be sued only in the state where he resides based on the subject matter and taking into account the rules of residence and domicile usually provided in the Civil Code.

Jurisdictional problems further arise for state prosecutors when causes of action are committed in different states, because the jurisdictional rules of criminal law require the prosecutor to prove that the defendant intended to cause harm within his state. American State courts have not yet seen many challenges to state assertions of extraterritorial

38. See the Internet Library of law and Court Decisions, which contains summaries of several important US cases relating to jurisdiction in Internet law;http://*www.internetlibrary.com/alldecisions.cfm.case33*.

jurisdiction in cases charging cybercrimes.[39] Examination of the noncyber case law and statutes demonstrates, however that state law currently would support an aggressive response to Internet-related unlawful activities that impact a particular state, even where the perpetrator is not physically located within the forum state. For example in Michigan, the enforcement of criminal and civil enforcement actions against on-line distributors of alcohol, prescription drugs, GHB manufacture kits, as well as child pornography and sexual predators has been initiated. The on-line sales of regulated items such as alcohol, drugs, and tobacco present a typical area in which state criminal actions may arise.[40]

The case of *US v. Gorshov*[41] raises controversy about a country's jurisdiction to enforce its law regarding cyberspace cases. The facts were some Russian nationals were identified as hackers who had been breaking into the computer systems of American businesses. They were trapped by FBI agents into coming to an interview in the United States and were subsequently arrested. Information was retrieved from Russian computers by the FBI agents without a warrant. The District court found that there had been no violation of the Fourth Amendment, which did not encompass extra-territorial searches of non-US citizens, nor was there any violation of Russian law. However, the Russian authorities charged the FBI agents with hacking and requested their

39. Most of the reported cases relate to the transmission of child pornography over the internet, or sexual solicitation of children over the internet, but do not directly address jurisdictional issues.
40. See Terrence Berg – State Criminal Jurisdiction in Cyberspace: Is There a Sheriff on the Electronic Frontier? *www.michbar.org/journal/article*.
41. 2001 WL 1024026. The question arose whether the actions of the FBI agents were justified or not as an exercise of enforcement of jurisdiction.

presence for trial in Russia, but the American government did not comply.[42]

Bold attempts are being made in the USA to respond to the increase in cybercrime, such as the Project Safe Childhood to combat child exploitation on the Internet, and the use of specialised prosecutors to fight cyber crimes in the US Attorney's Offices nationwide. Further initiatives have also been launched by the US Electronic Crimes Task Force and the FBI which brings law enforcement officers together with members of the private sector and academics in a collaborative effort against cyber crime. The department of Justice also continues to rely on dedicated attorneys in the Criminal Divisions Computer Crime and Intellectual Property Section.[43] In August 2008 the US Senate passed a Bill on cybercrime to modernize the country's computer crime laws and to provide prosecutors with more leeway in pursuing cyber criminals. Current federal cybercrime laws require prosecutors to demonstrate that the illegal activity caused at least $5,000 in damages before they can institute actions for unauthorized access to a computer. However, that threshold will now be eliminated under the new Bill. The new legislation contains the following amendments: (a) it is a felony to install spyware or Keystroke-monitoring programmes on ten or more computers regardless of the amount of damages caused; (b) the new legislation also enables identity theft victims to seek restitution for the loss of time and money spent restoring their credit; and (c) the Bill would also allow federal courts to prosecute cyber criminals who 'attack' computers located in the state in which they

42. Various questions have been raised as to whether the FBI Agents Acts were justified.
43. See *www.fbi.gov*.

live[44]. Another new provision covers cyber extortion to address shortcomings in the existing law.[45] These new provisions will be added to a bill known as the Former Vice President Protection Act *2008*.[46] The new government under President Barack Obama is also presently reviewing cybercrime regulations.[47]

Further the US introduced a new bill, which if passed will penalize economically foreign countries that choose or fail to put a stop to Cyber criminal activity originating from within their borders. This International Cybercrime Reporting Cooperation Act will make the White House responsible for pinpointing exactly which countries have to tackle the problem of cybercrime and have a "pattern of cybercrime against the U.S Government, private entities or persons". If they fail to act after being appraised of the situation they are looking at cuts in the US assistance and resources - new OPIC or Exlm financing, new multilateral financing, new TDA assistance, preferential trade programs, or new foreign assistance, as long as such do not limit projects to combat cybercrime.

---

44. Current law provides that federal courts have jurisdiction only if a thief uses interstate communication to access the victim's PC.
45. The existing law provides that the government can prosecute cyber extortionists who threaten to delete a victim's data or to damage a computer. There is no specific statute addressing cyber criminals who try to extort companies by publishing or releasing stolen information. However, this activity has now been criminalised. See *blog.washingtonpost-com/*
46. This is a bill to amend the title 18, US Code, to provide secret service protection to former vice presidents and other purposes.
47. During February 2009, President Barack Obama instructed the National Security and Homeland Security Advisors to conduct a review of the plan, programmes and activities dedicated to cyber security including new regulations to combat cybercrime. See *Cybercrime Law 2009 www.cybercrimelaw.net/*

The above discussion demonstrates that the United States is taking the lead in addressing cybercrime. The collaborative initiative involving the police, the private sector and academics is an encouraging attempt to involve all role players in the fight against cybercrime. The advent of the new Bill also illustrates that the US is taking the lead in updating outdated computer laws to keep abreast with advancing computer technology. The ratification of the Council of Europe Cybercrime Convention by the United States has received much needed support in the global fight against cybercrime.

India

The Indian parliament considered it crucial to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information technology Act 2000 was passed and enforced on 17th May, 2000 the preamble of this Act states its objectives to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers Book Evidence Act 1891 and the Reserve Bank of India Act 1934. *The rationale for this is to integrate the changes in these Acts and to make them attuned with the Act of 2000,* in order to regulate and control the affairs of the cyber world in an efficient manner. Aim[48]

The Act provides a legal framework for the security of all electronic records and activities carried out by electronic means. The IT Act 2000 also provides legal recognition of digital signatures and a legal framework for E-governance, offences, penalties, adjudication and investigation of

48. See F. Fahim *www.crime-research.org/articles.*

cybercrime.[49] Though the Act was a welcomed initiative it had its shortcomings, the Act contained ambiguous definitions and has been criticized for not effectively addressing cyber harassment and cyber stalking. Further there was an apparent lack of awareness by citizens about their rights; the questions of jurisdiction as well as extra-territorial jurisdiction were also not addressed in the Act.[50]

Though cybercrime is on the increase it is not adequately reported. One obvious reason is the non-cooperative police force. This was proved by the *Delhi Time Theft* case**.**[51] "The police are a powerful force which can play an instrumental role in preventing cybercrime and at the same time it can also end up harassing innocent citizens and preventing them from going about their normal cyber business. One of the reasons why the Act was not achieving its optimum is the lack of vigilance among the citizens about their rights, thus leading to a plethora of unreported cases. In order to achieve the complete realization of the provisions of this Act a cooperative police force was highly required.[52]

---

49. The Information Technology Act deals with various cyber crimes in chapters IX & XI. The important sections are Ss. 43,65,66,67 & 75. Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with 'hacking and computer system' and provides for imprisonment up to 3 years or fine. Further s. 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with a fine and s.75 provides for extra- territorial operations.
50. *See www.ind.ii.org.*
51. See Cyber crime by Parthasarathi Pati; www.naavi.org.
52. The role of the police in combating cybercrime has been criticised because of the poor rate of conviction. However, the police in India are now

The increase in ATM frauds and cybercrime led to calls to amend the IT Act 2000 and this resulted in the Cybercrime Bill being passed in Parliament in December 2008. It is called the Information Technology (Amendment) Bill.[53] It prescribes punishment which could extend to life imprisonment for cyber terrorism and imprisonment of five years, and a fine of Rs lakh (One hundred thousand rupees) for publishing obscene material or transmitting obscene material in electronic form. A severe punishment is also prescribed for offences relating to the misuse of computers and communication equipment.[54]

As a result of the shortcomings of the IT Act 2000, the Indian Government introduced the Amendment Bill to overcome shortcomings in the current law. The imposition of stringent punishment for cyber terrorism demonstrates the government's intention to prevent terrorists from using the Internet to perpetrate crime. The Cyber Appellate Tribunal is a specialised tribunal which hears appeals in cyber cases. Specialised tribunals are important because they prioritise and expedite cyber cases.

Global Cooperation

Cross border activities on the internet do not respect geographical limits, and as a result of illegal conduct or transactions, particularly in the field of internet commerce, the parties are subject in many cases to a wide array of laws

becoming cybercrime aware and hiring trained people, and cyber police stations are functioning in major cities throughout the country.

53. This bill amends the *Cyber Crimes and Information Technology Act* 2000. See further Special Correspondent 2008 *www.thehindu.com/*.
54. The Bill also includes a proposal to introduce a Cyber Appellate Tribunal to hear appeals.

and regulations, and often contradictory claims with regards to the interpretation of the laws and jurisprudence where the parties reside and where the transaction took place. The solutions to resolve conflict of laws issues and determine aspects of applicable law and jurisdiction for cross border transactions among private parties are usually achieved through the application of private international law.

In countries with civil law systems, jurisdictional aspects targeting the fields of cyber space has not specifically been addressed due to the judicial systems tradition to strictly follow and interpret legislation contained in written codes and regulations, as well as its inflexibility to follow and adapt foreign rules and precedents on jurisdiction in cyber space. Furthermore, the academic doctrine and literature in this particular field of law has just started to be developed. As identified in the previous section domestic laws on its own cannot effectively deal with the problem of cybercrime, a need for international coordination of laws and binding treaty agreements between countries (bilateral or multilateral) is timely due to the transnational nature of cyber crime. Various countries have established treaty agreements in place while others countries are still scuffling to adopt domestic penal laws.

Harmonization is necessary for both substantive and procedural laws. All countries have to reappraise and revise rules of evidence, search and seizure, electronic spying etc, to cover digitized information in order to conform to modern computer and communication systems, and the global nature of the internet. Better coordination of procedural laws, therefore, would facilitate cooperation in investigations that cover multiple jurisdictions.

Interpol was the first international organization addressing computer crime and penal legislations at a conference in Paris in 1979.[55] In a presentation on computer frauds it emphasized as follows:

> The nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc., between the different countries. International organizations, like Interpol, should give this aspect more attention.

In conjunction with this conference a summary of answers from Interpol member countries on computer crime and penal legislation identified several legislative areas with unsatisfactory existing penal legislations, such as:

a. modifications and erasure of data, or otherwise affecting data processing with destructive intent,
b. appropriation or obtaining data belonging to another with intent to gain the perpetrator,
c. obtaining, without authority, computer services for one's own purposes, using a computer belonging to another,
d. modifications of data with fraudulent intent, or with intent to be used in legal transactions,

55. The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979.

e. disclosure of data without authority.

The summary was the first step on the development of harmonizing penal laws dealing with computer crime around the world.

In 1982, the (OECD) in Paris decided on appointing an expert committee[56] to discuss computer- related crime and the need for changes in the Penal Codes. As a result of the expert committee proposals, the ICCP-Committee of the OECD in 1986 highly recommended and stated that:

> With respect to the transnational aspects of computer-related criminal activity, important issues have been noted which point to the desirability for international cooperation in repressing and controlling such. And that all member countries consider the extent to which acts committed knowingly in this field should be covered by national penal legislation. These acts may be expressed as far as possible in terms of functions rather than technology.[57]

The list of Acts which could constitute a common denominator between the different approaches taken by the

56. A group of experts met at the OECD in Paris on May 30, 1983. These founders of the harmonization of European computer crime legislation recommended that the OECD should take an initiative. An expert committee was established, and recommended in September 1986 through the ICCP Committee a common denominator between the different approaches taken by the Member countries.
57. Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986).

member countries was suggested. The list constituted computer fraud, computer forgery, damage to computer data and programs, unauthorised infringement of a protected computer program and unauthorized access to or inception of a computer system. The Council of Europe further conducted a study on computer related crimes in order to assist the parliament in determining the nature of computer related crime which should be prohibited by law. The result of this study is the enactment of the convention on cyber crime 2001. This convention was entered into force following its ramification by Lithuania, in accordance with its Article 36.[58] The Convention is now a Protocol for legislating against cyber crime, even amongst non-EU States.

The Council of Europe adopted on September 11, 1995 a recommendation concerning problems of procedural law connected with Information Technology. This Recommendation introduces 18 principles categorized in 7 chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international cooperation.[59] Under Article 37, the committee of minister of the council of Europe, with the consent of the contracting states "may invite any state which is not a member of the council and which has not participated in its elaboration to accede to this Convention.

This chapter merely seeks to lay a roadmap for Nigeria's accession to this Convention, Nigeria not being an EU State and having not participated in the Convention's elaboration.

58. See Chapter IV, Final Provisions on Convention on Cyber crime
59. Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on September 11 1995,

Nigeria as a Sovereign State can enter into treaties or convention as a contracting party. These powers which are vested in the President and can be contracted on behalf of the state. The president can exercise these powers personally or by delegation of authority.[60] The tenor of the constitution of the Federal Republic of Nigeria 1999, is such that mere ratification or accession of a Convention does not in itself confer on the treaty a binding force of law in Nigeria unless and until it is domesticated by the national assembly (parliament).

In the celebrated case of *Abacha v. Fawenhinmi*[61],the Supreme Court of Nigeria per Ogundare JSC had this to say:

> Suffice it to say that an international treaty entered into by the Government of Nigeria does not become binding until enacted into law by the National Assembly. See S. 12 (1) of the 1999 Constitution which provides: "No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly." Before its enactment into law by the National Assembly an international treaty had no such force of law as to make its provisions justiciable in our courts.

Under the Cyber Crime Bill now before the National Assembly for enactment, all crimes carried out with the use of computers, electronic and/or ancillary devices will be punished accordingly. The crimes are categorized into three.

60. S.5 of the Constitution of the Federal Republic of Nigeria 1999.
61. (2000) 4 F.W.L.R 533 at 546.

The first group includes unauthorized access to computer systems, access exceeding authorization, computer and system interference, data interception, denial of service, computer trespass and "e-mail bombing". The second category of crimes includes computer contamination, illegal communications, computer vandalism, cyber squatting, cyber terrorism, cyber pornography and intellectual theft. Also included in this category are the use of computers to corrupt a minor, soliciting to compel prostitution, sending obscene materials to minors over the internet, indecent exposure and tampering with computer evidence. The third category includes crimes targeted against critical infrastructure in Nigeria. This aspect protects infrastructure that are critical to the nation's security economic and social interests, The bill also contains procedural provisions with constructive amendments to enable admissibility and evidential weight on digital materials and empowers the Attorney General of the Federation to prosecute the Acts prohibited under the Bill.[62]

This bill, thus, in one fell swoop, seeks, to enact the Nigeria's version of UK's Computer Misuse Act, 1990, Terrorism Act 2001, Copyright Designs and Patent Act 1988 (with its amendments) Protection of Children Act 1978 (as amended) Obscene Publications Act, (as amended) to mention but a few.

Ultimately, the adoption of substantive cybercrime legislation is a step taken toward recognizing that cybercrimes represent a new phenomenon in criminal activity: the globalization of criminal conduct is a phenomenon which all jurisdictions- national as well as sub-national must combine to combat.

62 . See *www.ngrguardiannews.com.*

Recommendations

Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretation in the existing laws. When cybercrime laws are adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental and peripheral Acts. A brief evaluation of the draft bills in Nigeria will highlight disparities between already highlighted legislations.

The first bill titled "Computer Security and Critical Information Infrastructure Protection Bill" 2005 has raised debates amongst academics and stakeholders. The first been how do we determine what is critical infrastructure or system. First, must we determine what type of data it holds and the potential impact of any change or security breach will be before it is deemed critical. The upshot of the bill will mean that a thorough critical risk assessment on a wide range of issues such as the Business community, Terrorism and unauthorised accesss will need to be evaluated to establish the impact levels against information confidentiality, Integrity and availability. Secondly are these so called "critical infrastructures" the only milieu that the law will apply to when it is passed, will this invariably mean computer crime legislation will not be applied to other quarters; i.e. home users. It has been recommended that the bill should cover all quarters and not be limited in its applicability which will lead to the bill not having its desired

effect. Further the definition of critical infrastructure should be delineated in the interpretation to avoid perplexity.[63]

A critical analysis of the second draft bill titled "Cyber security and Information Protection Agency (Establishment, etc) Bill 2008. The proposed bill aims to make it possible to *use electronic evidence as primary evidence* in court. It states that "Notwithstanding anything contained in any enactment or law in Nigeria, an information contained in any computer which is printed out on paper, stored, recorded or copied on any media, shall be deemed to be primary evidence under this Bill". It further recognizes the quandary that Nigeria has when it comes to understanding and implementing adequate and sufficient computer crime and privacy legislations. The Bill addresses unsolicited Commercial E-mail (UCE), unsolicited spamming has for a long time been the scourge of Nigeria's reputation.[64] Recently the Lagos State Police Command arrested two suspects for allegedly committing internet fraud through which they attempted to defraud a businessman of $40,000. The suspects had successfully intercepted the victims e-mail, thus communicating with his foreign suppliers and received a bill of lading diverting his entire shipment to them. [65]

The section should be applauded in its effort to improve Nigeria's fairly tarnished internet image. Collaboration between appropriate authorities will be indispensable to let all countries and bodies know that we have introduced this as a way of combating the issue. The inclusion of this section will have the impact of showing that we have an understanding of the problem and could go a long way in reversing the tainted image.

63. See *www.privacyinternational.org.*
64. See *www.jidaw.com/security.*
65. See *Vanguard* Paper, *Crime Alert*, Tuesday 7,2010.

It is further recommended that the legislature and Senate Committees tasked with combating crime take this issue to the forefront of the initiatives with a view to ensuring that the best brains on the issue not only from a legal and technical point of view but also on experience are actually consulted and involved in the process. This is necessary so that we generate appropriate sections and wordings as well as anticipate what is on the horizon so that laws that constitute the framework are not obsolete and ineffective when passed.

Conclusion

African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime. African countries are pre-occupied with attending to pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes such as murder, rape and theft, with the result that the fight against cybercrime is lagging behind. It is submitted that international mutual legal and technical assistance should be rendered to African countries by corporate and individual entities to effectively combat cybercrime in Africa. African countries need to build partnerships to combat internet crime and corruption. Nevertheless, it is laudable that other African countries (besides South Africa) are making attempts to address cybercrime.

Most law enforcement personnel are not equipped with the requisite technological knowledge while most cyber criminals are experts in computer technology. In combating these crimes there is the need for education and human

capacity development which is one of the most viable strategies. Further, Universities, schools of higher learning and academic institutions should devise specific courses designed to allow the next generation of Judges and Lawyers become skilled in what is a challenging but lucrative area.