UNIVERSITY OF IBADAN JOURNAL OF PRIVATE AND BUSINESS LAW

Vol. 7, 2012

UNIVERSITY OF IBADAN

JOURNAL OF PRIVATE AND BUSINESS LAW

Published by:
Department of Private and Business Law
Faculty of Law,
University of Ibadan

December 2012 U.I.J.P.L. Vol. 7, 2012

University of Ibadan

Journal of

ISSN 1595-2495

2012

All Correspondence should be directed to:

The Editor –in-Chief
Journal of Private and Business Law
Faculty of Law
University of Ibadan

Printed by
Noble Printing Press
09039114256

CONTENT

A NEED FOR CYBERCRIME-SPECIFIC LEGISLATION TO ADDRESS CYBERCRIME AS A NEW PHENOMENON OF CRIME

MARCUS AYODEJI ARAROMI*

ABSTRACT

Cybercrime portrays a new concept of crime that needs to be specially addressed by the law. The ways and the avenues of commission of this type of crime are remarkably different from the traditional means of committing crime, though sometimes the same consequence may result irrespective of the method adopted, only that the gravity may differ. The aim of this research is therefore to address the phenomenon of cybercrime in order to determine if the crime needs special legislative provisions different from the traditional crime statutes applicable in Nigeria.

THE CONCEPT OF CYBERCRIME

It is imperative to state at the beginning that there has been no generally accepted definition of cybercrime, and some writers have equated cybercrime as a computer crime or any crime that involves the use of a computer to commit. According to Wall, there is a general agreement of the existence of cybercrimes but few people seem to

agree on what they are. [1]A similar view was adopted by Kowalski in her 2002 Canada Statistics paper when she said that: "To date, no single definition of cybercrime has emerged that the majority of police departments use [2]" Kowalski in the same paper submitted that Canadian law enforcement agencies have only come to accept a working definition for the purpose of defining what cybercrime entails, which is: "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence."

Okonigene *et al* believe computer crime is a general term which also encompasses cybercrime. They state that 'computer crime' can broadly be defined as: "criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is 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."

Okonigene *et al* further state that computer crimes encompass a broad range of potentially illegal activities and the crime may be categorized into two major groups, which are: (1) crimes that target computer networks and devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

* Department of Public and International Law, Faculty of Law, University of Ibadan, *demarc007@hotmail.com*

[1] Wall D.S. 'Maintaining Order and Law on the Internet', in D.S. Wall (ed.), Crime and the Internet, London: Routledge, 2001, p.168.

[2] Kowalski, M. (2002) Cyber-crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics, Catalogue no. 85-558-XIE, Ottawa: Canadian Centre for Justice Statistics. P.6. (pp.1-31) Available at http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf Accessed 22 December, 2009.

[3] Okonigene R. E. and Adekanle B. "Cybercrime in Nigeria", Vol.3, No.1 (January, 2010), Business Intelligence Journal, p. 94. (pp. 93-98).

Warren B. Chik distinguished computer crimes from what he termed as computer–enabled crimes. To him, computer crimes relate to crimes against computer hardware as well as the digital contents contained within it, such as software and personal data. He posited that computer crime only comes within the confine of crimes committed against a computer or similar device, and data or program therein. Thus, according to him, the computer is the target in committing computer crime. Warren further describes cybercrime to mean offences committed through the use of the computer in contrast to computer crime which refers to offences against the computer.[4]

Many writers have identified cybercrime and computer crime to be one or the same thing. For instance, it has been argued that since computer crimes may involve all categories of crimes, a definition must emphasize the particularity, the knowledge or the use of computer technology. [5] Computer crime or cybercrime can otherwise be referred to as any crime that involves a computer and a network, where the computer may or may not have played an instrumental part in the commission of the crime. [6]In another parlance, computer crime, cybercrime,[7] e-crime, hi-tech crime or electronic crime generally refer to criminal activities where a computer or network is the source, tool, target, or place of a crime.

Cybercrime is a criminal activity done using computers and the internet. It includes stealing money from online banks, and also includes non-monetary offences, such as creating and distributing viruses and stealing confidential business information on the internet. [8]It is a broad term that describes everything from electronic

---

[4] Warren B. Chik, "Challenges of Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore". Available at http://www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc. p.4. Accessed 07/04/2010.

[5] Judge Stein Schjolberg and Amanda M. Hubbard "Harmonizing National Legal Approaches on Cybercrime" ITU, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005, Document: CYB/04, 10 June 2005, p.4. See also Herselman M. E. 2003. Cyber Crime Affecting Some Businesses in South Africa. BSc. Project. Business Information System, Faculti of Computer Studies, Port Elizabeth Technikon. p.8.

[6] For instance, a computer on a network can be used to alter drug prescriptions of a patient which may lead to the patient taking wrong dosage of drug and leading to his eventual death, which can also be done manually if access is had to the prescription note of the said patient. Therefore, computer is only instrumental to the commission of the patient's death.

[7] Cybercrime and internet crime will be used interchangeably in this work as representing one and the same thing.

[8] Tech Terms Computer Dictionary available at http://www.techterms.com/definition/cybercrime. Accessed 22 October, 2010.

cracking to denial-of-service attacks that cause electronic commerce sites to lose money.[9]

NATURE AND CATEGORIES OF CYBERCRIME

The Council of Europe Convention on Cyber-crime of 2001 defines cybercrime in the Articles 2-10 on substantive criminal law in four different categories: (1) offence 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, which form the minimum consensus list, but which may be extended at domestic level through locally enacted legislations. [10] In a similar manner, Pavan Duggal in a report has clearly defined the various categories and types of cybercrimes based on the victims of such crimes. To him cybercrimes can basically be divided into three major categories:

1. Cyber-crimes against persons;
2. Cyber-crimes against property; and
3. Cyber-crimes against government.[11]

Pati categorized cybercrime as cybercrime against individuals, organizations or the society at large.[12]

It is trite to say that computer crime could not be committed before computers were invented. It should however be noted that the history of social control over unauthorized use of computers dates back to the late 1970s, and follows milestone achievements in the development of computer technology.[13] Some authors [14] have divided computer–related crimes into three categories, according to the role computer plays in the commission of any particular crime. First, a computer may be the "object" of a crime. This category primarily refers to theft of computer hardware or software. The second category is where a computer may be the "subject" of a crime.

---

[9] Maya Babu, Mysore Grahakara Parishat (2004): "What is Crime" Computer Crime Research Center. Available at http://www.crime-research.org/analytic/702/. Accessed 20 June, 2010.

[10] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Accessed 20 June, 2010.

[11] Pavan Duggal is the President of cyberlaws.net. See Maya Babu et al. op. cit..

[12] Pati, P. (2003), "Cyber Crime." Available at http://www.naavi.org/pati/pati_cybercrimes_doc03.htm. Accessed 7 January, 2010.

[13] Coldren, D. (1996), "Change at the Speed of Light: Doing Justice in the Information Age," (in :) Sherpenzeel, R. (ed.) Computerization in the Management of the Criminal Justice System, HEUNI Publication Series No. 30.

[14] Huang Xiaomin, Radkowski Peter III, Roman Peter (2007), "Computer Crimes", 44 American Criminal Law Review, Vol. 285 (pp.286-335). Available at http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/amcrimlr44&div=16&id=&page Accessed 12 November, 2009.

One factor that makes a hard-and-fast definition of cybercrime difficult is the jurisdiction dilemma, because different jurisdiction defines cybercrime differently.[20]

Though many writers have defined computer crime and cybercrime to be one and the same thing, it is not sufficient to say that the two phenomena are not mutually exclusive. Crimes that may be committed through the use of computer system or with the availability of computer system may not necessarily be a cybercrime. However, analysts and writers in the computer or information technology environment find themselves plunged into confusion due to the fact that the use of computer may be necessary in the commission of these two modes of criminal activities. It may be said therefore that even though many crimes that are committed through the internet may be carried out by the use of computers, it is not necessary that computers are the targets of such crime. Crimes committed through this means may fall under some other categories of cybercrime, like content-related offence; cyber fraud; infringement on copyright, etc.

Be that as it may, one can safely say that there can be a high threshold of likelihood that the two models can be addressed together by the same legal instrument, such as most developed nations have done.[21] What should be a fundamental compass is to see whether the traditional laws available to outlaw such traditional offences are sufficient in scope to conveniently accommodate such crimes if committed via cyberspace. If not, there is a need to make crimes committed through the internet medium an issue that needs legal solutions. A reliable scope of cybercrime can be distilled by shifting focus on the role the 'network' plays in the commission of the crime. As rightly stipulated by Wall, "the most effective way of reaching a useful definition of cybercrime is to look at it in terms of its evolution and its level of mediation by networked technology. In this way the test of a cybercrime is to simply ask what is left if networked technologies are removed from the equation".[22]

---

[20] Chawki, M., op. cit. p.9.

[21] For instance, "unauthorized access to computer" has reflected in many laws enacted at the national level and in most conventions and international instruments and aimed at curbing illegal access to computer systems and its programs, its contents, etc. such access could be gained in the physical world and the cyber world.

[22] Wall, D.S. (2007) "Hunting, Shooting and Phising: New Cybercrime Challenges for Cybercanadians in the 21st Century" The Second Eccles Centre for American Studies Plenary Lecture, Given at the British Association of Canadian Studies Annual Conference, 2007.

By and large, what makes a cybercrime to be so tagged is that, in the real sense of it, its commission must involve the use of network technologies; the absence of which takes such a crime away from the threshold of cybercrime.

ANALYSIS OF SOME ENDEMIC CYBERCRIME

At this juncture, it is germane that an in-depth discourse is made of the different types of crimes that may be committed through a computer or a computer network.

a, Hacking

Computer hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system.[23] Hacking has also been described as a means of securing unauthorized access to a computer or computer network.[24] Consequently, if unauthorized persons are able to penetrate computer systems and obtain access to confidential records, such information can be sold to competing companies.

The House of Lords[25] in the case of *R. v. Gold,*[26] highlighted the problem of computer hacking and the ease with which it could be done. In this case two computer hackers gained access into the British Telecom Prestel Gold computer network without permission and altered data. One of the accused also got into the Duke of Edinburgh's personal computer files and left a message therein. The two accused hackers who were journalists by profession claimed they hacked into the network in order to show the deficiencies in its security. The accused were found guilty at Crown Court and were respectively fined £750 and £600. Their convictions were later quashed by the Court of Appeal and this was confirmed in the House of Lords. In the Court of Appeal, the Lord Chief Justice, Lord Lane, said that the acts of the accused in gaining access to the Telecom Gold files by what amounted to a dishonest trick were not criminal offences. In the House of Lords, Lord Brandon of Oakbrook said:

---

[23] Bainbridge D. Introduction to Computer Law, 5th ed. (U.K: Pearson Longman, 2004), p.381.
[24] Toun Adebiyi, "Internet Crime", 2005, Modern Practice Journal of Finance and Investment Law, Published by Law and Economic Development, Lagos, Nigeria, p.160.
[25] House of Lords is the perceived highest court in England.
[26] [1988] 2 WLR 984.

> The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is matter for the legislature rather than the courts. We express no view on the matter.

The decision in *R v Gold* above sent a strong signal to all and sundry, especially the computer industry, that computer hacking was not a criminal activity. This unfavourable position led to the Law Commission Working Paper No. 110, Computer Misuse (HMSO, 1988), examining the scope of the law in terms of computer misuse generally and proposing alternative suggestions for legal changes directed at the problem of computer crime.[27]

Some other negative aspects of unauthorized access include modification of computer programs and data, data theft, destruction of computer files, imputing false commands in the computer, etc. Computer crimes affecting business most often include, but are not limited to:

1. Introduction of unauthorized data into a system;
2. Manipulation of data to gain access to associated asset (e.g. computer or telephone time, money, credit);
3. Creation of unauthorized duplicates of files, software, and other information asset;
4. Unauthorized use of passwords or account codes;
5. Theft or vandalism of hardware, software, computer time, or networks;
6. Using a computer as a weapon (e.g. tampering with real-time systems for flight control on an airplane).[28]

[27] Bainbridge D. op. cit., p.382. The necessary provisions of this Act and subsequent amendments will be discussed later on in this work.

[28] Chris Westland, "A Rational Choice Model of Computer and Network Crime", Vol 1, No.2, (1996/1997) International Journal of Electronic Commerce. Also available at http://www.jstor.org/stable/27750812 pp. 109-126.

The cost of economic crimes arises from at least four distinct sources, which are loss or transfer of property,[29] disruption of business, enforcement costs and illegal expenditures.[30]

b. Malicious computer programs

Malicious computer programs are programs developed or designed to harm the victim(s). The malicious programs are divided into the following categories:

c. Computer virus

A computer virus is a software program written with malicious intentions and designed to replicate itself by attaching to files or disks.[31] Viruses are primarily transmitted from one system to another in two ways, contaminated disks, which are used in clean or virus-free computers and via telephone lines. The rate of spread of computer viruses through the internet and email poses a greater danger than the spread via infected floppy disks.

The most common outside threat to a business's computer network is the virus. By the estimation of the National Computer Security Association (NCSA) in the United States in 1996, two out of three U.S. companies were affected by one or more of the estimated 16,000 computer viruses that were floating around the country at that time.[32] Viruses can come in two forms: *macro* and *binary*. *Macro* viruses are intentionally written to attack a specific program.[33] *Binary* viruses are either actual programs designed to attack computer data or attach themselves to program files to wreak similar destruction. Binary viruses can reformat a computer hard drive, wipe out data and stop computer operating system from working, which calls for an intense concern.[34] Viruses could automatically send email with the victim's name as the alleged source.[35]

[29] This is the commonest computer-related offence carried out by Nigerians. This malfeasance is mostly common amongst the Nigerian youth, and they are often called 'Yahoo Boys'.

[30] Chris Westland op. cit., p.110.

[31] Patrick Ling, "Is Australian Criminal Law up to the Threat of Computer Viruses" September Issue, (2000), NSW Society for Computers and the Law Journal. Available at https://www.nswscl.org.au/index.php?option=com_content&view=category&id=13:september-2000-issue&Itemid=31&layout=default Accessed 19 January, 2010.

[32] Computer Crime: West's Encyclopedia of American Law (Full Article) from Answers.com. Available at http://www.answers.com/topic/computer-crime. Accessed 19 January, 2010.

[33] Ibid.

[34] Ibid.

[35] A good example of such virus is the Melissa virus which infected computer networks in March 1999. It is sent via email which contained infected attachment. The subject of the message stated 'Here's the information you requested' and directed the reader to open the attachment word document. If the attachment was opened using Microsoft Outlook, the virus would send copies of the infected document to the first 50 email addresses in the user's address book. The effect could be more damaging where these addresses contained groups of users. The virus was estimated as having spread to 50,000 computers in less than 10 minutes. Another virus that caused similar but greater damage was the 'Love bug'. Its mode of operation is by attaching itself to every entry in the user's address book. Once opened, the attachment also destroyed selected files on the user's computer. Although reports vary greatly, computer experts estimate that about 80 per cent of businesses received the full effects of the virus. Apart from these viruses, new ones are now being discovered which have even more deadly effects on computers among which is 'explore.zip'.

d. Worm attack

A worm is a program that copies itself. It spreads copies of itself through a network. The difference between a virus and worm is that a virus does not copy itself a virus is copied only when the infected executable file is run.[36] Another difference between a worm and a virus is that a worm operates through networks and a virus can spread through any medium (but usually uses copied program or data files. which can also be done on the internet).[37] In its original form, a worm neither deletes nor changes files on the victim's computer; it simply makes multiple copies of itself and send those copies via the Internet with multiple copies Releasing such a worm into the Internet with the ability to reproduce itself will slow down the computer, as continuously increasing amounts of traffic are mere copies of the worm.[38] In other words, worms, unlike viruses, do not need the host to attach themselves to and they do this repeatedly till they eat up all the available space on a computer.

e. Trojan Horse

It does not operate by replicating itself which makes it different from viruses and worms. A more serious form of a Trojan Horse program allows a hacker to control the victim's computer remotely and perhaps collect passwords and credit card numbers and send them to the hacker, or launch denial-of-service attacks on websites.[39] There are two possible ways a Trojan Horse can get into the computer system of the victim:[40]

a. It may be installed on the victim's computer by an intruder, without the knowledge of the victim;
b. It may be downloaded (perhaps in an attachment in an e-mail) and installed by the user, who intends to acquire a benefit that is quite different from the undisclosed true purpose of the Trojan Horse.

The significant legal concern about a Trojan Horse is that it is the computer user and not the writer of the Trojan Horse that executes the main program, as the program lies indolent until activated by the user.[41]

---

[36] Ronald B. Standler, op. cit.
[37] Ally Abdallah, (2011) "The Impact of ICT Revolution in Tanzania's Legal System: A Critical Analysis of Cybercrimes and Computer Forensic Evidence." A LL.M Research Paper (Thesis), Open University of Tanzania. P.55.
[38] Ibid. It is also possible for a worm to drop a virus into the victim's computer. This started with klez worm in early 2002, and it came to be known as a 'blended threat', because it combined two different types of malicious code.
[39] Ibid.
[40] Ibid.
[41] Ally Abdallah, (2011) op. cit., p.57.

f. Logic Bomb

A logic bomb is a hidden program, like the Trojan Horse, which when triggered by a particular event performs its intended function. In the event of detonation of this program it crashes the computer, releases a virus in it, deletes data files, or performs such other heinous tasks on the computer.

g. Web-jacking

This occurs when someone forcefully takes control of a website by cracking the password and later changing it. The actual owner of the website is thus disposed of control over the website or what appears on that website. The hackers take control of the website and decide what appears on it. The term is derived from hijacking. It is sometimes done to achieve political objectives or for money.[42] Example of the monetary motive is found in the 'gold fish' case where a site was hacked and the information pertaining to gold fish was changed. A ransom of US $1 million was demanded to release the website to the legitimate owners.[43]

h. Denial-of-service attack

In a relative term, Denial of Service involves flooding computer resources with more requests than it can handle. This causes the resource (e.g. a web server) to crash, thereby denying authorized users the services offered by the resource. Distributed-Denial-of-Service (DDoS) attack involves a technique used in flooding a target website with requests until it crashes. It is a variation of Denial of Service attack but in its own case the offenders are much in number and widely distributed. Messages are generated by computers that have themselves been hacked into to serve as launch pads for the electronic bombardment.[44]

One big reason hackers do resort to this form of attack is that a business may want to harm a competitor by crashing his systems. Another reason may be that the hacker might have installed a Trojan in the victim's computer but needed to have the computer restarted to activate the Trojan.[45]

---

[41] Ally Abdallah, (2011) op. cit., p.57.
[42] Ibid. p.58.
[43] See http://en.asianlaws.org/library/cyberlaws/index.htm. Accessed 20 November, 2009.
[44] Douglas Holmes op. cit., p.199. Note that this type of attack is used to launch terrorism against adversary nation and also a reprisal attack by the targeted nation. The flooding of email boxes at government offices, denial-of-services attacks, and web page hijacking are relatively primitive techniques of information warfare, achieving a low level of disruption but a high level of publicity.
[45] Ibid.

Denial-of-Service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo and eBay.[46] This type of attack was also experienced in 2008 just prior to Super Bowl XLII. To launch Denial-of-Service attack is very simple as its tools can easily be procured from the Net, and its major versions include Trinoo, TFN, TFN2K and Stacheldraht. [47] Denial-of-Service tools allow the attackers to automate and present the times and frequencies of such attacks so that the attack is launched and then stopped to be launched once again later. This makes it difficult and in fact impossible to trace the source of the attack.

Denial-of-Service attack can also work in a way by which the attacking computer can change its source address randomly thereby making it seem as if the attack is originating from thousands of computers while indeed there may only be a few computers as the sources. This mode of operation further complicates the problem as it will be very difficult for the sources to be traced. In most cases these attacks are directed towards very sensitive systems or networks sometimes including those that are vital for national security.

CYBERCRIMES THAT CAN BE REPLICATED IN THE PHYSICAL WORLD

The European Commission[48] has itemized the following areas as

- national security (instruction on bomb making, illegal drug production, terrorist activities);
- protection of minors (abusive forms of marketing, violence, pornography);
- protection of human dignity (incitement to racial hatred or racial discrimination);
- economic security (fraud, instructions on pirating credit cards);
- information security (malicious hacking);
- protection of privacy (unauthorised communication of personal data, electronic harassment);

[46] Ibid.
[47] Ibid.
[48] Communication to the European Parliament, the Economic and Social Committee and the Committee of the Regions, Illegal and Harmful Content on the Internet 2: How does the Internet work? COM (1996) 487. Available at www.epic.org/CDA. Accessed 20 November, 2011.

- protection of reputation (libel, unlawful comparative advertizing);
- intellectual property (unauthorized distribution of copyrighted works, for example, software or music).

In addition to the various traditional crimes, some of which can also be perpetrated through the computer, like pedophilia, child pornography, money laundering, drug trafficking, embezzlements of bank deposits, fraud (credit card numbers), industrial and political espionage, a number of IT-specific malevolent attacks against the security of critical infrastructures, such as telecommunication, banking and emergency services, may be launched through computer networks across national boundaries.

Computer crimes are separated into two categories: which are crimes committed using a computer and crimes where a computer or a network is the target. The former category includes crimes such as storing records of fraud, producing false identification, reproducing and distributing copyright materials, collecting and distribution of child pornography – which are crimes that can also be committed traditionally without the use of a computer. Crimes where computers are the target, on the other hand, can result in damages or alteration to the computer system.

Some of the offences that are committable in cyberspace that can also be committed traditionally without a computer will now be discussed.

a. Cyber extortion

Cyber extortion is demanding money or something of value in exchange for not carrying out threats to commit harm that will involve the victim's information systems. [49] This offence is a cyber variation of illegal use of force or one's vantage position or power to obtain property, funds or patronages in the traditional crime style. While there is scanty evidence of cyber extortion, available evidence indicates that it is a significant variety of cybercrime that is underappreciated as a threat and underreported. [50]

---

[49] Adam J. Sulkowski and Timothy Shea: "Cyber-Extortion in the Server Room", Available at http://www.papers.ssrn.com/sol3/results.cfm?abstract-id=9559169. Accessed 29 December, 2009.
[50] Ibid.

There is evidence that the threat of cyber-extortion has been increasing. In 2004 the number of networks set up for criminal uses skyrocketed from 2,000 to 30,000 within six months as reported by Symantec Corporation's Security Response Service.[51] One of the common tactics in cyber extortion is to threaten to incapacitate a victim's transactional website or other components of their information system.[52] This can be done by employing the denial-of-service attack.

Cyber extortion is now professionalized with the resultant effect that the systems for committing a DDoS attack are now available for rent or for hire.[53] For further clarity, there are now cyber criminals who inconspicuously hijacked businesses' information systems and assemble them into a coordinated network that can be used to send electronic transmissions that overwhelm a target business' website. These hijacked information systems are referred to as "zombies".[54] The coordinated networks of zombies-for-hire are referred to as "botnets".[55] An extortionist may follow-through on a DDoS attack, such an attack can render an entire company network unusable, potentially resulting in the loss of email, loss of external access to a company's transactional website and the unavailability of critical company systems.

b. Computer fraud

Some writers once said:

> The computer revolution has provided tools with which to steal with, control and manipulate the thoughts and movements of millions, and hold an entire society hostage.[56]

---

[51] George V. Hulme, Extortion Online, Information Week, September 13, 2004. Available at http://www.informationweek.com/story/showArticle.jhtml;jsessionid=XHCTLPEBU4LVCQSNDBGCKHY?articleID=47204212. Accessed 2 February, 2007.
[52] Adam J. Sulkowski and Timothy Shea, op. cit., p.8.
[53] Adam J. Sulkowski and Timothy Shea op. cit., p.9.
[54] Ibid.
[55] Ibid. Botnet can comprise hundreds, thousands or even tens of thousand computers.
[56] Diane Rowland and Elizabeth Macdonald, op. cit. p.448.

Computer or cyber theft is described as the stealing of money or property by means of a computer: i.e., using computers to obtain, dishonestly, property (including money and cheques) or credit or services or evade dishonestly some debts or liabilities.[57] Computer fraud has been described by the Council of European Convention on Cybercrime as intentionally causing a loss of property in order to improperly secure economic benefits and advantages by any input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer or system. According to *Article 8* of the Convention:

> Each Party shall adopt such legislative and other measures as criminal offenses under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
> a. Any input, alteration, deletion or suppression of computer data,
> b. Any inference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.[58]

Also included in the definition by the convention is fraud related to internet auctions, telemarketing fraud,[59] intentional illegal entry into sites for economic gain, and misuse of a computer for the purpose of achieving an illegal economic advantage.[60]

---

[57] David Bainbridge, op. cit., p. 366.

[58] The Commission of Experts on Crime in Cyber-Space, Council of Europe, Draft Convention on Cyber crime, approved by the European Commission on Crime Problems, 50th Session, June 18-22, 2001, Doc. No. CDP(2001)17.

[59] Telemarketing fraud has become one of the most pervasive forms of white-collar crimes in the United States and Canada, with the annual losses tuning to billions of dollars in both countries. See The United States-Canada Cooperation Against Cross-border Telemarketing Frauds, Report of The United States-Canada Working Group to then President Bill Clinton and Prime Minister Jean Chrétien, (Nov. 1997) (examining incidence of telemarketing fraud between United States and Canada suggesting ways to address it. Available at http://www.usdoj.gov/criminal/uscwgrtf/index.html. Accessed 12 February, 2001.

[60] The types of fraud that are increasing in number include: "auction or retail fraud", "securities fraud", "pyramid or ponzi schemes", "credit card fraud", "identity theft", "business opportunity schemes". See Jonathan Rusch "Consumer Fraud via the Internet", Symposium on Federal Sentencing Policy for Economic Crimes and New Technology Offences 290-94 (October 13, 2000). Available at http://www.usse.gov/2000sympo/vGroupFourDayTwo.pdf. Accessed 12 February, 2001

Computer related offence can also take place in fund related activities. For instance, dishonestly giving instruction to a computer to transfer funds into a bank account or using forged bank cards to obtain money from a cash dispenser (automated teller machine).
There are two main types of computer fraud, which are:

1. Data frauds and
2. Programming frauds[61]

Data fraud can also be divided into *input fraud* and *output fraud.*[62] The programming fraud seems to be the less common as it requires considerable knowledge and expertise. Programming fraud include writing of program which automatically 'slices off' small amounts from a number of accounts and transfers them to another account created for the purpose. Scrapping small amounts of money from each account may be unnoticeable because such amounts will be so negligible to arouse suspicion. One of the programs that can be developed to carry out such fraud is the *salami program*. Salami and other program frauds can also be activated at a later date, creating consequent problems in detection of both the fraud and the perpetrator.[63]

c. Drug trafficking

Drug traffickers have also taken the advantage of the internet in plying their illicit trade. The drug traffickers sell their illegal substance through encrypted email and other Internet Technology. Some drug traffickers arrange deals at Internet cafes, use courier web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in internet drug trafficking may be attributed to the lack of face-to–face mode of transactions between the parties to this trade. In other words, these drug traffickers operate in the cyberspace where they are not 'physically' present. This virtual relationship creates a haven for timid actors to carry out their transactions without fear. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.[64]

---

[61] Ibid.
[62] Diane Rowland and Elizabeth Macdonald, op. cit, pp.449-450.
[63] Ibid.
[64] Anon. "Computer Crime". Available at http://www.answer.com/topic/computer-crime. Accessed 2 February, 2009.

. Furthermore, drug recipes information is now being made available to anyone with computer access as against the traditional secrecy in which it is being kept.

d. Spam

Spam, in the context of the internet, generally refers to unsolicited and unwanted electronic messages, usually transmitted to a large number of recipients. Spam is also referred to as Unsolicited Bulk Email (UBE), or the more narrowly defined Unsolicited Commercial Email (UCE). [66] Most spam is of a commercial nature and is often used for advertising dubious products, financial scams, and get-rich quick schemes. For a message to qualify as spam it need not be offensive or commercial, or be sent fraudulently. Spam takes on many forms, including advertisements of products and services, [67] chain letters, [68] destructive codes or viruses, [69] cartoons, [70] scams, [71] and other general spam that comes from pedophiles, pornographers, and other familiar sources. [72]

A replica of this offence which can be committed traditionally is seen under *section 5* of the *Advance Fee Fraud and Other Related Offences Act* [73] of Nigeria which states that sending of letter or document to a victim with a false pretence, and the receipt of same, with the intention to defraud him constitutes an offence under the Act.

---

[65] Ibid.

[66] Michelle Lara Geissler (2004), "Bulk Unsolicited Electronic Messages (SPAM): A South African Perspective," A doctoral thesis submitted to University of South Africa, p.16.

[67] Such advertisements include the ones proclaiming money-making opportunities, including pyramid-style schemes, multi-level marketing systems, and investment opportunities. It may also include advertisement adult entertainment, single services, sexually-oriented products and services, phone services, vocation packages, nutritional supplements, weight loss products, credit cards, cable de-scramblers, and online newsletters, etc.

[68] Electronic mail often contains messages that promise good luck if such messages are forwarded to others and bad luck if such messages are not sent.

[69] Most virus hoaxes falsely claim to describe an extremely dangerous virus; use pseudo-technical language to make impressive sounding, but impossible claims, falsely claim that the report was issued or confirmed by a well known company; ask you to forward it to all your friends and colleagues. Continuous forwarding of these hoaxes waste time and email bandwidth, and where emails contain file attachments they need to be treated with caution as they may be infected with virus.

[70] The cartoons type of spam can easily be infected, either deliberately or accidentally with virus.

[71] This is the most common type of spam, and it includes money and identity theft schemes. The scammers in their style may ask for credit and personal information. Emails are sent to the receivers from alleged "official" representing a foreign government or agency or a reputable business, with an offer to transfer millions of dollars into their personal bank accounts. Some of the scam messages may also include phoney information stating that the targeted user has won a lottery and should send handling fee to receive the winning. It may also include message asking for your ATM codes and account details with which they can fraudulently track the money in your account.

[72] Michelle Lara Geissler (2004) op. cit., p.88.

[73] Cap A6, Laws of Federation of Nigeria, 2004.

e. Cyber terrorism

The first known terrorist act against a country's computer systems was carried out in 1998 when an offshoot of the Tamil Tigers bombarded Sri Lankan embassies with 800 emails a day over a two-week period, and the messages read: "We are the Internet Black Tigers and we're doing this to disrupt your communications." [74] In a like manner, in 1999 during the Kosovo conflict the North Atlantic Treaty Organization (NATO) computers were hit with email bombs, macro viruses, and denial-of-service attacks by Serbian hackers and other groups protesting the bombings. A reprisal attacks were carried out by hackers from Albania and NATO countries on Serbian computers.[75]

International warfare is now taking a new turn and a new form as attacks are now being focused on strategic information infrastructures of the enemy countries.

The most technologically advanced nations are the most vulnerable to acts of cyber terrorism, the reason being that those weaker countries that do not have the military muscle to engage the powerful nations in fights can easily do so in cyber space.[76]

All countries that make use of computer technology and especially, those connected to the internet are vulnerable, though the level to which the United States has incorporated new technologies and the highly networked nature of its infrastructure makes it the most vulnerable.[77]

The claim that cyber terrorism is more humane than conventional warfare because it will not inflict loss of life and severe economic hardship has been disputed. Douglas Holmes said that:

> Chaos would ordinarily ensue if terrorists broke into computer Mission Impossible-style to disrupt railways and air traffic control, overload telephone lines, change the pressure in gas pipelines, shut down electricity grid, sabotage stock exchanges and banking systems, block communications used by emergency services, alter hospital patient records such as blood types and reprogram robots used in telesurgery.[78]

---

[74] Douglas Holmes, op. cit., p.200.
[75] Ibid.
[76] Douglas Holmes, op. cit, p.201.
[77] Richard W. Aldrich, "Cyberterrorism and Computer Crime: Issues Surrounding The Establishment of International Legal Regime" INSS Occasion Paper 32, Information Operation Series, April 2000, USAF Institute of National Security Studies, USAF Academy, Colorado.
[78] Ibid, p. 202.

f. Identity theft

This crime involves wrongfully or fraudulently obtaining and using another person's identifying information in some way that involves fraud or deception, typically for economic gain.[79] The person's identity may include names, social security number, credit card numbers, and so on.

The criminal in this case can use the victim's information to purchase goods or enter into such other transactions. This crime of identity theft can be carried out without the use of any technical means, as well as online, by making use of internet technology. By the use of the internet, the perpetrator persuades the victim to disclose confidential information on a website and uses it in criminal activities.

The United States Federal Bureau of Intelligence (FBI) breaks identity theft into two types, which are account takeover and account creation.[80] Account takeover is defined as the use of a victim's current accounts to make purchases. Account creation on the other hand, is the use of personal identification data to open new accounts in the victim's name.

g. Copyright-related offences

Before the representation of intellectual materials in digital form they could be represented on paper, tape or celluloid and other traditional storage media. Copying or duplication of intellectual works could not be carried out with ease as the digital storage media. Digitalization has opened the door for new copyright violations. The act of copying materials with the advent of digitalization has been done with accuracy. Before digitalization, copying a material or a video-tape always resulted in a degree of loss of quality. It is however possible to copy or duplicate information represented in a digital format without loss of quality. Duplication and distribution of digital materials are now very easily done with technology and internet. This has encouraged copyright violation where digital information can easily be copied illegally irrespective of national borders.
The most common copyright violations include:[81]

---

[78] Ibid, p. 202.
[79] Marco Gercke "Internet Related Identity Theft". A Project on Cybercrime sponsored by Council of Europe and and Microsoft. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf , p.4. Accessed 7 September, 2011. (pp.1-32).
[80] Ally Abdallah, op. cit. pp.66-67.
[81] International Telecommunication Union (ITU) Cybercrime Legislation Resources "Understanding Cybercrime: A Guide For Developing Countries", ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Communication Development Sector, Draft April 2009, p.41.

- Exchange of copyright-protected songs, files and software in file-sharing systems;
- The circumvention of Digital Rights Management (DMR) systems.[82]

The latest technology of file-sharing systems which work on peer-to-peer[83] technology enable users to share files with millions of people on the internet in a short period of time. With a file-sharing software installed on a computer, users can select files to share and use equally to search for other files made available by others for download from hundreds of sources. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software.

Due to direct communications between computers in peer-to-peer networks, it is possible for law enforcement agencies to trace copyright violations by users through their Internet Protocol (IP) addresses. However, with the recent version of the Peer-to-Peer network which can work based on anonymous communications, technology investigations of copyright breaches will be more difficult to carry out. This has posed a serious challenge to the entertainment industry and the intellectual world, among others. In response to this situation, the entertainment industry designed technologies to prevent file-sharing through an encryption technology preventing content on DVDs from being copied. The problem, however, is that this technology has also been circumvented by copyright offenders who have developed software tools[84] that allow them to make copies of protected material or files. Once the DMR is removed from the file, copies can be made available and shared among users. It should be noted that the same challenges are being faced by the Pay-TV channels that use encryption technologies to ensure only paying customers have access to their services. Offenders have succeeded in breaking the encryption security using software tools.[85]

---

[82] Digital Right Management describes access control technology used to limit the usage of digital media.
[83] Peer-to-Peer (P2P) is a direct connectivity between two or more computers and facilitates direct communications between the computers without the need of a central server.
[84] These tools are available on the Internet free of charge or at a low cost.
[85] See International Telecommunication Union (ITU) Cybercrime Legislation Resources "Understanding Cybercrime: A Guide For Developing Countries", ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Communication Development Sector, Draft April 2009, p.44.

Violation of copyright on the Internet has become a thorny issue that needs to be adequately addressed. There have been discussions on the criminalization of copyright violations, not only on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable users to carry out copy right violations.[86]

Cybercrime is a concept that has taken with it new ways of committing traditional crimes and has also introduced entirely new types of offences that are peculiar to the computer system or network. Thus, there has been difficulty in properly defining the laws needed to allow for apprehension and prosecution of cybercriminals. While seemingly a straightforward task, difficult issues are raised. One is whether the definitional scope of cybercrimes should include only laws that prohibit activities targeting computers or should also outlaw crimes which can traditionally be committed in the physical environment but only see computer as a new and faster avenue for committing these old crimes. Another is whether these laws should be cybercrime-specific, targeting only crimes committed by exploiting computer technology. Is it, for example, necessary for a country to add a "computer fraud" offence if it has already outlawed fraud?

The question that demands an answer hitherto is what is the best legislative practice to be adopted in cybercrime matters? Some scholars believed that the traditional existing criminal statutes were sufficient for successfully prosecuting any type of computer abuses, many others presented strong legal, technical and practical arguments, and strongly believed that the existing criminal statutes were not suitable for the digital era; submitting that the nature of computer crime necessitates specialized legislation.[87]

According to a scholar, the questions to be addressed for there to be a legislative intervention can be expressed thus:

---

[86] Ibid. The Council of Europe Convention on Cybercrime, 2001 also address the issue of copyright on the Internet in Article 10.

[87] Douglas H. Hancock, "To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention?" Vol 12, (2001) Albany Law Journal of Science & Technology (Alb. L.J. Sci. & Tech.), 97, Carla Ottaviano, "Computer Crime," V. 26, (1985-1986) IDEA: The Journal of Law and Technology, p163 at 167.

> For the legislative intervention to be sound and successful two major questions should be adequately addressed; the scope of legislative intervention and the nature of computer crime legislation enacted. Regarding the first question, new criminal provisions are needed only to cover those crimes that are unique to computers themselves, other crimes in which a computer is used simply as an instrument for perpetration are either covered by existing criminal provisions or can be covered by simple amendments of said provisions. Another step that should be taken by legislators is the amendment of existing criminal laws with an aim to cover some special cases such as the cases in which the computer is used as an instrument for committing known traditional crimes, making the perpetration of such crimes easier or resulting in more dangerous consequences compared to their more traditional forms and cases in which intangible digitized property comes under threat from criminal activities.[88]

It is important therefore to study the possible categories cybercrime can come under to appropriately determine its nature and possible scope of legislative intervention.

COMPARISON OF SOME CYBERCRIME THAT HAVE RELATIVE PROVISIONS UNDER THE NIGERIAN LAW

It is necessary at this juncture to make critical comparison of some cyber crimes that have similar provisions of crimes addressed under extant law.

a. House Breaking or Burglary versus Computer Hacking

Computer hacking may be likened to burglary or house-breaking in the real world situation. These two phenomena involve unlawfully having access to a prevented "place." One may however draw a very clear distinction between the two concepts. In the case of burglary *section 411* of the *Nigerian Criminal Code*[89]

---

[88] Rizgar, Mohammed Kadir, "The Scope and Nature of Computer Crime Statues- A Critical Comparative Study" German Law Journal Vol. 11 No. 6 , 2010. Available at http://www.germanlawjournal.com/pdfs/Vol11-No6/PDF_Vol_11_No_06_609-632_RM_kadir.pdf. Accessed 17 December, 2011. (pp. 609-632)

[89] Criminal Code Act, Cap C38, Laws of the Federation of Nigeria, 2004.

provides that any person who *breaks* and *enters* the dwelling–house of another with intent to commit a felony therein; or having entered the dwelling-house of another with a like intent or having committed a felony in the dwelling-house of another, breaks out of the dwelling-house, is guilty of a felony. If the offence is committed in the daytime it is appropriately called house-breaking and is punishable with imprisonment for 14 years. If such is committed at night, it is called burglary and is punishable with imprisonment for life.

Adapting the above provision to computer hacking will not produce a perfect result. In the first place, hacking does not need a physical breaking or entering into a property which is one of the requirements of the offence of burglary. It cannot be assumed that "forcefully" gaining unauthorized access to a computer or its network constitutes breaking in the real sense of the word, since such computer is not put under physical locks and keys. Breaking requires exertion of force [90] on an object, which is not the case in computer hacking that only requires manipulation of codes to gain access to the computer. Also, entry requires that any part of the accused's body or any part of any instrument used by him is within the building which cannot be said to occur in computer hacking.[91] Therefore, the provision of *section 411* of the *Criminal Code* which deals with burglary and house- breaking is not sufficient for computer hacking. Offence of hacking can be dealt with using unauthorized access to computer provision as done under the Council of Europe Convention on Cyber-crime and other countries' cyber-crime laws. [92]

[90] See R v. Boyle [1954] 2 Q.B. 292 and R v. Chandler [1913] 1 k.B. 125.
[91] R v. Apesi [1961] W.N.L.R. 125.
[92] Council of Europe Convention on Cybercrime, 2001.

b. Extortion versus cyber extortion

Extortion is using one's vantage position to forcefully obtain things of value from a victim.[93] In the cyber environment it may include hacking into and controlling various industries' databases (or the threat of) promising to return the control back to the company if funds are released or other demands satisfied. It may also require a threat to carry out some damage on the network or website of an organization unless certain demands are met. The provisions of *sections 406-409* of the *Nigerian Criminal Code* are meant to prosecute extortion in Nigeria. *Section 406* of the Code provides that any person who, with intent to steal anything, demands it from any person with threats of any injury or detriment of any kind to be caused to him, either by the offender or by any other person, if the demand is not complied with, is guilty of a felony.

It is also provided under the code that any person who, with intent to extort or gain anything from any person, and knowing the contents of the writing, causes any person to receive any writing demanding anything from any person without reasonable or probable cause, and containing threats of any injury or detriment of any kind to be caused to any person, either by the offender or any other person, if the demand is not complied with, is guilty of a felony, and is liable imprisonment for 14 years.[94]

The above provisions of the *Criminal Code* may be extended to cover cyber extortion which can also be done by the accused without the victim actually being physically in his presence. A threat can be transferred in writing online, for instance, through email, to the victim who may not even have physical access to the accused. The same threat can also be carried through telephone lines. Since the code does not require physical presence of the accused and the victim in close proximity to each other, the provision of the code can apply to online extortion. Note however that the problem of jurisdiction may rear its head in online extortion.

---

[93] See the cases of R v. Eka (1945) 11 W.A.C.A. 39; Motayo v. C.O.P. (1950) 13 W.A.C.A. 114; Otuji v. I.G.P. (1960) L.L.R. 123; R v. Olua (19943) 9 W.A.C.A. 30; Ogbegbor v. C.O.P. (1950) 13 W.A.C.A. 22; and R v. Ibrahim (1953)20 N.L.R. 137.

[94] Section 407 of the Criminal Code, op. cit.

c. Fraud versus cyber fraud

The offence of fraud is provided for in *section 419* of the *Nigerian Criminal Code Act*. It provides that any person who by false pretence, and with intent to defraud, obtain from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony. To obtain in this crime, one must induce the owner to transfer his whole interest in the property. [95] This means that the owner must be deceived to part with his goods. [96] In terms of computer fraud, the difficulty is that it requires a deception and this implies that it is an actual person that is being deceived, not a machine. [97] The court held in the English case of *DPP v. Ray* [98] per Lord Morris that for a deception to take place there must be some person or persons who will have been deceived. This means that the deception must work upon a human's mind.

The above deduction will mean that if a person has illegal access to a bank's computer and dishonestly transfer money from one account into another that means that person is "deceiving" a computer system by claiming he has an authority to make such transfer. Such a person cannot be successfully prosecuted with the provision of the fraud law because he has actually deceived nobody but the computer – which cannot be deceived in the real sense. It means therefore that a person who illegally obtains services from a computer database services, for instance LexisNexis, cannot be successfully prosecuted for fraud under the code because he has actually deceived no one.

An alternative solution may be to bring such case under theft. The requirement of law of theft is permanent deprivation of the owner of the thing capable of being stolen of that thing. [99] A person who has illegally transferred money from an account in a bank's computer to his own account may therefore be said to have stolen the money. However, this provision may not be sufficient for all types of undue advantages that can be achieved on the internet. For instance, a person who has gone on the website of a database provider and illegally accessed and copied data from the site cannot be said to have permanently deprived the provider of such data but has only

---

[95] Okonkwo, C. O. Okonkwo and Naish on Criminal Law in Nigeria, 1996 (reprint), 2nd ed. Spectrum Nigeria, p. 309.

[96] Note also that the supplemental provision of section 419 of the Nigerian Criminal Code which is the Advanced Fee Fraud and Other Related Offences Act also requires in sections 1 and 2 that human beings must be deceived to commit the offence of obtaining property by false pretence.

[97] Bainbridge, D. Introduction to Computer Law, op. cit. p. 371.

[98] [1974] AC 370.

[99] See section 383 of the Nigerian Criminal Code, op. cit.

copied the data; such data are still available for the use of the owner.[100] In such a case, traditional theft law is not sufficient to prosecute the accused in this case. It is therefore important that special law should be enacted to take care of such cases.

d. Obscene publication versus cyber pornography

Obscene publication is an offence under the Nigerian law prohibited by *section 233D* of the *Criminal Code*[101] and it is titled 'Prohibition of publication of obscene matter.' *Subsection (2)* of that section provides that any person whether for gain or not, distributes or projects any article deemed to be obscene commits an offence punishable on conviction by a fine not exceeding four hundred naira or by imprisonment for a term not exceeding three years or by both.[102] A quick look at this provision will seem as if it covers cyber pornography. The problem with that section is the silence on the definition of "publication." When can a material be published? A simple dictionary meaning of publication "is the act of printing a book, a magazine, etc., and making it available to the public."[103] Furthermore, publication also includes "the act of printing something in a newspaper, report, etc., so that the public knows about it."[104]

The above succor from the simple dictionary meaning of publication does not help in the case of cyber pornography. From the definition of obscene publication above, when an obscene image is sent to a selected few through their email accounts it cannot be said that such obscene image is published. Even a respite cannot be taken in the case of sending cyber pornography by email from the provision of *section 170* of the Criminal Code which deals with sending or attempt to send obscene materials. *Section 170(b)* of the code provides that any person who knowingly sends, or attempts to send, by post anything which encloses an indecent or obscene print, painting, photograph, lithograph, engraving, book, card, or article, which has on it, or in it, or its cover any indecent, obscene, or grossly offensive words, marks, or designs, is guilty of a misdemeanor, and is liable to imprisonment for one year.[105] Even if the provision is adapted to cyber pornographic material, such material sent through email may create a problem of jurisdiction if the email is sent from another jurisdiction, because the provision of the code is limited to act done partially or wholly within Nigeria.

---

[99] See section 383 of the Nigerian Criminal Code, op. cit.
[100] See R v. Lloyd [1985] 2 All E.R. 661.
[101] Section 233D of the Nigerian Criminal Code Act, op. cit.
[102] Section 233D(1) of the Nigerian Criminal Code.
[103] Oxford Advance Learner's Dictionary of Current English, 6th ed. A. S. Hornby, Oxford University Press.
[104] Ibid.
[105] Section 170(b) of the Nigerian Criminal Code.

The above observations notwithstanding, the punishments prescribed for the offences relating to obscene material in the *Criminal Code* are too simple for cyber pornography given the expediency of the internet in distributing materials and the speed at which information can be sent through the medium.[106] It is therefore important from the foregoing that cyber pornography needs to be separately addressed to deal with the technicalities that may be involved in the offence.

NEED FOR CYBERCRIME LEGISLATION

The need to have separate cybercrime specific-legislation has been given credence by a school of thought. This is for example revealed in the dictum of Warren B. Chik who said in one of his works that:

> Although cyber crimes are generally an extension of traditional crimes in that the electronic media is a relatively new instrument by which traditional offences are carried out, that does not mean that existing laws are adequate or even appropriate to deal with these new scenarios in terms of coverage or public policy. Moreover, as we have seen, there are more unique problems that relate to cyber more than they do to real world crimes, in particular, jurisdictional and enforcement issues.[107]

Accordingly, there is a "lost in transmission" phenomenon when it comes to country practices in updating traditional penal laws in a piecemeal, statute-by-statute manner to cyberspace transactions. This probably happens whenever the process of augmentation is either slower than developments in cybercrime techniques or technology used to further such offences, or is fraught with mistakes or is immediately outdated due to the speed of developments in this area.[108]

---

[106] Section 170 of the Criminal Code provides for a maximum of one year imprisonment for sending or attempt in sending indecent or obscene materials, while section 233D(1) of the Code provides for a fine of four hundred naira or imprisonment for a term not exceeding three years or both

[107] Warren B. Chik "Challenge to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore." Available at http://www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc Accessed 3 June, 2011. The jurisdictional issues will be treated later in this work.

[108] Ibid.

[109] Ibid.

Situations like this will always lead to lacunas in the law which cybercriminals can take advantage of.
As regards this situation Warren Chik also observed as follows:

> Even where there is coverage (by traditional crime legislation), it does not mean that the punishment suits the crime as some of the existing provisions may contain penalties that are outdated or that fail to achieve other social policy objectives such as in deterring or preventing further offences or in punishing or rehabilitating offenders.[109]

This dispute could be resolved in favour of the class that believed cybercrime specific statutes should be enacted, especially in order to avoid unnecessary technical quibbles of bringing acts committed through the use of computer under traditional crime laws, which prompted many nations to embark on the journey of enacting new and separate laws to tackle the nascent cybercrime. In addition to the increased scale cybercrime offers to criminal activity, it also has a tendency to evade traditional offence categories. While some cybercrime consists of using computer technology to commit traditional crimes such as fraud and theft, it also manifests itself as new varieties of anti-social activity that cannot be prosecuted using traditional offence categories.[110] The dissemination of the "Love Bug" virus illustrates this: the suspected author of the virus could not be prosecuted under the available offences prescribed under the Philippines Penal Code because none of them encompassed the distribution of a computer virus, even one which destroyed property (e.g., computer files) and stole passwords.[111]

A better example is a denial-of-service-attack, which cannot be prosecuted as vandalism, trespass, burglary, theft, arson or extortion, even though it is a malicious activity that damages, perhaps even destroys, the victim's ability to conduct business.[112]

---

[109] Ibid.
[110] Ibid, p.21.
[111] Ibid.
[112] Eric J. Sinrod & William P. Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws," Vol 16, (2000), SANTA CLARA COMPUTER & HIGH TECH. LAW JOURNAL p.177, at 194.

Moreso, the Council of Europe's Committee of Experts on Crime in Cyberspace stated that:

> . . . The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. . [113]
> .

Prior to the enactment of computer misuse statutes the practice was to seek remedy through the existing enacted laws which are meant for traditional types of crime. This practice was not without its attendant challenges. The prosecutors were wont to bring their charges for computer misuse under existing property crime laws, such as laws prohibiting trespass, burglary, and theft. It will appear that the same forms of actions that apply in the real world are also applicable in the virtual world without more, and these actions may culminate into the same effects. However, proper analyses of actions in the two worlds will reveal the dissimilarities between the two. The trespass crime [114] involves making intentional personal entry into property owned or occupied by another person without the person's permission.[115] Similarly, unauthorized access, otherwise called 'illegal access' and 'computer trespass' can be defined as the "access without right to a computer system or network by infringing security measures". [116] This act of infringement may occur where an actor, for instance, enters into a target's files or programs without permission. [117]

---

[113] Council of Europe, Committee of Experts on Crime in Cyber-Space, Explanatory Memorandum to The Draft Convention on Cyber-Crime, p.1-6 (May 25, 2001), Available at http://conventions.coe.int/Treaty/EN/cadreprojets.htm. Accessed 12 December, 2011.

[114] Trespass does not constitute a crime under the Nigerian law, rather is it a civil wrong under the law of torts which is basically regulated by the common law system in Nigeria.

[115] Kodilinye, G. The Nigerian Law of Torts 4th Impression (Nigeria: Spectrum Law Publishing, 1997), P.178.

[116] Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Vienna, 10-17 April 2000, UN Docs A/CONF. 187, at p.15.

[117] Rizgar, M. K. "The Offense of Unauthorized Access in Computer Crimes' Legislation – A Comparative Study", Journal of Sharia and Law, Issue No. 40- Rajab 1430 H- October 2009, p. 42. Available at http://sljournal.uaeu.ac.ae/en/issues/40/images/3%20%20English.pdf Accessed October19, 2011. (PP. 39-65).

This definition is wide enough to accommodate a wide range of computer misuses which can be prosecuted under unauthorized access.[118]

A quick glance at the ingredients of trespass and burglary may seem to give the same legal implications to unauthorized access to computer as a computer misuse offence. Hacking, for instance, is analogous to trespass. In both, the offender gains physical access to a prohibited area a physical area in trespass and a virtual area in hacking. In the same vein, a hacker may gain access into a computer with the intent of committing a crime therefore having similar content with burglary in which an offender breaks into a house.

There is a technical difference in the way the traditional laws are being applied to traditional offences like trespass and burglary which makes such application unpleasant for computer misuses. In the first place, trespass and burglary statutes are primarily created for offences committed in the physical world without the virtual world in the minds of the draftsmen, and thus, they have not been used to prosecute computer misuse.[119] For example, the offences of trespass and burglary require that part of the body of the offender or the instrument used has entered the premises.[120] The offences of trespass and burglary focus on the location of the offender in the physical world and do not cover computer misuse as the user does not physically enter the target computer.

The offence of theft is hinged on the defendant taking property that belongs to another. Most theft statutes provides for intention to cause permanent deprivation of a person of his proprietary interest in a "thing" for the offence of theft to be committed. Property under the theft statutes may also be categorized as tangible (e.g. a car) and intangible property (e.g. a chose in action). It has been held that computer system itself constitutes a property,[121]

---

[118] Such misuses include, inter alia, hacking and dissemination of computer viruses, and both criminal acts are subject to unauthorized access statutes in the United States and the United Kingdom. Hacking is defined as "gaining unauthorized access to a computer system either for the purpose of exploration or for causing damage once inside". See Marc D. Goodman & Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace, Vol.10, (2002), International Journal of Law and Information Technology, p.139 at 146. Available at http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf Accessed October 19, 2011. (pp. 1-153).

[119] Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", New York University Law Review, Vol.78, No.5, (November 2003), p.1607. Available at http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-78-5-Kerr.pdf Accessed October 19, 2011. (pp. 1596- 1668).

[120] For burglary, see section 410 of the Nigerian Criminal Code, LFN 2004,

[121] See United States v. Collins, 56 F.3d 1416, 1420 (D.C. Cir. 1995). Here the court held that federal conversion statute prohibits the conversion of computer time and storage.

likewise the data stored in it [122] and computer password. [123]

Even to ascribe property to some aspects of computer misuse offences may seem adequate in some instances, it is not always tidy for such reasoning to be sufficient for all the instances of computer misuse. For instance, where the owner is being denied of his interest in a password, as in the case of password theft, it can readily fit into the offence of theft, though an intangible property was involved. However, it is not very clear if a denial-of-service attack can key into a situation where the owner is permanently denied of the use of his property in the computer system. In another breath, copying of data from a computer would not seem to have permanently deprived the owner of the property as the property still remains intact, only a copy of it was made. [124] It is therefore doubtful if a theft statute can adequately take care of computer misuse offences.

Another important aspect of computer misuse is 'fraud'. The use of such term as 'fraud' may be quite misleading in computer use as the activities commonly regarded as computer fraud can involve criminal offences other than those notoriously considered as fraud. [125] The provisions of the available criminal law statutes for the offence of fraud make 'deception' a necessary ingredient for such an offence to be committed.

Can it then be said that a person who ordinarily should not have access to a particular service on a website has committed a fraud by using a technical means, for example by by-passing security code, to enter into the website to enjoy such service? Thus, computer is a machine and it is hard to subject it to deception. Lord Morris in *DPP v. Ray* [126] held that for deception to take place there must be some person or persons who will have been deceived.

It is seen that where a user is dealing with a computer directly without any other person sitting at the other end of the terminal, the user is having a deal with the computer and not any other person, therefore an offence of fraud cannot be committed on such computer following strictly the provision of *section 15(1)* of the *Theft Act 1968.*

---

[122] See United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) where the court held that information viewed from inside a computer is property under the wire fraud statute.
[123] See United States v. Girard, 601 F.2d 69, 71 (2d Cir, 1979).
[124] See United States v. Seidlitz op. cit. where copying of software was held not to be a denial of property in the software.
[125] David Bainbridge, op. cit., p. 370.
[126] [1974] AC 370.

The inability of the traditional crime statutes to adequately deal with computer misuses led to agitations for creating separate statutes for these new brand of offences. Therefore, computer crime legislation was canvassed for. [127] It was argued that new and specific laws were needed because such laws will avoid the legal fictions of having to use other criminal statutes that were not meant to apply to computer crimes to them, and that these new laws would make it possible to convict criminals for their explicit acts.[128]

The harm of computer misuse is distinct in nature compared to traditional crimes because there is interference with the intended function of computers by either exceeding or denying intended privileges, and the existing laws had no clear remedy for many instances of misuse.

CONCLUSION

In conclusion, crime is a product of the law and cannot be seen as a mere exercise of moral valuation. As discussed above, definition of crime presupposes a legal authority who pronounces an act or omission a crime through law which is an instrument of the State. In this light, "cybercrime" in Nigeria is not yet a crime recognized under her law apart from some types of crimes that can be committed through computer network and can also be committed traditionally without the use of computer network. Therefore, "cybercrime" needs the response of the law in Nigeria to make it a recognized crime. This means that for there to be a cybercrime law in Nigeria it has to pass through the normal legislative process.

Cybercrime has posed peculiar challenges which are difficult for the traditional crime laws to address with relative ease and adequacy. Amending extant traditional crime laws to accommodate the daunting cybercrimes peculiar challenges may not bring about the desired result of successfully blocking every available avenue for cybercriminals who may want to exploit the weaknesses and loopholes in the law. Moreover, the rate of development of techniques of perpetrating cybercrime may be too fast and puzzling for extant criminal law to address in accurate details.

It can be seen from the above discussion that although existing laws can pretend to cover electronically perpetrated crimes, they are not suitable, appropriate or relevant for the following reasons, among others:

---

[127] Such agitations were made by scholars and legal commentators in the late 1970s and early 1980s.
[128] Orin S. Kerr, op. cit., p. 1614.
[129] Orin S. Kerr, op. cit., p. 1615.
[130] Warren, B. C. "Challenges to Criminal Law Making in the New Global Information Society: A Critical Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore". Op. cit.

1. the punishments are generic and inadequate to meet public policy objectives such as crime prevention and control as well as the maintenance of integrity and information technology networks;
2. jurisdiction is confined to acts perpetrated within the country and territorial jurisdiction is the rule adopted by the courts in trying such offences, except in limited circumstances;
3. some provisions are rendered inapplicable due to antiquated definitions of key elements or words.

It is therefore imperative for Nigeria and other nations who have not enacted laws to address cybercrime to adopt cybercrime-specific legislations which can take care of the technicalities of this pecular form of crime and are pliable enough to address any new techniques of perpetrating cybercrime. This flexibility cannot be addressed by the extant traditional crime law otherwise it might lose its originality and technical flavours.