AFRICAN JOURNAL OF LAW AND CRIMINOLOGY

AJLC Volume 5 Number 1 (2015) 47-58
ISSN 2045-8525 (Online) ISSN-2045-8401(Print)
Publishers: Sacha & Diamond, England, United Kingdom
Website: www.sachajournals.com
Paper Status: Priority Peer Reviewed, Accepted and Published

HACKING: THE NEW FACE OF CYBERCRIME IN NIGERIA

IFEANYI-AJUFO, Nnenna[1]
and
OBALUM, Dike Chijioke[2]

[1]Faculty of Law, Baze University, Abuja, Nigeria
[2]National Open University of Nigeria, Nigeria

ABSTRACT

The digital age, though welcome on many fronts has brought on its heels a myriad of ills. As at 2011, there were nearly 2 billion internet users and over 5 billion mobile phone connections worldwide and about 294 billion emails and 5 billion phone messages were exchanged.[1] Most people around the world now depend on consistent access and accuracy of these communication channels,[2] where almost all our traditionally recognized dealings, are being done, thus attracting so many cyber crimes including hacking. This paper will analyse the threat of 'Hacking'[3] having become a huge concern for the law and presently trending, as the new face of cybercrime particularly for a jurisdiction like Nigeria with little or no cyber crime laws.

Keywords: Criminality, Hacking, Cyber crime, Nigeria

1. INTRODUCTION

In 2014, a United States (US) security firm uncovered what appeared to be the largest Internet security breach in recent memory, conducted by a group of Russia-based hackers.[4] According to a Milwaukee-based firm, Hold Security, which conducted an 18-month investigation into the breach, the online gang stole 1.2 billion username and password combos, as well as more than 500 million email addresses.[5] The hackers pulled off the data heist, which ultimately scooped up 4.5 billion records, using unsuspecting systems of network victims (in this case, computers with viruses that allowed a single operator to control a large group of affected systems) to test websites for vulnerabilities.[6] Once vulnerability was discovered, the hackers were able to execute injections, enabling them to send malicious commands to a website and steal its data, including usernames and passwords. The group managed to steal

[1] EUROPOL Public Information 'Internet Facilitated Organised Crime'. (The Hague: File No. 2530-264, January 2011)
[2] Office of Cyber Security and Information Assurance in the Cabinet Office. 'The cost of cybercrime', https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf Accessed 12/01/14
[3] Mine for emphasis
[4] British Broadcasting Corporation. 'Russia Gang Hacks 1.2 Million Usernames and Password. Available on: http://www.bbc.com/news/technology-28654613 Accessed 12/01/15
[5] Ibid
[6] Ibid

information from 420,000 web and sites.[7] Accounts were hacked and credentials were stolen every day; however, the number of credentials reportedly stolen in that instance was on a massive scale.[8] This is just one of the many numerous stories related to hacking in contemporary times and it is a huge wake-up call to consumers and companies, but most importantly, to jurisdictions like Nigeria with little or no laws to tackle cyber crimes like hacking.

Today, Processes that were once done manually are accomplished with a simple click or two and various cumbersome events are performed effortlessly in every facet of life by one click. One click can affect millions of people positively or negatively across cultural, regional and national divides. This and the speed at which the world is being digitized means that dependency on computers and their programs, the internet and electronic communication across the board has increased.

Presently, many factories, hospitals, schools, governments, and business offices are totally dependent on computer programs and any slight anomaly can cause grave havoc which may shut down entire systems or cause problems that may not be solved for a long time; in addition to this a huge amount of money is spent on preventing hacking attacks or clearing problems created by hacking. The effect of computer hacking is quite detrimental in exploiting information like personal data, social security numbers, credit card numbers, bank account data and personal photographs. That is why the law has become very interested in tackling hacking. Hacking has become an issue in legal systems because of its new-face when compared to other traditional offences.

The word 'hack' is regarded as a clever solution to a restriction[9]. It is regarded as a crime that entails cracking systems, breaking security features and gaining unauthorised access to the data stored in them.[10] Hacking is the deliberate and unauthorized access, use, disclosure, and/or taking of electronic data on a computer.[11] Hacking is also an act of modifying computer hardware or software, in order to cause damage to sensitive data on a computer or to simply steal confidential information.[12] Again, hacking is the act of breaking into computer systems, usually with the intention of altering or modifying existing settings.[13] Hacking has also been described as gaining unauthorized access to somebody's computer system in order to secretly find a way of looking at and/or changing information on that system without permission.[14] Hacking also refers to unethical use of technology for gaining access to sensitive information on a computer, thereby hampering the security and privacy of a computer.[15]

Hacking is presently classified as a cybercrime. The crime is committed when a person willfully, knowingly, and without authorization or without reasonable grounds to believe that he or she has such authorization, attempts, or achieves access, communication, examination, or modification of data, computer programs, or supporting documentation residing or existing internally or externally to a computer, computer system, or computer network.[16] The following categories of people may be referred to as hackers[17]

---

[7] Ibid

[8] Ibid

[9] Asholu, D and Oduwole, OA (eds). *Policing Cyberspace in Nigeria* (Ibadan: Lifegate Publishing, 2009) p . 84

[10] Ibid.

[11] Verma, A. *Cyber Crimes and Law* (Allahabad: Central Law Publications, 2009)

[12] Oak, M. 'What are the effects of Computer Hacking' Available on: http://www.buzzle.com/article/what-are-the-effects-of-computer-hacking.htm >accessed 20/12/ 2014

[13] National Conference of State Legislators. 'Computer Crime Statutes' Available on: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx accessed 20/12/2014

[14] Oxford Advanced Learner's Dictionary 7th Edn (Germany: Cornelsen, 2010)

[15] Ibid

[16] Federal Bureau of Investigation. '*FBI Computer Crime Survey 2005' Available* on: www.fbi.gov/publications/ccc2005.pdf. accessed 19/12/2014

[17] Raymond, E. *The New Hackers Dictionary* (U.S.A: MIT Press, 1997)

a) A person who explores already programmed systems to determine their capabilities and strength.
b) A person who breaks limitations
c) A person who gets information by poking around

While most people associate hacking with breaking the law and assume that everyone who engages in hacking is a criminal, it has been argued that in fact hacking is more about following the law than breaking it, because it involves applying the skills of new inventions for solving computer problems. According to Ericson[18] "hacking is more about following the law than breaking it. Its essence is finding unintended or overlooked uses for the laws and properties of a given situation and then applying them in new and inventive ways to solve a problem"[19]. Thus Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent and earning 'bragging rights'.[20] For levy[21] hacking was first an engineering accomplishment in hardware, which later came to take on the meaning of an original and efficient programming solution to problems in software. A hack has also been regarded as an inelegant but effective solution to a programming problem; though it is what we call a necessary evil; it is widely admired for its efficiency and fast motion.[22] Thus, hacking is more of an entertainment in most places where breaking into secured computer systems is no news, and the hacker successfully gains access to the computer at will, much to his excitement and with no fear of being caught by the law.

The Convention on Cybercrime[23], makes it an offence to intentionally, and without authorization, beyond authorization or without reasonable grounds to believe that a person has such authorization, intercept, download, copy or extract by technical means, any non-public transmission of computer data, including electromagnetic emissions, in whole or in part from or within a computer, computer program, computer system, or computer. The U.S. Department of Justice (DOJ), in its manual on computer crime, defines such crime as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution."[24] In essence hacking is a form of trespass, it is Illegal access and has come to be regarded as a cybercrime.

[18] Erickson, J. *Hacking: The Art of Exploitation* 2nd edn (San Francisco: No Starch Press, 2008)
[19] Ibid
[20] Levy, S. *Hackers: Heroes of the Computer Revolution* 1st edn (California: O' Reilly Media, 2010)
[21] Ibid
[22] Alleyne, B '"We are all hackers now": critical sociological reflections on the hacking phenomenon'. (2011) Under Review, pp. 1-32. Goldsmiths Research Online p.2 tp://research.gold.ac.uk/6305/1/Alleyne__We_are_all_hackers_now__critical_sociological_reflections_on_the_hacking_phenomenon.pdf> Accessed 19/01/2015
[23] Council of Europe. Convention on Cyber Crime, 2001 Article 7 States that "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches". Article 8 also states that "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by : (a) Any input, alteration, deletion or suppression of computer data; and, (b). Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
[24] Parker, DB. *'Computer Crime: Criminal Justice Resource Manual'* (U.S. Department of Justice. National Institute of Justice: August 1989) Available on: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf. Accessed 12/01/2015

The first form of hacking was recorded in 1903 when magician and inventor Nevil Maskelyne disrupted John Ambrose Fleming's public demonstration of Guglielmo Marconi's purportedly secure wireless telegraphy technology, sending insulting Morse code messages through the auditorium's projector.[25] In the 1960's, malicious hacking now started with compromising telephone systems and the stealing of telephone services which in no time spread to computers and networks.[26] Since then, hacking has evolved and refers to multiple activities including breaking passwords, creating e-mail bombs, denial of service attacks, writing and releasing viruses and worms, viewing restricted electronically-stored information owned by others, URL redirection, adulterating Web sites, or any other behaviour that involves accessing a computing system without appropriate authorization. Although for the most part hacking is restricted to computers, it may be extended to fraudulent activities relating to telephones (e.g. "phreaking"), credit cards (creating gadgets to "steal" the magnetic code stored on credit cards and copying it on to others), subway passes (adulterating passes or pass readers to enable unlimited free rides), parking meters (rigging parking meters to allow unlimited free parking) or virtually any other item with electronic components.

2. CONCEPTUAL FRAMEWORK

The international nature of cyber crime results in the involvement of not only the target region, but also other countries or regions different from where the attacks originate.[27] In the year 2000, a mass-mailed computer virus affected nearly 45 million computer users worldwide. [28] By 2010, politically motivated cyber crime had penetrated global cyberspace[29]. A major attack came from a complicated computer worm Stuxnet which infected a large number of industrial controls worldwide. It was able to give false machinery instructions, subsequently leading to nuclear malfunctions and break-down operations at gas pipelines. The worm's target location was believed to be Iran, but it also affected Indonesia, India and Pakistan[30] causing untold losses. With incidents such as the hacking of Yahoo, Amazon, Google and Wikileaks disclosures, hacking has become a huge concern for the Law. The cost of hacking is incalculable to the victim be it an individual, corporate entity or government. All over the world, government spending on prevention of hacking has increased. In February 2011, the United Kingdom (UK) government allocated 63 million pounds ($100 million) to build upon the existing expertise within the UK Serious Organised Crime Agency (SOCA) and the Metropolitan Police Central e-Crime Unit.[31] Similarly, in 2012, the US Pentagon increased its budget to protect military networks, to $3.2 billion.[32] This is not surprising in view of the fact that in 2009, computer hackers broke into the Pentagon's $300 billion Joint Strike Fighter

[25] Marks, Paul 'Dot-Dash-Diss: The Gentleman Hacker's 1903 Lulz' *New Scientist*, December 27, 2011 <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html#.VOx9wPvPGwE>accessed 16/01/15

[26] Chirillo, J *Hack Attacks Encyclopedia: A Complete History of Hack, Cracks, Phreaks and Spies* (Canada: John Wiley, 2001) p. 1

[27] KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor.* Vol 8 July 2011 <https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf> Accessed 17/01/2015

[28] Ibid p. 6

[29] Information Age 'National insecurity' January 26, 2011 in Ibid p. 7

[30] 'Stuxnet Worm Causes Worldwide Alarm', *Financial Times,* September 23, 2010 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor.* See footnote 27

[31] United Kingdom Public Services, '*£63m to tackle UK cybercrime',* February 15, 2011 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor* .See footnote 27

[32] 'Pentagon seeks $3.2 billion for revised cyber budget', Next Gov, March 24, 2011 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor* .See footnote 27

project, F-35 Lightning II. The F-35 program has been the costliest weapons program ever. As hackers carefully encrypted the stolen data, investigators were unable to determine the amount or nature of the lost data.[33] Canada has also been a victim of a cyber attack. In January 2011, hackers infected computers in two Canadian Government departments, leaving many officials without internet access for nearly two months.[34] In March 2011, the computer network in the European Union (EU) headquarters was targeted by hackers, prior to an EU leaders' summit on economic reforms and current affairs.[35] In December 2010, hackers broke into computers at the French Finance Ministry and stole sensitive information related to the G20 Summit that was to be held in France in February 2011. The criminals took control of nearly 150 computers at the French Finance Ministry, and accessed many documents that had sensitive information on the G20 summit.[36] Nigeria is not left out yet one would wonder if the Nigerian Government is even aware of the existence of hackers and the effect of hacking.

2.1 Types Of Hacking

There are lots of classifications of hackers which include[37]

(a) The white hat hacker; this hacker breaks computer security for no criminal intent. It is often done by law enforcement agents in a bid to tackle crimes and by individuals working for security companies that make security software. [38]This classification includes those who perform penetration tests and vulnerability assessments within their contractual agreements. White hat hackers see hacking as an art form. They feel hacking is often misunderstood.[39] Thus, they are benign hackers with no malicious intent.

(b) The black hat hacker; this hacker violates computer security for little more reason beyond maliciousness.[40] They are the worst of all computer criminals. They break into the security network to destroy data or make the network a little more problematic for those authorized to use the network, they maliciously sabotage computers, steal information located on secure computers and cause disruption to networks for personal or political motives.[41]

(c) A grey hat hacker; this is a combination of a black and white hacker. This hacker, hacks into a computer network for the purpose of notifying the administrators about a defect and offer to correct it usually for a fee.[42]

(d) Script kiddie; this involves a non expert who breaks through computer systems by using pre-packaged automated tools written by others and he usually knows little or none of how the computer system operates.[43]

(e) Clandestine hacking: A clandestine hacker's activity includes breaking and entering, intelligence gathering and technical attacks designed to make systems malfunction.[44] For

[33] 'Computer Spies Breach Fighter-Jet Project', WSJ, April 21, 2009 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor* .See footnote 27

[34] 'Canada Hit by Cyber attack', New York Times, February 17, 2011 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor.* See footnote 27

[35] 'EU Headquarters Under Cyber Attack Before EU Leaders Meeting,' Bloomberg, March 24, 2011 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor.* See footnote 27

[36] 'Cyber attackers target G20 documents', Financial Times, March 7, 2011 2011 in KPMG International Cooperative 'Cyber Crime - A Growing Challenge for Government'. *Issues Monitor.* See footnote 27

[37] 'Types of Hackers and How Hackers are Classified' Available on: http://www.omnisecu.com/ccna- security/types-of-hackers.php Accessed 16/01/2015

[38] ibid

[39] Op cit. Erickson, J

[40] See footnote 37

[41] *Burleson v State*. 502 S.60 2d, (182 Tex. App. 1991)

[42] See footnote 37

[43] Ibid

some clandestine hackers, a usual break through into government computer networks is more of an achievement in itself while others see it as a step to gathering information to crack systems.[45] These sorts of hackers, often include anti-government criminals, as well as terrorists, and their activities are directed largely against the infrastructure of states and corporate computer systems.

(f) Open hacking; an open hacker unlike those who aim to break into security systems, are more interested in sharing their hacking work. Open hacking is built on sharing knowledge and resources and their practice is done in the open.[46] Those who work in free and open software systems are more prone to open hacking activity. According to individuals like Raymond,[47] an advocate of open hacking, the fundamental principle of hacking is that hackers, and others, are better off if the information is freely shared, thus hacking should be open. Those hackers who fall within this category believe in sharing information with their counterparts no matter where they are.

(g) Hacktivism; as the term implies 'hacktivist' combines both a hacker and activist. It also manifests in various other forms; attacks on websites in order to deny access to users, editing the content of websites to fit his aim of hacktivism, using the internet communication channels and more recently social networking to share information not meant to be there for the purpose of denying the user his privacy.[48] It was only in 2010 that hacktivism came to be known with the leaking of a US department documents by wikileaks.

There has been a tendency to divide hacking practice into a good/evil dichotomy.[49] Moreover, how particular hacking activities are read in moral or ethical terms is as much dependent on the perspective of the person doing the reading as, it is on the actual content of the practices under scrutiny that the clear intentions of the hacker in question can be understood.[50]

3. HACKING IN THE NIGERIAN JURISDICTION

Hacking is Illegal access. In essence, it is a form of trespass which involves both civil and criminal liability. The first part which is a criminal action aims at punishing hacking by way of imprisonment, fine or both. While civil action is employed to claim tortuous liability by way of compensation. Hacking like other traditionally recognized crimes is not only punishable, but also tortuously redressible before the law.

Nigeria is an extremely high risk country in cyber crime issues. She ranks third in the world in the commission of cyber crime. Nigeria in comparison to other countries has a large number of ongoing cyber crimes with very few successful investigations and hardly any prosecution. Many Nigerians including government officials seem to think that cybercrime only involves using the internet to swindle unsuspecting individuals. The target of law enforcement officials is mainly those who acquire money fraudulently and dupe others; particularly people living overseas via the use of the internet. There is a really low level of education amongst Nigerians in relation to cybercrimes. The reality today is that somebody in Nigeria could sit at a computer in Nigeria and hack into a computer in Austria thereby causing cross border crime.

---

[44] Chiesa, R *et al. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (Milan: Auerbach Publications, 2008)

[45] ibid

[46] Alleyne, B '"We are all hackers now": critical sociological reflections on the hacking phenomenon'. (2011) Under Review, pp. 1-32. Goldsmiths Research Online at: http://research.gold.ac.uk/6305/1/Alleyne Accessed 19/01/2015

[47] Raymond, E S, & Guy, L S *The New Hacker's Dictionary 3rd edn* (London: MIT Press, 1996)

[48] Op cit See footnote 37

[49] Op cit See footnote 46. http://research.gold.ac.uk/6305/1/ Accessed 19/01/2015

[50] Ibid

Truth is, successful hackers, could in one click wreck governmental, economic and financial systems in a country.

To the public, a hacker is seen as one who breaks into other's computer systems. Like other arts hackers believe information should be free and anything that comes in their way of freedom shall be destroyed or broken. This act has advanced into different ugly forms of crimes one of which is cyber murder. Hacking can also degenerate to acts of terrorism. Another noteworthy fact is that this hacking issue can be seriously malicious and at the same time seriously detrimental to the state.

The undetected entry of a hacker in and out of secured documents is enough nightmares to the government officials. Various laws concerning the crime of hacking exist in the International legal systems which are as yet sadly lacking in the Nigerian legal system. In the US, for instance, there are lots of laws forbidding hacking which includes 18 U.S.C 1029[51], which concentrates more on devices that gives hackers, unauthorized access to computer software with the intent to defraud and 18 U.S.C 1030[52] which deals with computer trespassing, especially hacking into a government computer. In 1986, Congress enacted the Computer Fraud and Abuse Act (CFAA) as an amendment to the existing computer fraud law, which had been included in the *Comprehensive Crime Control Act of 1984*. It was written to clarify and increase the scope of the previous version of 18 U.S.C. 1030 while, in theory, limiting Federal jurisdiction to cases with a compelling federal interest, where certain financial institutions are involved or where the crime itself is interstate in nature. In addition to clarifying a number of the provisions in the original Section 1030, the CFAA also criminalized additional computer-related acts. Provisions addressed the distribution of malicious code and denial of service attacks. Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.[53] The Act has been amended a number of times in 1989, 1994, 1996, and in 2001.[54] Another law in the US is the *Computer Software Privacy and Control Act, which* was created to prevent deceptive software transmission practices in order to safeguard computer privacy, maintain computer control, and protect internet commerce. In addition to laws specifically tailored to deal with computer crimes, traditional laws can also be used in the US to prosecute crimes like hacking involving computers. For example the Economic Espionage Act (EEA) created in order to put a stop to trade secret misappropriation and the Electronic Communications Privacy Act[55] (ECPA) passed in 1986, as an amendment to the Federal Wiretap Law.[56] The Act made it illegal to intercept stored or transmitted electronic communication without authorization.

Part of the *Fraud and Related Activity in Connection with Computers Act*, section 1030 (a) (1) in particular, makes it illegal to access a computer without authorization or in excess of one's authorization and obtain information about national defense, foreign relations, or restricted data. It is worth noting that section 1030 (a) (1) requires proof that the individual knowingly accessed the computer without authority or in excess of authorization for the purpose of obtaining classified or protected information. Section 1030 (a) (1) criminalizes the use of a computer to gain access to the information, not the unauthorized possession of it or its transmission. Another act that deals with hacking is the National Information Infrastructure Act (NIIA) which was passed in 1996 to expand the CFAA to encompass unauthorised access to a

[51] United States Code. Title 18, Part 1, Chapter 47, Section 1029 Fraud and Related Activity in Connection with Access Devices

[52] United States Code. Title 18, Part1, Chapter 47, Code 1030 Fraud and Related Activity in Connection with Computers

[53] Hitchcock, J A. 'Net Crimes & Misdemeanors' *Information Today, Inc.* (2002) Available on: <http://www.infotoday.com/pressreleases/pdf/051206_NetCrimes_2ndEd.pdf>Accessed 12/02/2015

[54] by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution

[55] Electronic and Communications Privacy Act, 1986. 18 U.S Code 2510

[56] United States Code 18, Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications.

protected computer in excess of the parties' authorisation. Other laws in the United States pertain to hacking include the Computer Misuse Act 1990, Communication Decency Act of 1998, No Electronic Theft Act of 1997, 17 U.S.C. Section 506 (a) and Data protection Act of 1998 amongst others.

The United Kingdom has the Computer Misuse Act of 1990. Under the Computer Misuse Act it is an offence to hack into somebody else's computer or send them a form of virus that allows them to obtain information from somebody else's computer.[57] The reasoning for the introduction of this Act was the fear that individuals might be able to obtain information about other individuals without their knowledge or consent.[58] Individuals should be entitled to keep what they have on their computer private and only allow others to use it by giving their consent and companies have the paramount need to store confidential data or keep intellectual property rights securely.

In Nigeria where there is still no conclusive legislation on hacking, hacking would be mostly related to criminal trespass found in the Criminal Code and the Penal Code.[59] Whether the content of the codes can apply to hacking is yet to be proved, because intangible things like data stored on computer systems may not qualify as property for the purpose of the offence of criminal damage[60]. To prove criminal trespass in Nigeria, the ingredients of unauthorised entry into or upon property against the will of the person in possession or lawfully obtaining entry but wrongfully remaining thereon with the intention to commit a felony must be satisfied.[61] The crime of trespass under the Nigerian Criminal Code and the Nigerian Penal Code is applicable only where no damage occurs and where there is a malicious damage of a property, it becomes insufficient to apply sections 442[62] and 451[63] of the Criminal Code because property includes animate and inanimate objects for which data that is stored on computer systems will not qualify as property for the offence of criminal damage.[64]

The very basis of laws is the definition of terms and there is no uniformity as to most definitions of cybercrimes. For example The Council of Europe Convention on Cybercrime[65] includes a provision in Article 2 on illegal access protecting the integrity of computer systems by criminalizing unauthorized access to a system. Noting inconsistent approaches at the national level,[66] Article 2 also requires that the offender carries out the offences intentionally.[67] The Convention does not contain a definition of the term "intentionally". In the explanatory report, the drafters pointed out that "intentionally" should be defined at national level[68]. Thus, what is intentional in one country may be unintentional in another.[69]

The very nature of cyberspace poses a number of challenges to the implementation of cyber related regulations in any country. For hacking, there are no borders for the perpetrators

[57] MacEwan, N 'The Computer Misuse Act 1990: Lessons From its Past and Predictions for its Future'(2008) 12 Criminal Law Review 955-967

[58] Ibid

[59] Section 442 and 451 of the Nigerian Criminal Code Cap 77 LFN 1990 and Section 342 of the Nigerian Penal Code Cap 89 LNN 1963

[60] *R v Gold& Schrifreen* (1988) AC 1063

[61] Op Cit Asholu, D and Oduwole, OA p.88

[62] According to S. 442, " The term "damage" used in relation to a document, or to a writing or inscription, includes obliterating and rendering illegible, either in whole or in part".

[63] According to s. 451, "Any person who wilfully and unlawfully destroys or damages any property is guilty of an offence, which, unless otherwise stated is a misdemeanour, and he is liable, if no other punishment is provided, to imprisonment for two years."

[64] Op Cit Asholu, D and Oduwole, OA p. 90

[65] Council of Europe ETS No. 185 Convention on Cyber Crime 2001

[66] *Schjolberg*, S ' The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries'(2003) Moss District Court, Norway. Available on: <http://www.mosstingrett.no/info/legal.html > accessed 01/02/2015

[67] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

[68] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

[69] Op cit Schjolberg, S

and victims, but political boarders dictate the laws in each sovereign state and the laws are certainly not uniform.[70] Furthermore, cyber criminality is continuously evolving, making it more challenging for governments and investigation of cyber crimes are complex, as the criminal activity it is borderless by nature.

There is also the problem of jurisdiction with a lack in international laws to address the jurisdictional issue. The issue of jurisdiction is a huge concern for the law in Nigeria because a hacker may commit a crime by just clicking his computer to commit crime in another country, making the prosecution of a hacker more of an impossible task and a more difficult process because the petition has to be made to a country to extradite the suspect which may also take a longer time. For instance the case of Gary McKinnon which started in 2002 but only came to an end in 2007[71]. Hacking has really become an issue when it comes to questions of jurisdiction, for the internet is a gateway for a computer to connect to the world, as such, courts find it somehow impossible to address issues concerning hacking. The trouble with internet jurisdiction is the multiple parties in various parts of the world who have only a virtual nexus with each other.[72] If a party wants to sue the other, where does he sue? This is difficult to establish due to the lack of physical boundaries. The decision in *CyberSell Inc v Cybersell Inc*[73] is a typical example. The court had to decide whether the mere use of a website of the Florida Corporation was sufficient to grant the court in Orlando Jurisdiction. The 1996 case of *United States v. Thomas*[74] brought to the limelight the question of jurisdiction in cybercrime when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. Also, there is the question of foreign judgements and whether they can be enforced in other countries. In the famous case of *Yahoo! Inc. v La Ligue Contre Le Racisme et L'antisemitisme*[75] the court in France directed Yahoo! to remove all links and materials pertaining to Neo Nazism on its web site which Yahoo! challenged in the United States saying that its enforcement would be a violation of the first amendment of the United States Constitution. The U.S Court recognised the powers of the French court, but refused to enforce the order. Though Yahoo! later removed the offending articles it was not due to the orders of the French court. This is significant in that it exemplifies a situation where a foreign court assumes preliminary jurisdiction to hear a matter concerning a web entity located outside its physical boundaries, because the content of the site is targeted at the said country.

Tracing hackers poses a challenge for Nigeria because finding and tracing hackers in cyberspace is difficult. The cyberspace is not limited to, any geographical boundary or location and hackers use several methods to hide their crimes which make it very difficult to trace their activities. These include the use of passwords to lock files, encryption or multiple encryption of messages, hiding of data in secret files or in unallocated sectors of storage, making them invisible, computer penetration and looping which entails accessing a number of computers and forwarding the message to a chain of others before it arrives at the desired destination making it all the more difficult to be traced. Hackers also employ the use of remote storage, which means hackers can store data on remote hosts without the knowledge of the hosts.

---

[70] Glanville, L. 'The Responsibility to Protect Beyond Borders' (2012) Human Rights Law Review 1-32 Available on: http://hrlr.oxfordjournals.org/content/early/2012/01/23/hrlr.ngr047.full Accessed 12/02/2015

[71] 'US Hacker looses Extradition Fight' *BBC News* 3 April, 2007 <http://news.bbc.co.uk/2/hi/uk_news/6521255.stm > Accessed 10/02/2015 In this case, a British man has lost his High Court fight against extradition to the US for allegedly carrying out the "biggest military computer hack of all time". Glasgow-born Gary McKinnon, of North London, is accused of gaining access to 97 US Military and NASA computers. Home Secretary John Reid granted the US request to extradite him for trial.

[72] Karnatak, C 'Cyberspace: Jurisdictional Issues of E-Commerce and Consumer Protection'. (2014) 3 No 7 Abhinav Journal of Research in Commerce and Management 22

[73] 1997 US App LEXIS 33871 (9th cir. Dec 2 1997)

[74] 74F 3d 701 (6th Cir 1996)

[75] 2001 U.S. Dist. LEXIS 18378 (ND Cal 2001) &145F. Supp.2d 1168 (ND Cal 2001)

Additionally, there is a dearth of cybercrime fighters and forensic experts in Nigeria. Law enforcement agents have little or no knowledge of hacking as a cyber crime. Another dimension to the problem is that hackers need not be present at the crime scene to perpetrate the crime which implies that conventional policing where the criminal is caught in the act will not apply in cases of hacking. Another major challenge is the fact that theft of computer data is invisible. When a physical item is stolen, it is missing and an alarm can be raised immediately, but when data is stolen, it is merely copied leaving no evidence that it was stolen. The invisibility of the theft means it may not be discovered until months after, if at all and this makes it all the more difficult to apprehend the perpetrators.

The Nigerian regulatory bodies, the lawmaking body and the administration of justice system are yet to give full recognition and standard approaches to hacking as they have given to other traditional crimes. It is incontestable that the evolution of our laws came from our traditional way of dealings, therefore almost all of our existing laws to deal essentially with our traditional dealings, and now that the computer system is of the essence in conducting those same traditional dealings, the laws have not expanded fully to contain this development. It is a common knowledge that before the advent of computer, transactions are carried out directly. Where if party A wants to have a transaction with party B, goes to the party directly or sends his agent directly for negotiation of the deal, and where they reach an agreement may establish a contract which may be evidenced in writing. Today, that computer is used to carry out the same traditional dealings at even a much faster pace.

Another problem worthy of mention is the fact that law firms have even become particularly attractive targets for hackers since computer-savvy intruders are drawn by the quality of documents available in law offices.[76] Infiltrating a lawyer's computer system is an optimal method of obtaining sensitive material because law firms have a concentration of really critical, private information.[77] In order to obtain legal advice, a client will often have to reveal valuable data, future plans, harmful evidence, and embarrassing facts. There is a long standing professional tradition that people should be able to seek legal advice with confidence that their secrets will not be exposed.[78] Hacking is eroding that confidence and the effect today is that if the client cannot trust that the information will remain private, he or she may hesitate to obtain legal advice at all.

In 2011, the hacker collective "Anonymous" stole law firm files concerning the defense of a U.S. Marine accused of misconduct and posted them on the Internet[79]. Chinese hackers attacked several Canadian law firms working on the $40 billion acquisition of the world's largest producer of potash (a valuable agricultural and industrial chemical) and stole strategic data and bidding information[80]. This problem is serious and growing.

The computer also provides the user with a degree of anonymity which is unparalleled in the non-electronic environment.[81] The hacker can be any person he or she wishes to be at a particular time and this anonymity has significant criminal law consequences.[82] Not only does this make the task of detecting hacking and the offenders more difficult, it complicates the

[76] Brenner J, 'America The Vulnerable: Inside The New Threat Matrix Of Digital Espionage, Crime, And Warfare, (New York: Penguin Press, 2011) p.61–62

[77] Finkel, E 'Cyberspace Under Siege', Nov. 2010 *ABA Journal*, , *available at* <http://www.abajournal.com/magazine/article/cyberspace_under_siege> accessed 12/02/2015

[78] *United States v. Grand Jury Investigation,* 401 F. Supp. 361, 369 (W.D. Pa. 1975)

[79] Albanesius, C 'Anonymous Hacks Law Firm Representing Haditha Marine', PC MAG. February 6, 2012 Availaible on< http://www.pcmag.com/article2/0,2817,2399909,00.asp.> Accessed 12/02/2015

[80] Riley, MA &Pearson, S 'China-Based Hackers Target Law Firms to Get Secret Deal Data', BLOOMBERG (Jan. 31, 2012) Available on:< http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html. > Accessed 12/02/2015

[81] Rasch, MD 'Criminal Law and the Internet' in *The Internet and Business: A Lawyers Guide to the Emerging Legal Issues* (Computer Law Association Inc: 1996) Online Version Available on: <http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html>accessed 12/02/2015

[82] Ibid

various proof issues which may be presented at such trial[83] (if it ever comes up in the Nigerian courts). The problem of anonymity is further complicated by the fact that, in computer crime prosecutions, the integrity of computerized data is frequently in question.[84] For example, it was not until 2011 that the admissibility of computer generated evidence was included in the Nigerian Evidence Act[85]. Even then, computer generated evidence will have to go through stages of authentication before being rendered admissible.[86] It is a common contention in Nigeria that the computerized information and the computer system that contains it which may have been the subject of a hacker attack is vulnerable to alteration or destruction, while at the same time, the bulk of the evidence to be presented is frequently generated by the very same corrupted or attacked computer system.[87]

Presently, computer technology is moving faster than the law, as such rendering the courts toothless to bite in such situations. When crimes emanate from the use of computer technologies, it takes long years before the law begins to grapple with establishing laws to curb those crimes. Thus the justice administration system is left with the employment of the other laws originally meant for traditional offences to treat cyber-related offences, thereby causing a lacuna in the administration of justice system as to contain cyber crimes such as hacking.

4. CONCLUSION AND RECOMMENDATIONS

Hacking has become an issue because of the existence of computers and its relevance and it entails both criminal and civil liabilities. Presently in Nigeria there are shortcomings in finding available and appropriate laws and remedies to salvage the situation both for the offenders and the victims as well. Based on the present impact of hacking activities both internationally and locally, the Nigerian legal system should be interested, both in putting measures in place to regulate and curb the activities of hackers and to provide remedies for victims of hacking activities. It is submitted that the remedies be achieved in two different manners; civil and criminal.

The legislative bodies have to identify and define what constitutes hacking as well as the consequences attached to it. Nigerian lawmakers should eradicate the use of laws promulgated solely for traditional offences for addressing crimes such as hacking. This is simply trying to force square pegs into round holes. Our administration of Justice System must expand its scopes to contain the crime of hacking. There is necessary need for international laws to be put in place to deal with the issue of jurisdiction. Law enforcement and security agencies should have special departments trained to be able to access and investigate hacking cases.

It is believed that to fight the borderless and continuously evolving cybercrimes, global leaders must collaborate on joint initiatives. Thus far, the discussion on how to set international standards has been low profile and largely confined to the UN General Assembly or European Union. Overcoming significant diplomatic hurdles requires a concerted effort on the part of the Nigerian Government. The international and multi jurisdictional nature of hacking calls for external partnerships, which is definitely fundamental to the successful investigation and prosecution of Hacking. Nigeria should as a matter of priority, seek partnerships with countries like USA, Canada and UK that already have laws and are presently engaged in investigation and prosecution of cybercrime.

Cyber crimes such as hacking require highly responsive and internationally coordinated control measures, making investigation and reporting of such crimes highly productive.[88]

[83] Ibid
[84] Ibid
[85] The Nigerian Evidence Act Cap 112 LFN 1990
[86] See Section 84 Evidence Act of Nigeria
[87] Op Cit M.D Rasch
[88] Op Cit EUROPOL Public Information. See Footnote 1

Active engagement with the private sector should be a priority for the Nigerian Government to ensure that hackers are properly identified and referred to law enforcement agencies. Relevant authorities should enhance and maintain cordial relationship with cyber providers, particularly Internet service providers (ISPs) with the mission of arresting the situation. Both ISPs and any Internet security organizations in Nigeria should as a matter of priority, monitor the Internet for suspicious traffic; then law enforcement agencies can draw on their resources and technical skills to investigate and prosecute hacking more efficiently and improve its knowledge of Internet facilitated offending.[89]

Education in this area should also be given priority because many Nigerians are even unaware of what hacking is. The problem cannot be over emphasised because in this part of the world, people do not know and understand the implications of hacking and they many a times do not care to know how it affects them. Majority of Nigerians would never report incidences of hacking because they simply do not notice the offence taking place or understand what it is all about. Again, Underreporting is an obstacle to appreciating the true scale and nature of cybercrimes like hacking and where crimes are underreported; the government would be unable to take action for those crimes. Nigerians need to be educated on the crime of hacking and while the government is yet working on providing a solution to the problem Nigerian should tackle hacking individually. Individuals should perform regular required software updates for their operating systems. This action, largely reduces the risk of being hacked. People should have antivirus and anti spyware software installed on their operating systems, particularly those that are efficient enough to prevent hacking. Individuals should be taught to delete emails from unknown sources because opening such emails creates leeway for hacking.

In view of all the aforesaid, it is easy to see how hacking has become a problem for the Nigerian legal system, be it legislators, law enforcement agencies, lawyers as well as the criminal justice system. So far there are no hacking focused laws in Nigeria meaning it would be difficult to convict Hackers. Nigeria is part of the international community and it requires laws in this field to be able to prosecute offenders. It is difficult enough as it is to bring the perpetrators of hacking to book without having to worry about the lack of proper legislation. It is imperative that the country is not left behind in this regard.

We acknowledge that hacking is a serious crime which needs to be treated with caution not by the government alone, but by everybody since we are all at risk. In the world of technology and the internet everybody has to be on alert. Individuals should be conscious of what they do on the internet to reduce crimes and prevent the emergence of new ones. If individuals, and then the Nigerian Government take up the challenge, we will be left with little or no problems to deal with as regards hacking and hopefully that will be in the near future.

[89] Ibid