HALREV

Volume 2 Issue 2, August 2016: pp. 195-212. Copyright © 2015-2016 HALREV. Faculty of Law, Hasanuddin University, Makassar, South Sulawesi, Indonesia. ISSN: 2442-9880 | e-ISSN: 2442-9899.
Open Access at: http://pasca.unhas.ac.id/ojs/index.php/halrev

An Overview of the Legal framework of Advanced Fee Fraud and Cybercrime in Nigeria

Mu'azu Abdullahi Saulawa
Faculty of Law, Umaru Musa Yar'adua University
P.M.B. 2218, Katsina State, Nigeria
Tel./Fax: +234-65290280 E-mail: muazu.abdullahis@gmail.com

Submitted: Jul 26, 2016; Reviewed: Aug 3, 2016; Accepted: Aug 11, 2016

Abstract: *The paper seeks to discuss an overview on the advanced fee fraud offences as well as cybercrime in Nigerian. The aims of the paper focus on discussing the advanced fee fraud under the related provisions of Advanced Fee Fraud Act 2006 on the success of the law in addressing the practices of crimes in relation to information technology. The paper also discusses the cybercrimes in Nigeria with a brief look out on the Cybercrime (Prohibition and Prevention) Act 2015. Further, it also aims at examining the application of the law in the fraud offences which raises an issue of the regulatory framework of the cybercrime. The methodology adopted by the paper is doctrinal approach method wherein both primary and secondary sources of data were analysed, particularly the local laws and other relevant documents. The finding of the paper reveals that the relevant section of the in the Advanced Fee Fraud Act that deals with electronic communication has not been invoked. This is because the discussed relevant law under the advanced fee fraud did not in any away deal with cases concerning electronic communication under section 13. The paper recommends that there is a need to strengthen the adequacy of the legal framework on the Cybercrimes so as to checkmate such practices in Nigeria.*

Keywords: *Advanced Fee Fraud; Convention; Cybercrime*

DOI: http://dx.doi.org/10.20956/halrev.v1n2.304

INTRODUCTION

The focus of the paper is on the relationship of advanced fee fraud and cybercrime offences in Nigeria. The majority of the crimes perpetrated revolve around hacking, credit card fraud, advanced fee fraud sis generally known as 419, fraud, forgery and websites defacement etc. This involves the application of computer technologies and other related devices. These are the major common crimes in the related platform affecting the country in particular and the world at large. Nothing can be further from the truth that the perpetrated crimes in Nigeria are rising, for instance, the computer fraud and forgery usage of government documents in the recruitment applications and websites are engaged in among the common crimes being perpetrated in the recent times.

The target victims usually are credit card users and people who are engaged in other online transactions. The reason is not far-fetched from the truth that cybercrimes in Nigeria has grown through the platform

of advanced fee fraud which has become so prominent and notorious. The essence for the spread is the absence of coherent cybercrime legislation in the country, the Penal law addresses fraud practices but it does not cover the application of computer devices in the contemporary aspect. In addition, the existing Advanced Fee Fraud Act of 2006 actually discusses the relevant fraud offences in relation to telecommunications; those do not include credit card offences, POS intrusion and other related offences. At least, there is an impact from the current Fraud Act of 2006, considering that the offence falls within the purview of computer related devices due to current realities. Though, the Nigerian current situation in the cybercrimes activities involves the exercise of fraud means by accessing credit card details, forged and hacked devices.

These practices have generated a lot of concern from the global community considering the fact that a sizeable number of above 85, 202 Nigerian citizen scammers outside and excluding "money mules" were monitored. As at March 3003, a report forwarded to the relevant authorities in a country indicated the figure of 22,669.[1] The further report that the activities of 419 in 2013 when a reviewing 9274 complaints (in 2007 - 17475 / in 2009 - 8503), it reflects on Nigerian 419 advance fee fraud coming from 152* countries (161 in 2007/ 152 in 2009).[2] It has become a disease to Nigerian with reasonable evidence that 82% of the lottery scams and 78% of checks fraud are Nigerian AFF related; 72% of counterfeit checks in transit belong to a Nigerian.[3] Also, the related bad image attributed to Nigeria has become of bigger concern to Nigerians and this practice has caused serious lamentations. The widespread of 419 Advance Fee Fraud, internet fraud and corruption has been generating mixed feelings in the public domains these days. The perception is that some of the millions of Nigerian that travel overseas are not there for the good means of the countries rather they are there for a different objective that does not resonate with the countries' faith, i.e. they are there to engage in the practices of advance fee fraud scams. [4] The discussion on the paper will look into the advanced fee frauds in Nigeria.

ANALYSIS AND DISCUSSION

Advanced Fee Fraud in Nigeria

The activities of advanced fee fraud [5] is a medium whereby perpetrators traffic emails requesting the addressee to assist them in

1 Ultrascan Advanced Global Investigations. (2014). p. 13. Available at http://www.ultrascan-agi.com/public_html/html/pdf_files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf, accessed on 20/12/2015.

2 *Ibid*. the Ultrscan is not an official reporting Unit on 419, but with the collaboration of experts in 419, they monitor, survey and collect results.

3 *Ibid*, Most counterfeit checks were produced in Nigeria, Canada and India of which a significant number under control of Nigerian AFF.

4 *Ibid*, p. 27.

5 The term "advanced fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: Pauline C. Reich. (2004). *Advance Fee Fraud Scams In-Country and Across Borders.* Australian Institute of Criminology International Conference, Hilton on the Park, Melbourne, Australia Nov. 29-30, 2004, page 1; Smith, Holmes, and Kaufmann, *Nigerian Advance Fee Fraud, Trends & Issues* in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; Oriola, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237; Beales, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

the wiring or transfer a huge sum of money from one part to the other thereby involving multiple parties by promising them a share in the percentage. The agreed parties in the transaction present their personal account[6] and more often deceitfully. The perpetrators logically request the parties to transfer a little amount of money to their main account so as to authenticate the existence of the account information or request the account information straightway. Once the transfer is confirmed, the perpetrators will disappear. One advantage they enjoy is the use of the bank account confidential information for fraudulent transactions. The perpetrators use emails as their conduit in achieving their target and evidence supported that.[7] The information indicates that advanced fee fraud is on the rise; the number of the activities keeps on multiplying on a regular basis, notwithstanding the affected number of victims and the loss ensued.[8]

The practice in Nigeria is increasing and some were engaged in their mystical ways of practices as a scored advantage. The perpetrators are classified as a modern name popularly known as 'Yahoo boys'. The name replaces the 419 because of the advance use of computer and internet, thus attributes to be their prey. Yahoo Boys' as the name implies, is a nickname given to the class of youths who are experts in numbered types of cybercrime.[9] Based on an interview conducted in another research paper reveals that at least 40 active 'Yahoo Boys', are usually between the age of 22 and 29 years and were involved Nigeria's cybercrime offences. They are undergraduates with a different standard of living compared to others.[10] The mode of operation includes spiritual and other inhuman methods thus include:

> "Their strategies include collaboration with security agents and bank officials, local and international networking, *and the use of voodoo* [emphasis added]. It was clear that most were involved in online dating and buying and selling with fake identities. The Yahoo boys usually brag, sag, do things loudly, drive flashy cars, and change cars frequently. They turn their music loud and wear expensive and latest clothes and jewellery. They also have a special way of dressing and relate, they spend lavishly, love material things, and go to clubs. They are prominent at night parties picking prostitutes at night. They are in groups, always walk together, even at the point of the eatery and used communicate in an alinet language or grammar for their only understanding, like "Mugun," "Maga," while "Maga don pay," refer as "the fool (i.e., their victim) has paid."[11]

Previously, 'Yahoo Boys' were known as 419 scams in the 1980s, at that time when

6 Advance Fee Fraud, Foreign & Commonwealth Office, available at: www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

7 For an overview of estimated losses, see Reich, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, p. 3.

8 For more information, see: the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

9 An extract of a study from an interview conducted by Dr. Joshua Oyeniyi Aransiola, a Sociology lecturer at Obafemi Awolowo University-Nigeria in the city of Ile-Ife in 'Nigeria's '419' email scams uncovered: The truth behind the Yahoo Boys', Metro.com, Accessed 4/4/2015, available http://metro.co.uk/2012/03/02/nigerias-419-email-scams-uncovered-the-truth-behind-the-yahoo-boys-338017/.

10 Spy Service Exposes Nigerian 'Yahoo Boys', Krebson Security, Accessed 4/4/2015, available at http://krebsonsecurity.com/2013/09/spy-service-exposes-nigerian-yahoo-boys/.

11 *Ibid*, and an extract of Joshua Oyeniyi Aransiola and Suraj Olalekan Asindemade. (2011). "Cyberpsychology, Behavior, and Social Networking". 14(12): 759-763. doi: 10.1089/cyber.2010.0307.

the Nigerian economy vanished, these act of 419 are carried out by graduates who are unemployed and they used a document or application to fraud/play foreign businessmen into depositing money to the non-existent business.[12] These groups of ('Yahoo Boys'/419 scam) used voodoo that is charms for spiritual protection to successfully carry out the inhuman act on the one hand and to also charm the potential victim's on the other hand which is the commonest act in their practices.

Cybercrimes in Nigeria

Cybercrime covers different perspective of computer related offences and networks. The act of the crimes revolves around confidentiality, integrity and availability of computer data or system defined the essentials of cybercrime.[13] The paper adopted the definition of USDOJ[14], Cybercrime defined to be 'any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution'.[15]

Cybercrime cannot be committed, itself; it is a group of people or individual with a different expertise in crimes perpetration.[16] These computer criminals sometimes are youths who are good in hacking, staff corporations, anger employees, secret agents (spies) and class of terrorists.[17] They are referred as 'cybercriminals' where the crime committed using computer as an object. Computer can be attributed as an object in crimes perpetration as well as a target [18] and sometimes referred as subjective to a crimes due to its visibility in the crime scene.[19]

The rate of cybercrime today continued to grow rapidly and operate globally.[20] The exchange of communication through E-mails with illegal content across the globe such is stored outside the country.[21] The cybercrime investigations, must be in a close assistance across the country's borders involved is very significant.[22] The application of legal model for having a unification in the agreements are based on formal, complex and often time-consuming procedures, and in addition often do not cover computer-specific investigations. Initiating a strategy and procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital.[23]

So many countries acknowledge their understanding for mutual legal assistance

12 'Nigeria's '419' email scams uncovered: The truth behind the Yahoo Boys', *Op. Cit*.

13 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations New York, Draft-February 2013, at xvii.

14 The United State, Department of Justice.

15 Sheri A. Dillon *et al.,* (1998). "Note, Computer Crimes", 35 *Am. Crim. L. Rev*. 503, 505 (defining "computer crime") (quoting National Institute of Justice, U.S. Dep't of Justice, Computer Crime: Criminal Justice Resource Manual 2 (19 89)).

16 *Ibid*, at 506.

17 *Ibid*.

18 *Ibid*, at 507.

19 *Ibid*.

20 Regarding the transnational dimension of cybercrime, see Sofaer and Goodman, "Cyber Crime and Security – The Transnational Dimension", in Sofaer and Goodman (eds.) (2001). *The Transnational Dimension of Cyber Crime and Terrorism,* p.7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

21 Regarding the possibilities of network storage services, see: Clark. (2005). *Storage Virtualisation Technologies for Simplifying Data Storage and Management*.

22 Regarding the need for international cooperation in the fight against cybercrime, see: Putnam and Elliott, "International Responses to Cyber Crime", in Sofaer and Goodman, (eds.). (2001). *Transnational Dimension of Cyber Crime and Terrorism*, p.35, available at: http://media.hoover.org/documents/0817999825_35.pdf.

23 Gercke, (2006). "The Slow Wake of a Global Approach against Cybercrime", *Computer Law Review International*, 141.

regime on the principle of 'dual criminality'.[24] Outlooks on a global level are generally limited to those crimes that are criminalized in all participating countries. Although the numbers of offences are minute – such as the distribution of child pornography – that can be prosecuted in most jurisdictions, regional differences play an important role.[25] One example is the illegal content of hate speech. The criminalization of illegal content differs in various countries.[26] Materials that can lawfully be distributed in one country can easily be illegal in another country.[27]

The computer technology today is essentially the same across the world.[28] Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardization, the network protocols used in countries on the African continent are the same as those used in the United States.[29] Standardization enables users around the world to access the same services over the Internet.[30]

The question is what effect the harmonization of global technical standards has on the development of the national criminal law. In terms of illegal content, Internet users can access information from around the world, enabling them to access information available legally abroad that could be illegal in their own country. The details of this discussion will be in the subsequent chapters. Ideally, the advancement arising from technical standardization go far beyond the globalization of technology and services and could lead to the harmonization of national laws. However, as shown by the negotiations

[24] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; Schjolberg and Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005, p.5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; Plachta, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, p.87., available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

[25] See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; Mitchison et tal, 'Identity Theft' – A discussion paper, 2006, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; Schjolberg, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[26] The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol.

[27] With regard to the different national approaches towards the criminalization of child pornography, see for example: Sieber, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

[28] Regarding network protocols, see: Tanebaum, Computer Networks; Comer, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[29] The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: Tanebaum, Computer Networks, 2002; Comer, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

[30] Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itut/oth/06/15/T061500000A0015PDFE.pdf. Regarding the importance of single technical as well as single legal standards, see: Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7.

over the First Protocol to the Council of Europe Convention on Cybercrime (the "Convention on Cybercrime"),[31] the principles of national law change much more slowly than technical developments.[32]

Interestingly, the cyberspace may not recognize border controls, due to the openness of the technology, though there are means to restrict access to certain information.[33] The access provider can generally block certain websites and the service provider that stores a website can prevent access to information for those users on the basis of IP-addresses linked to a certain country ("IP-targeting").[34] Both measures can be get around, but however are devices that can be used to retain territorial differences in a global network.[35] The OpenNet Initiative[36] reports that this kind of censorship is practised by about two dozen countries.[37]

[31] Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

[32] Since parties participating in the negotiation could not agree on a common position on the criminalization of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

[33] See Zittrain. (2006). "History of Online Gatekeeping", *Harvard Journal of Law & Technology, 19*(2): 253, available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

[34] This was discussed for example within the famous Yahoo-decision. See Poullet, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; Goldsmith/Wu, Who Controls the Internet?: Illusions of a Borderless World, 2006, at p. 2.

[35] A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.

[36] The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

[37] Haraszti, 'Preface, in Governing the Internet Freedom and Regulation in the OSCE Region', available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

Cybercrimes in Nigeria are crimes that opened a new form of business to criminals, with the growing of internet transactions which has transformed the financial sector opens a window for criminals to extend their crime net. The Nigerian community graduated from traditional set of crime perpetrated to electronic crimes which unfortunately have reception in Nigeria cyberspace. The emergence of cybercrime in Nigeria is the transformation of information and technology, its reception centrally focuses on electronic transactions and this particularly on financial institutions and the individuals, the use of ATM fraud, spam email messages, POS, piracy of patents etc.

For a number of decades, crimes are committed in the internet, speaking of the fact that a record exhibiting the Nigerian position on crimes net and related activities. Both locally and internationally reference to some of the activities of the criminals. The financial sector as the major concern have striven hard to make use of security application so as to protect the financial institution and their customers from menace of cybercrime, but still the criminals are looking for another way. They are very tricky and sometimes used to follow victims to ATM centres for the purpose of getting closer to their victims and attempt to play ignorant of the system all in effort to have a slight clue of the victim's card. More often they target individuals as their prey not directly the computer system.

The cyber offences are committed against individuals, groups and government infrastructure though the act of the crime is intentional, purposely to harm the individu-

al or property and sometimes to the government.[38] The Nigerian cybercrimes are committed by the youths between young and old ages, but more often, the young-youths are the perpetrators. The youths feels it to be a hacking competition or mainly profit making show and considering the fact that the devices used to initiate the act are inexpensive in today's cyber world.[39] Some of the criminals falsify documents and tells a number of stories to get money from victims,[40] sometimes they make used of non-existent charity organization requesting for a support or hoax corporation as clearing agents. That in information that reveals the Nigerian government is risking the sum of 80 USD to fake and counterfeit productions of software.[41]

The Applicable Laws

The applicable laws in this context focused on Nigeria though there are local laws that extensively deal with the crimes but there is an important legislation yet to become a law that will enhance the fight against such crimes.

Nigerian Penal Code 1963

The Penal Code Law [42] has been existing for a number of decades and it is still in active practice. However, it has not incorporated any technology device in the commission of the crime, but some of the provisions discuss devices, which by extension are referred to as trademarks. Notwithstanding, the law recognise the use of forged document, fraudulent acts, mark, seal and trademark as offences.

The law discusses the stages of falsification of documents done by a person [43] and further provides where as a result of forging the document leads to damage a property, reputation or injury to person [44] is said to commit an offence punishable under the said provision.[45] That the production of any related counterfeits such as plates, seals and other objects with the intending manner of using it, commits the offence of forgery and shall be punished under this section[46] and if uses the device or any material related for any reason intended for forgery commits an offence and punishable under the section.[47] The provision discusses devices which relate to the offence of advance fee fraud in which event of fraud practices lead to the usage of a machines or device in creating an object for the purpose of committing the offence.

Advanced Fee Fraud Act 2006

The relevance of this law is that the offenders defraud victims of their electronic device

[38] Ibikunle Frank and Ewedeniyi Odunayo. (2013). "Approach to Cyber Security Issues in Nigeria: Challenges and Solutions", *International Journal of Cognitive Research in Science, Engineering and Education, 1*(1):1-14.

[39] Anah Bijik Hassan, Feunmi David Lass and Julius Makinde. (2012). "Cybercrime in Nigeria: Causes, Effects and the Way Out", *ARPN Journal of Science and Technology, 2*(7): 626-635.

[40] *Ibid*.

[41] The report was compile by Institute of Digital Communication in the South Africa couple with collaboration of America National Fred Information Centre thus highlights the ration of amount of money Nigeria is losing as a result of online fraud as 90 % in 2001 which rises the cybercrimes in Nigeria input per capita as strangely high. For further information see Ehimen O.R and Bola A. (2010). "Cybercrime in Nigeria", *Business Intelligence Journal, 3*(1): 92-98.

[42] That the Penal Law is meant for the Northern Region of Nigeria, the law is Gazetted as the Northern Region Law Number 18 of 1959. It was assented to in Her Majesty's name by Sir Gawain Bell, K.C., M.G, C.B.E, Governor of the Northern Region of Nigeria, on the 26th of September, 1959 and was designated as Cap. 89 in the Laws of Northern Nigeria, 1963.

[43] Section 363(a)-(c), Cap 89, Laws of Northern Nigeria, 1963.

[44] Section 363, *Ibid*.

[45] Section 364, *Ibid*.

[46] Section 367, *Ibid*.

[47] Section 369, *Ibid*.

or make use of electronic communication to advance their fraud practices. The Economic Financial Crime Act, 2004[48] differs from Advanced Fee Fraud Act, as Advanced Fee Fraud Act is limited to only obtaining property by false pretence and also acknowledging using electronic communication to perpetrate an act of fraud as offences under the Act. The law proceeds to discuss the provisions of advanced fee fraud, electronic telecommunication offences and other related.[49]

The Act provides that notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud.[50]

(a) Obtains, from any other person, in nigeria or in any other country for himself or any other person;
(b) Induces any other person, in nigeria or in any other country, to deliver to any person; or
(c) Obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.

It further provides that a person who by false pretence, and with the intent to defraud, induces any other person, in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.[51] The Act also provides for the punishment of the offence; a person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine.[52]

The presentation of this case involves in the subject matter of the case concerning the evidence in relation devices and information technology in the Nigerian courts. The present case of *Nuradeen Adewale Arije v. Federal Republic of Nigeria*,[53] thus, on appeal against a charge by the appellant in respect of obtaining goods by false pretence under section 1 (3) of the Advanced Fee Fraud and other Fraud Related Offences Act No. 13 of 1995 as amended by Act No. 62 of 1999. Section 1 (3) is the punishment section. Section 1(1) which provides that notwithstanding anything contained in any other enactment or law, any person who by any false pretense, and with intent to defraud:

(a) Obtains from any person, in Nigeria or in any other country, for himself or any other person;
(b) Induces any other person, in Nigeria or in any country, to deliver to any person, or
(c) Obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by false pretense, is guilty of an offence under the Act."

As to the question that bothers on obtaining property or its delivery induced by a means of a contract induced by false pre-

[48] Laws of the Federation of Nigeria. the purpose of the law is to deals with money laundering matters.
[49] Part II, *Ibid*.
[50] Section 1(1).
[51] Section 2, *Ibid*.
[52] Section 3, *Ibid*.
[53] (2013), LPELR-33125 (CA) by the Court of Appeal of Nigeria, delivered on the 6th day of November 2014, CA/L/770/2009.

tense is guilty of offence. That the charge was framed under Section 1(1) of the Advance Fee Fraud and Other Fraud Related Offences Act No. 14 of 2006 which is the repealed Section 21 1995 Act as well as the Amended Act of 2006. The appellant submission is that he was charged tried and convicted under a repealed law and this renders the trial and conviction a nullity given the fact that the offence he was alleged to have committed was in 2007 in which case he ought to have been charged under the Advance Fee Fraud and Other Fraud Related Offences Act No. 14 of 2006 and not the Act of 1995 which has been repealed. The appellate Judge was persuaded with the submission but consider the submission of learned Judge as in Per OSEJI J.C.A at pp. 34-36, paragraphs E-B that:

> *'if an accused person can only be charged with an offence created by penal statutes/law and that a court of law can only have jurisdiction to punish for the offence provided'.*[54]

The Court further explicitly stressed that a mere misdescription of the law under which a charge have been brought does not necessarily render the offence charged not known to the law at the time of its commission. Therefore, as much as the offence charged discloses an offence in a written law and such law existed at the time of the commission or omission of the alleged act was done, the information of the charged is valid and merely defective in the event of misdescription of the law charged against the accused.

Part of the main issue is that the appellate judge agreed with the submission of learned counsel to the appellant that the trial judge erred in refusing to accept appellant defence where it indicates that one WESCO Company, the victim alleges the crime is not engaged in the business of computer accessories at the time the offence was committed. The reason is plain that the prosecution counsel has not presented evidence to that effect. But the reference to page 316 of the record; it is the duty of the respondent to prove that. An extract of the record of the proceedings of the evidence, at page 382 where the trial judge made some findings:

> *'Exhibit P10 stating the chain of shipment from WESCO to Moro Cargo and to Basmak was confirmed by the defendant in his statement Exhibit P53. The goods ordered by suspects stated in Exhibit P10 and P17 included ink cartridges, RAM, projectors etc. The goods recovered from the defendant were Kingston Memory RAM admitted by him in his statement. The attempt by the defendant to show that WESCO is not into computer accessories business through a website said to have been assessed the morning of defendant's defence cannot be accepted as a good defence. The search Engine used to get the results is not shown on Exhibits D8-D11. How the search was done is not clear and whether this was the only result for WESCO is not stated. I cannot attach weight to this evidence. Also, the fact that the type of computer RAM recovered is available in the open market in Nigeria is of no moment. The RAM was meant for sale in the Nigerian Market. The particular Computer RAM, in this case, were not recovered from the open market but from the defendant. It is true that the details of the credit card application process are not before this court.'*

[54] See *Ifegwu v Federal Republic of Nigeria*, (2001) 13 NWLR (Pt. 729).

The court held that having examined the case at hand, the error of convicting under the then repealed Act of 1995 instead of Act 2006 did not alter or affect the conviction as no miscarriage of justice has been occasioned. The appellate judge after carefully evaluating the evidence in the main judgment dismissed the appeal and affirmed the judgment of Justice M. O Obadina on the 25th day of May 2009.

Discussions on the case: that the real issue, in this case, is on an offence relates to obtaining property by false pretense and the subject matter here involved is the property also contain computer accessories. The prosecution may possibly not have evidence to produce to the court in relation to the assessors such flash drive, RAM and other devices which also lead to charge the accused for obtaining a property by false pretense.

The main hitch in the case in the application of computer crimes in the Nigerian courts which is still a non-existing issues because there is no regulation empowering a court to deal with such offence, considering the fact that for accused to be charged before the court of law, such offence must be a written law, in the absence of such, the prosecution has no option than to charge the accused under the advance fee fraud Act.

The important point here is that the prosecution have charged the accused under section 12(1) of the Advance Fee Fraud Act 2006 since it discussed services of electronic communication services and thus from the record of the proceedings there is discussion on sending information online and also the website of one company WECO, looking at the extract of the judgment it highlighted thus:

> *'Exhibit P 31-P33 are documents recovered from the flash drive of the defendant which he acknowledge authorship. The documents composed by the defendant have a computer generated signature of foreign names which he admitted was generated by him, the court further look at the relevance of the above Exhibit and concluded that it is similar facts and if he generated a signature of Larry Smith of Voyager Electronic using the computer, then it is safe to conclude that he generated also the signature of Ola Rhodes in Exhibit P43. Exhibit P58-P55 is statements of the appellant and duly tendered and admitted in evidence without any objection whatsoever. In the said statement, the appellant further informs that his flash drive was opened in his presence and some scam mail were printed out and the said scam emails were composed by him with fake names and address. He also further said the transaction was fraudulent and dubious.'*

Also in a related case of fraud in the *United States of America v. Nnamdi Chizuba Anisiobi and others*,[55] where all three defendants each pleaded guilty to one count of conspiracy, eight counts of wire fraud and one count of mail fraud. Three of the defendants were arrested in Amsterdam on Feb. 21, 2006, and were subsequently extradited to the United States based on an investigation was initiated by Dutch law enforcement authorities. After identifying

[55] Department of Justice, Office of Public Affairs, for immediate release on Thursday, April 2, 2009, accessed on 12/1/2016, available at http://www.justice.gov/opa/pr/three-defendants-sentenced-advance-fee-fraud-scheme-cost-victims-more-12-million.

victims in the United States, Dutch authorities notified the U.S. Postal Inspection Service, which opened its own investigation, resulting in the charges against the defendants. The indictment reads that on a complaint filed earlier, the defendants sent "spam" e-mails to thousands of potential victims, in which they falsely claimed to control millions of dollars located abroad.

Attempting to conceal their identities, the defendants admitted they used a variety of aliases, phone numbers and e-mail addresses. That the defendants sent e-mails purporting to be from an individual suffering from terminal throat cancer who needed assistance distributing approximately $55 million to charity. In exchange for a victim's help, the defendants offered to give a 20 percent commission to the victim or a charity of his or her choice. Subsequently, as part of the ruse, the defendants sent a variety of fraudulent documents, including a "Letter of Authority" or a "Certificate of Deposit," making it appear that the promised funds were available, and pictures of an individual claiming to suffer from throat cancer. The evidence to the court established that Anisiobi telephoned victims, disguising his voice to give the impression that he was suffering from throat cancer.

After obtaining their victims' trust, the defendants asked them to wire-transfer payment for a variety of advance fees, ostensibly for legal representation, taxes and additional documentation. In return, the victims received nothing. In a variation of the scheme, if the victims said they could not afford to pay the advance fees, the defendants admitted they would send them counterfeit checks, supposedly from a cancer patient, to cover those fees. Many victims deposited the checks and then drew on them to wire-transfer the advance fees. Subsequently, when the checks did not clear their accounts, the victims suffered substantial losses. Based on their guilty plea, the court sentenced them in January 2008 to federal charges of operating an "advance-fee" scheme that targeted U.S. victims with promises of millions of dollars.

The convicts names were Nnamdi Chizuba Anisiobi (a/k/a Yellowman, Abdul Rahman, Michael Anderson, Edmund Walter, Nancy White, Jiggaman and Namo), 31, citizen of Nigeria, all was sentenced to 87 months in prison. And Anthony Friday Ehis (a/k/a John J. Smith, Toni N. Amokwu and Mr. T), 34, a citizen of France, was sentenced to 57 months in prison. Then Kesandu Egwuonwu (a/k/a KeKe, Joey Martin Maxwell, David Mark and Helmut Schkinger), 35, citizen of Nigeria, was sentenced to 57 months in prison.

The Act provides that any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain from the customer or subscriber; their full names and residential address, in the case of an individual and corporate address of its offices.[56] Failure to abide the provision of this section is also an offence with a prescribe punishment [57] and where a person also fails to comply in submitting an information to the Commission in any manner he/she commits an offence and liable on conviction.[58]

[56] Section 12 (1)(a), (b) and (c), *Ibid*.
[57] Section 12 (2),(a)-(b) *Ibid*.
[58] Section 12 (3), *Ibid*.

The Act enjoys telecommunication firm as well as service providers in business to register with the nation financial crime commission and such must be maintained.[59] Such telecom firms are required to submit data in relation to their electronic activities to the commission [60] and further, ensure the services they provided are purely legal.[61] Such shall be in compliance with the Act.[62] It stressed that every person or company is expected to strictly follow the provision of sub-sections.[63] Therefore in the event of liable, such licence shall be deemed to be cancelled.[64] It also provides that the jurisdiction [65] of the offences by the court, both Federal High Court and State High Court to try and punish the offenders [66] and must be satisfied that he cannot ascertain the property in question or their sources.[67]

In the case *Nnachi Ephraim v. Federal Republic of Nigeria*[68] In this case the appellant filed an appeal to the Court of Appeal against the decision of the lower court in respect to charge of offence where an operator of a cybercafé must register with the Economic Financial Crime Commission and thereby committed an offence under section 13(1) (a) of the Advanced Fee Fraud Act of 2006. The judgment was delivered by My Lord, Theresa Ngolika Orji-Abadua, J.C.A., raised an issue to determine the guilty of the appellant as follows:

'for a person to be guilty under section 13(1)(a), the person must be in the normal cause of business, provides telecommunications or internet services, or must be the owner or the person in the management of any premises being used as a telephone or internet café or by whatever named called. I must observe that the fact that the signboard of Primegate Cyber café is posted at No. 1 Okpara Street, Abakaliki, Ebonyi State, notwithstanding, there must be some overt act on the part of the owner of the cyber café to prove that he actually provides telecommunications or internet services to the public. There was no shred of evidence adduced by the prosecution establishing that Primegate cybercafé was indeed providing telecommunications and internet services at No. 1, Okpara Street Abakaliki, Ebonyi State. The fact that the signboard of Primegate is hanging there at does not constitute any proof that the said cybercafé was providing any internet services at the said address. I think the saying; 'the hood does not make the monk' suits appropriately here. All the document tendered before the lower court profoundly showed that it was Artifice colony cybercafé that was indeed providing both the telecommunication and internet services at No. 1, Okpara Street Abakaliki and not Primegate. PW. 1 admitted that no investigation was carried out by the EFFC to decipher whether Primegate cybercafé was indeed taken over by Artiface Colony Cybercafé or not. They did not obtain the tickets and receipts normally issued to customers to strongly establish that it was the Primegate cybercafé that was running the said business. The question is; if there was no proof that Primegate was indeed offering any internet or telecommunication ser-

59 Section 13(1),(a)-(b) *Ibid*.
60 Section 13(2), *Ibid*.
61 Section 13(3), *Ibid*.
62 Section 13(4), *Ibid*.
63 Section 13(5), (a), (b) and (c), *Ibid*.
64 Section 13(6), *Ibid*.
65 Part III, *Ibid*.
66 Section 14, *Ibid*.
67 Section 15, (a)-(b) *Ibid*.
68 (2012), LPELR-22363 (CA), see also, is in the Court of Appeal of Nigeria, on Tuesday, the 10th day of July 2012 with Appeal Number, CA/K/C/312/2010.

vices, where then lies the offence? It is only when the cybercafé or person is offering the services enumerated in Section 13(1) (a) of the Advanced Fee Fraud and Other Fraud Related Offences Act, 2006 that person or entity is required by law to register the same. A moribund or defunct company, whose signboard is still hanging out on its former business address without iota of proof of it running any business there at, cannot be said to be carrying out the same services it had wound up, merely because of the continued display or affixation of its signboard at its former business address. It is not an offence to display a signboard, but, it is an offence to carry out such internet or telecommunication services or being the owner or person in the management of any premises being used as a telephone or internet café without registration of the cybercafé. There must be proof of usage of the place as a telephone or internet café. This was lacking in evidence proffered by the prosecution in the instant case. It is glaring that the judgment of the lower court was not properly guided in line with the principles of law. The court terribly erred. Accordingly, I find the decision of the lower court as being perverse.

Nigeria Cybercrime (Prohibition, Prevention etc) Act 2015

The Act is an enactment of the National legislature of Nigeria which has been passed by the Senate and which carries the assent of the President of Nigeria, President Goodluck Jonathan at the peak of his tenure before the 2015 general election. The Act provides for its own objectives [69] and shall be applicable in Nigeria,[70] for the concern of protecting of the nation's critical infrastructure against the usage of computer and network as a matter of national security, [71] and as such provides some guidelines.[72] It also stipulates for the Office of the National Security Adviser has a major role to play [73] and provides for the punishment of offenders.[74]

An extract from the Act under Section 15 discussing computer fraud, The Act provides that any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held on any computer, whether or not for the purpose of conferring any economic benefits on himself for another person, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than 7,000,000.00 or both fine and imprisonment.[75]

The Act also provides that any person who with intent to defraud sends electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than N10, 000,000.00 or to both fine and imprisonment.[76] That any person who with intent to defraud, franks electronic messages, instructions, super scribes any electronic message and or instruction,

69 Section 1, (a)-(c), Cybercrime (Prohibition, Prevention etc) Act 2015.
70 Section 2, *Ibid*.
71 Section 3(1), *Ibid*.
72 Section 3(2)(a)-(g), *Ibid*.
73 Section 4, *Ibid*.
74 Section 5(1)-(3), Ibid. the Act has a number of 59 sections and from sections 5-40 discusses offences related issue.
75 Section 15 (1), *Ibid*.
76 Section 15(2), *Ibid*.

commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment.[77]

Budapest Convention on Cybercrime

The Budapest Convention on cybercrime as the international treaty is meant to curb the crimes in relation to computer devices and information technologies; it has a wider application and intent to address the cybercrime across the globe. The increase of cybercrimes today is affecting the nations, corporation and private individuals, users are always at risk and afraid of their businesses. The Convention is an important legislation in the contemporary practices of technology devices. The Budapest Convention encompasses crimes related to internet through the use of internet. The connection has a wide range of application not only limited to internet but to its sister- computer and other related crimes.[78]

The Budapest Convention on Cybercrime is an offshoot of Council of Europe Convention on Cybercrime, Convention on Cybercrime is known as the Budapest Convention on Cybercrime; sometimes refer as Budapest Convention or Council of Europe's Convention on Cybercrime. Usually addressed as Convention on Cybercrime-Budapest, 23.XI.2001[79] and is also reference as ETS 185 – Convention on Cybercrime, 23.XI.2001[80]

The Convention gives a clear identification of the offences which are related to Nigerian perspective. Thus the Budapest Convention will be a great assistance to Nigeria in fighting the crimes; it will add a greater value to the cybercrime bill in Nigeria, particularly by strengthening the law in the area of ISPs operation and the general picture of computer system in relation to the crime. The illegal access warrant the control of the credit card and other identity personalization which are the most prominent offences committed in Nigeria today and such is not only limited to some of the offences highlighted but will cover a wide range of its application in the near future. This is the first factor that Nigerian government is lacking.

The Convention provides for computer related forgery and 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.[81]

Computer forgery plays a significant role in destroying the originality of a document in whatsoever manner, is a crime that gain popularity in Nigeria, because with the use of technology it has becomes apparent that some student undergraduate in the

[77] Section 15 (3) Ibid, see also sub-section (4)-(5) of the Act.

[78] Convention on Cybercrime, available at http://www.coe.int.

[79] Council of Europe, available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[80] ETS-185 means European Treaty Series - No. 185.

[81] Article 7, *Ibid*, see Explanatory Report of the Convention, at No. 81-85.

Nigerian universities and other institutions forged admission letters, result, National Youth Service Corps (NYSC) certificate and other certificates in their favour. This acts of crimes, mandated institutions to used and installed devices that track and identify the originality of the documents. If these provisions properly construed in the Nigerian cybercrimes law by highlighting the major issues concerning the offences and penalty will automatically and adequately addresses this menace in Nigeria.

In a related crime, recently the Ebonyi State University (EBSU) issued a notice to the public on alert that some students are engaged into presentation of forged documents by some criminal cyber café operators across the nation for the purpose of securing admission in the university and some even printed the forged admission letters.[82] Also in the same vain a seventeen (17) National Youth Service Corps (NYSC) certificate were find and discovered to be fake, awarded and used by 17 staff members of Guaranty Trust Bank plc (GTB) in Nigeria. Four of the arrested suspects were in the police custody to be prosecuted in the court while the others are to be arrested.[83]

The Convention also highlight on computer-related fraud 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:[84] any input, alteration, deletion or suppression of computer data;[85]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.[86] Computer fraud is among the prominent crimes affecting the nation and to implore this provision will assist in addressing the crime, looking at fraud is not only limited to credit card but has now extended to online shopping mall server in Nigeria.

Findings

The finding of the paper reveals that advanced fee fraud is among the acts of criminals in advancing their crime net in the area of computer and related device and has also found that such practices have been dominant practices in Nigeria. These practices have long existed but in the traditional concept whereby the perpetrators use fraud and false pretence through the means of the fake cheque and forged documents whereas the contemporary practices deal with the activation of information and communication technology.

The usage of computer related devices to initiate criminal offences has been the prime object of advanced fee fraud acts. It is the finding of the paper that based on the consistent practices of the acts in the related electronic communication; the government of Nigeria enacted an Act which succinctly

[82] 'Fraud Alert-EBSU Alert the Public on Forged Admission on October, 17, 2015, available at http://naijafengist.com/fraud-alert-ebsu-alert-the-public-forged-admission-letter/, accessed on 20/10/2015

[83] A statement issued by the Director Certification, National Youth Service Corps (NYSC), Alh. Hudu Aliyu Taura, on November 15, 2015, available at http://scannewsnigeria.com/news/17-gtb-staff-members-found-with-fake-nysc-certificates/, accessed on 20/11/2015.

[84] Article 8, Budapest Convention, op cit, see Explanatory Report, op cit, at No. 86-90.

[85] Article 8 (a), *Ibid*.

[86] Article 8 (b), *Ibid*.

deals with practices of advanced fee fraud in the telecommunication means, due to the fact that the electronic communication has been a prelude to an engagement of criminal offences.

One issue is that the provisions of the Advanced Fee Fraud Act address fraud offences but not some of the common offences of cybercrimes such as electronic means, for instance the unsolicited messages, emails scams and telephone calls for request to an uninvited, uncontracted transactions or deals usually ensued as a prelude to the initiation of the offence but to perfect such ingredients of the offences, we need to closely examine the substance of the offence. This is where the challenges come in relation to offences under section 12 and 13 of the AFF Act, more often. The Nigerian authorities are unable to establish evidence in relation to such offences of the law due to the lack of mother law that regulates the general nature of offences in relation to cybercrimes in Nigeria. Because such offences are under the purview of communication devices as an introduction process or ways of direction but the main offence that has been committed through the objects of computer and related devices which has become the subject of cybercrime has not been accorded a reception of law in Nigeria.

That only and too created a glitch in the success of prosecuting of offenders under section 12 and 13 of the Advanced Fee Fraud Act and thus has been the challenge in the presentation of evidences and as such not successful whereas the relevant cases under the offence discussed in the paper border more often in section 1 of the Advanced Fee Fraud Act and were successfully prosecuted. Because having cybercrime law existed fully will undeniably change the scope of the trials by amending the charges with the relevant section of laws in relation to the cybercrime offences. Therefore, the paper recommends that a special court is created in the country that will purposely deal with cybercrimes and related matter. Further there is need for special prosecutors from the Office of Attorney General of the Federation and State in the related offences because the classes of these offences deal with computer and technology devices so as to strengthen the smooth operation of combating the practices of advanced fee fraud in Nigeria. Lastly, emulating the Budapest Convention on Cybercrime will significantly lower the rate of cybercrime activities in Nigeria.

CONCLUSION

Advanced fee fraud is a criminal offence affecting the development of a nation and has been among the offences related to computer and related devices that have risen to different levels in Nigeria and thus requires the attention of the government. The discussion on the offence has been the modern practice though it has its own scope in the past years but has now dominated from every angle due to the application of technology devices. The relevant laws have lightly addressed the offences but to complete the application of the law through the objects and subjects of the substance of the offences, there is the need for coherent cybercrime law in the country. In addition, the Budapest Convention has proven to be of significant use and guide to Nigeria in

the fight of cybercrime. The discussed cases highlighted the significance of the acts as well as the application of the law and what is required to the fight of advanced fee fraud to checkmate the acts.

BIBLIOGRAPHY

Advance Fee Fraud, Foreign & Commonwealth Office, available at:

Anah Bijik Hassan, Feunmi David Lass and Julius Makinde. (2012). "Cybercrime in Nigeria: Causes, Effects and the Way Out", *ARPN Journal of Science and Technology, 2*(7): 626-635.

Convention on Cybercrime, available at http://www.coe.int.

Council of Europe, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Department of Justice, Office of Public Affairs, for immediate release on Thursday, April 2, 2009, accessed on 12/1/2016, available at http://www.justice.gov/opa/pr/three-defendants-sentenced-advance-fee-fraud-scheme-cost-victims-more-12-million.

Ehimen O.R and Bola A. (2010). "Cybercrime in Nigeria", *Business Intelligence Journal, 3*(1): 92-98.

Gercke. (2006). "The Slow Wake of a Global Approach against Cybercrime", *Computer Law Review International*, 141.

Gercke. (2008). "National, Regional and International Approaches in the Fight Against Cybercrime", *Computer Law Review International, 7.*

Haraszti, 'Preface, in Governing the Internet Freedom and Regulation in the OSCE Region', available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

Ibikunle Frank and Ewedeniyi Odunayo. (2013). "Approach to Cyber Security Issues in Nigeria: Challenges and Solutions", *International Journal of Cognitive Research in Science, Engineering and Education, 1*(1):1-14.

Ifegwu v Federal Republic of Nigeria, (2001) 13 NWLR (Pt. 729).

ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf;

Joshua Oyeniyi Aransiola and Suraj Olalekan Asindemade. (2011). "Cyberpsychology, Behavior, and Social Networking". 14(12): 759-763. doi: 10.1089/cyber.2010.0307.

OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itut/oth/06/15/T061500000A0015PDFE.pdf.

Oriola. "Advance fee fraud on the Internet: Nigeria's regulatory response", *Computer Law & Security Report, 21*(3): 237.

Pauline C. Reich. (2004). *Advance Fee Fraud Scams In-Country and Across Borders.* Australian Institute of Criminology International Conference, Hilton on the Park, Melbourne, Australia November 29-30, 2004.

Plachta, International Cooperation in the Draft United Nations Convention

against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, p.87., available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

Poullet. (2006). *The Yahoo! Inc. case or the revenge of the law on the technology?* Available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; Goldsmith/Wu, Who Controls the Internet? Illusions of a Borderless World.

Schjolberg and Hubbard. (2005). *Harmonizing National Legal Approaches on Cybercrime*, 2005, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf;

Sheri A. Dillon *et al.,* (1998). "Note, Computer Crimes", 35 *Am. Crim. L. Rev.* 503, 505.

Sofaer and Goodman, "Cyber Crime and Security – The Transnational Dimension", in Sofaer and Goodman (eds.) (2001). *The Transnational Dimension of Cyber Crime and Terrorism,* p.7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

Spy Service Exposes Nigerian 'Yahoo Boys', Krebson Security, Accessed 4/4/2015, available at http://krebson-security.com/2013/09/spy-service-exposes-nigerian-yahoo-boys/.

The Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

Ultrascan Advanced Global Investigations. (2014). p. 13. Available at http://www.ultrascan-agi.com/public_html/html/pdf_files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf, accessed on 20/12/2015.

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations New York, Draft-February 2013.

Zittrain. (2006). "History of Online Gatekeeping", *Harvard Journal of Law & Technology, 19*(2): 253, Available online at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

***