AN EMPERICAL EXTRAPOLATIONS OF CYBER CRIMES IN NIGERIA

DAGACI ALIYU MANBE (Ph.D)
Department of Sociology
University of Abuja
aliyumanbe2009@yahoo.com

ABSTRACT

Cyber crime and cyber criminals in future are more likely to continue keeping steps ahead of the law. This is because; it is a technology-driven social problem. It is only natural that technology will evolve faster than the law. For instance, since the introduction of the internet in Nigeria it has continually broadened in terms of its content and character but it took 16 years to bring the evidence act, an instrument of warfare against internet crime, up to speed. Thus, its control will continue to be reactionary.

INTRODUCTION

Today, only 1/3 of the global community is logged on to the net, yet cyber crime gulps up to $1 trillion annually. By the time, it hits 2/3 the financial weight of the crime could have doubled. Suffice it to say that in the nearest future, more valuables will be lost through the cyberspace as more cyber criminals are being recruited. By the time countries like Liberia with less than 0.2% internet penetration begins to catch up with Iceland that is 95% logged on the situation will worsen (Hague, 2011).

Already, Philip Emeagwali, the internet prophet had prophesied that a society shall come in which individual's fitted with micro chips in their brains shall communicate through e-mail (telepathic mails) and live in smart homes that know their owner's voices.

> *A century from now, the computers at each node of the internet will be a "zillion times" faster and more intelligent rendering the computer and even the internet obsolete. Mean while, bionic implants will rewire our brains into computers… With everyone "logged on" at all times, e-mail will be telepathic (Mayeda, 2005).*

A guaze into professor Emeagwalis future society, suggests that cyber crime in future will involve hacking into people's mind or head to steal their pieces of thought or influence their behavior. For instance, a hired assassin may save his bullet by hackling into the head of his target's doctor and cause him to kill his patient through wrong medications. Even, a political party may hack into people's head and swap their voting plans to their favour.

CONCEPTUAL CLARIFICATIONS

Internet: A computer network electronically interlinked in such a way that they share information (Kent, 1998:8 interlined).

Cybercrime: This refers to any criminal activity carried out in the virtual world of networked computers. Examples are sabotaging or stealing electronically stored data via the cyber space.

Cyberlaw (cyberspace law): It is simply the usual laws brought up to the speed of "the (internet) technological complexities". They are generally meant to regulate human and organizational online behaviours. It covers such things as formation, registration of domain names, conducting electronic commerce transaction by ISPs, and the use of application of the internet by subscribers. It makes room for order, trust and justice in the cyber society.

Cyberspace: It generally means the virtual atmosphere in which online activities are carried out. It is "the area in which you can move around online when you are on the internet, on an online service", or even charting with someone in your blackberry.

Cyber piracy: Any form of illegal copying or mass producing of video software programs, games, books, music for profit making. It is an act of registering a well known name or mark (or a confusingly similar one) as a website domain name, usually for the purpose of deriving revenue" e.g. cybersquating.

Cyberterrorism: Terrorism (the use or threat of violence to intimidate or cause panic especially as a means of influencing political behavior) is committed by using a computer to attack another computer and to make threats of such attacks "against computers, network and electronically stored information and actually, causing the targets to fear or experience harm" and or loss.

Cybertheft: This involves the use of internet-linked computer software to steal someone else's property or to interfere with someone else's use and enjoyment of property". This may be inform of hacking into a bank's computer records to wrongfully credit one account and debit another or interfering with a copyright by wrongfully sending protected material over the internet.

Cyberstalking: This refers to a treat, harassment or annoyance achieved through a battery of e-mail messages sent via the cyber space with the internet of creating fear that an injury will be inflicted on the recipient or a member of the recipient's household".

Cyber payment (Internet or e-payment): An on-line transfer of money usually through internet based payment service.

Patterns of Cybercrime: A regular way of perpetrating cybercrimes or mode of cybercriminal behaviours that have proved to be consistent overtime. Thus, patterns of cybercrime capture the gimmicks or ways by which cyber crimes are committed.

Effects of cybercrime: This entails all the recognizable results, outcomes or consequences of cyber crimes. It may be at the national or international; individuals or organizational spheres.

Cyber Crime Control: All the efforts by governments, scientist, international community etc to ensure that the incidence of cyber crime is minimized. The approach may be legal, technological, or social-political. It could also be regulatory or preventive in nature, provided it is backed up by a legal or moral force.

Mis-governance: This has to do with maladministration, failure of governance or poor management of public resources. The failure of the ruling class to legally control a country, provide basic needs of its citizens and promulgate relevant laws as and when needed. Capitalist greed, money laundering and other forms of corruption are captured here.

THEORETICAL EXPOSITIONS

The issue of cyber criminal behavior in Nigeria may be explained from two different theoretical angles namely:

- Space transition theory
- Differential opportunity theory

SPACE TRANSITION THEORY

The space transition theory was deliberately developed by an Indian cyber criminologist, Jaishankar (2008) to serve as "a separate theory of cyber crimes". The crux of the theory lies in the fact that persons move from one environmental space to another and as they move, they behave differently. He thus, postulated that:

1. Persons with repressed criminal behavior in the physical world may release it as soon as they get into the cyber space. For instance a priest or a child may avoid sexual behavior considering their position and status but get randy once online.
2. Identify flexibility, dissociative Anonymity and absence of deterrence factor in the cyber space may encourage cyber crimes.
3. Criminal behaviours may be exported into the cyber space and vice versa.
4. Intermittent ventures of cybercriminals as well as the fluid natures of the cyber space hinders the control of cyber crime.
5. Strangers may unite online to commit a crime offline wile associates offline can unite to commit offence online.
6. Closed societies are more likely to have a higher rate of cybercrime than open societies.

7. When there is a clash between the norms and values in the physical space and that of cyber space, cyber crime may occur.

The theory offers some vital information as to why internet crimes exists, but it is silent about why one pattern dominates another, especially in Nigeria. Secondly, not all crime is possible online as the theory claims. For instances, robbery which involves physicals contact is not yet achievable online. Notably, gaining access to the cyber space does not guarantee cyber crime since it requires some technical knowhow.

The assumption that closed societies are more prone to cyber crime is unacceptable since available literature proves otherwise (Nwankwo, 2011) above all; the theory is yet to be tested both culturally and cross-culturally.

DIFFERENTIAL OPPORTUNITY THEORY

The differential opportunity theory as expressed in the works of Richards Cloward and Lloyd Ohlin is apparently, the most ideal in explaining the sociological analysis of the patterns, effects and control of cyber crime in Nigeria. The central tenets of the theory can be summarized in the following statements.

- The same institutions that limit people’s access to legitimate means also limit their access to illegitimate means (Cloward, 1959).
- Access to both legitimate and illegitimate opportunities is unevenly distributed in any society.
- The structure and access to deviant subculture produce deviant behaviours (Cloward and Ohlin 1960).

Thus, the issue of Cyber crime in Nigeria is one that the youths are embarking on as a means of survival or a way of meeting up with the posh life-standard set for them by the corrupt public servants who block up all the legitimate means of achieving a poverty free-life. The Nigerian cyber criminal may be likened to a soldier under conditions of warfare gunning for dear life. In Nigeria, cyber crime is more or less a function of a denied rights or needs and values. Hence, cyber fraud, for instance, becomes necessary and supportive for many Nigerian youths left unemployed or unemployable by the social order (Smalleger, 1999:367).

The role of Misgovernance, in blocking the people’s access to legitimate means to upward mobility in Nigeria, is not in doubt. So many graduates have been so frustrated by the age discrepancy in job recruitment process that they now have no other choice than to achieve their dream “any how”. No preacher many convince them to quit cyber fraud when they know that up to $400bn has been cornered into private pockets since independence. No! at least, not when they continue to live among the corrupt public servants who live like gods among men, while the masses stand so small (Sagay, 2010).

Secondly, the theory also explains why all youths cannot pursue career in cyber crime. This, they suggest, is because cybercrime requires computer literacy and availability. To the extent that not all can afford to operate a computer, some cyber criminal aspirants may never become one. The 3rd point is that life style of those who overcome poverty and the attendant “worship” they receive from the society, paves the way for more youths to join the trade irrespective of how far the image of the nation is stained. (Olusesi, 2008).

It is in view of these that differential opportunity theory is hereby adopted as the most appropriate for the study.

RECOMENDATIONS

Educational institutional should install such software as *turnitin.com* to enable the lecturers detects playwright works.

Furthermore, the government must imbibe good governance that will raise stronger structures capable of frustrating corruption and creating enabling environment for citizens to be self empowered.

Importantly, all public and private institutions need to make their security department’s information technology complaint, to shield off hackers who may want to compromise their data base.

It is high time; all the members of the cybercrime working group to created their own special units that must be well equipped with gadgets and skilled minds capable of monitoring, detecting and tracking the criminals. They all must synchronize to achieve the desired result. For instance, a formidable cyber policing unit (as in India) could help in regulating the cyber culture in Nigeria. Hence, control may prove proactive and effective.

Similarly, Nigerian military must equally create an army of white-hat hackers ready to defend our public facilities such as dams, refineries, websites, etc and to attacks our attackers as and when necessary. This has become imperative since the nations tend to have shifted modern warfare to the cyber space.

The national orientation agency must collaborate with the relevant institutions to embark on mass cyber education. This will go a long way to awaken both the unsuspecting victims and ignorant offenders. It will also help parents, guardians and preachers to raise the quality of their socialization drills. However, no awareness creation or sensitization may bear fruit until the common wealth is equitably distributed and effectively utilized.

The Abuja technology village should be speedily built to serve as our national bridge to the information age. This all important project will create conducive atmosphere for talented Nigerian youth to channel their energies and intelligence into more socially acceptable and development pulling ventures.

CONCLUSION

The focus of the study was on the patterns, effects and control of cybercrime in Nigeria. One of the major findings was that both the law and its enforcement were perceived to be largely ineffective in controlling cybercrime in Nigeria. For instance, it was discovered that the general public scored the law enforcement agencies very low even though some of them claimed otherwise.

The study equally surveyed the patterns of cyber crime in Nigeria and found that the three major patterns are present in Nigeria even though cyber theft is the dominant pattern. Similarly, an assessment of the effects of cyber crime in Nigeria revealed that the socio-economic effect is already heavy.

More so, it sought to know the rate at which a special cyber crime controlling unit or department was needed amongst the staff of the institutions and discovered that the need was indeed very high. In the same vein, an enquiry into people's view concerning the relationship between Misgovernances and cybercrime, did uncovered that almost everybody agreed that cybercrime can only be controlled in Nigeria when corruption and incapacity is divorced from the seat of governance. For instance, some of the challenges to law enforcement itemized include lack of political will, high rate of corruption, unemployment and poverty, lack of good governance among others.

It was in line with all these that recommendations bordering on how to re-channel the energy and wizardry of the cyber criminals into more productive and socially helpful ventures; how to proactively curb the menace and avoid some lacuna in our national security by not neglecting a possible attack via the cyber battle field, were made.

REFERENCES

Adaramola, Z. (2011) “Nigeria to launch two satellites into orbit in July” in Daily Trust, Friday, June 24, 2011, pp. 11.

Adeola, A. (2010) “History of internet in Nigeria” in Ada, S. (ed) *Introduction to Mass Communication.* Accessed on 03/10/2011 from www.introductiontomasscommunications2.Blogspot.com/2010/05/history-of-internet-in-Nigeria.html.

Adesina A.A. (2011) Interview granted to “fact file” crew on capital fm, October 2011.

Adler, F., Mueller, G.O.W, Laufer, W.S. (2007) *Criminology and the criminal justice system* (6th ed), U.S: Mc-Graw Hill.

Arase, S.E. and Obaedo, a. (2007) “Hi-Tech (Computer and Cyber) crimes in Arase, S.E. and Iwuofor, (eds) *Policing Nigeria in the 21st century*, Ibadan, spectrum books E, pp. 299-307.

Ayantokun, O. (2006) “Fighting cybercrime in Nigeria” from www.tribune.com/ng/08062016/infosys2.html.

Babalola, A. (2011) “EFCC An organ of Reformation” interview to ZT. Vol 6, No. 1, March, 2011.

Bashir, M. (2011) “NSA: Cyber terrorism days are numbered in Daily trust, Friday June 24, 2011, pp. 3.

Bohm, R.M and Haley, K.N. (2007) *Introduction to Criminal Justice (3rd ed)*, califonia; Glencoe/Mc Graw Hill.

Bontrager, S. (2011) "Richard Cloward and Lloyed Ohlin (1960) and Modern criminology" accessed on 16/12/2012 from www.criminology.fsu.edu/crimthery.

Chapman, C. (2009) "The history of internet in nutshell" accessed on 03/10/2011 from www.sixrevisions.com/resources/the-history

Clinton, H (2009) "The future of Nigeria is up to Nigerians" A speech at a town Hall meeting with NGOs. August 19, 2009 in Abuja. Published in ZT Vol. 4 No3, December 2009 pp. 54.

Cloud and Ohlin (1960) "Deferential Opportunity" as interpreted in www.http://megaessays.com

Cloward, R. (1959) "Illegitimate Means, Anomie and Deviant Behaviour. America Sociological Review, 24(2) pp. 164-174.

Dambazau, A.B. (2007) *Criminology and Criminal Justice (2nd ed)* Ibadan, spectrum Books.

Dion, M. (2010) "Advance Fee Fraud Letters as Machiavellian//narcissistic Narratives" in www.cybercrimejournal.com.

Edozien, C.J. (2009) "We need protection to tackle corruption" interview granted to ZT Vol. 4, No. 3 December 2009 pp. 43.

EFCC (2006) *Advance Fee Fraud and other Related Offences Act*, 2006.

Emeagwali, P. (1997) "Can Nigeria leapfrog into the information ages?" Accessed on 7/4/2011 from http://Emeagwali.com/speaches/igbo/7.html.

Gabriel, C. (2010) "History of internet in Nigeria"… Same as in Adeola 2010 above.

Goodman, M (2002/2003) "making Computer crime Count" in victor, J.L. and Naughton, J (eds) *Annual Editions. Criminal Justice,* Connecticut McGraw Hill/Dushkin.

Grabosky, P. (2010) "9 types of cybercrime" Accesed on 7/6/2011 from www.hku.hk/cybercrime.htm.

Haag, et al (2002) *Computing concepts (1st ed)* New York: McGraw-Hill.

Hague, W. (2011) "The London conference on cyberspace" THISDAY, Vol. 16, No 6021, page 7, Tuesday, October 18th 2011.

Hansen, B. (2003/2004) "Cybercrime: Should penalties be tougher?" in victir, J.L. and anughton, J. (eds) *Annual Editions: Criminal Justice.* USA, McGraw Hill and Dushkin pp: 19-27.

Jaishakar, K. (2007) "Establishing a theory of cyber crimes" (editorial) international journal of cyber criminology Vol. 1. issues 2 July 2007 Retrieved on 31/8/2011 from www.cybercrimejournal.com.

Jedlicka, L.S, (2004) Computers in Our world. Boston; Thomson.

Kent, P. (1999) *The Complete Idiots Guide to the Internet (6th ed)* Indianpolis: Que.

Longe, O.B and Chiemeke, S.C. (2008) "Cyber crime and criminality in Nigeria-what roles are internet Access points playing?" in www.eurojournal.com/ejss-6-4-12.pdf.

Maya, E. (2010) "Cyber terrorism hits Nigeria" www.abujacity.com.

Mayeda, A. (2005) "You Aint seen nothing yet" Accessed on 27/6/11 from http://emeagwali/com/speaches/future/internet/index.html.

Mbasekei, M.O. (2008) "Cybercrimes: effects on youth Devlpt" A paper presented at clean foundations' youth against crimes quarterly interactive forum in Bola Ige Millennium Secondary School Ajegunle, Lagos 1st Sept. 2008 accessed on 14/6/2011 from http://i.genuis.org/member/profile.php./id/1138/post1007.

Molenkap and Saffioti (2001) "The cyber sexual addiction" *journal of Human Development,* spring 2001 vol. 22, No. 1, pp: 5-7.

Numbai Police (2011) "Cybercrime Awareness" from www.cybercellnumbai.com

Njoku, E.T. (2011) "Globalization and terrorism in Nigeria" *Foreign Policy Journal, accessed* on 24/10/2011 from http://www.foreignpolicyjournal.com.

Nkanga, E. (2011) "Non-passage of cyber crime Bill Decried" Retrieved on 31/08/2011 from www.thisdaylive.com.

NPC, (1998) 1991 population census of the Federal Republic of Nigeria: Analytical Report at the National level Abuja.

Nwankwo, I.S. (2011) "Nigeria law: Attacks in information systems: How safe is the Nigeria cyberspace? *International Legal Strategists Group.* Accessed on 14/6/2011 from www.facebook.com/note-php? Note-id=496656445826-52k.

Obiekwe, O.T. (2006) *The Impact of Pornography on Nigeria Youths in Gwagwalada Area Council of Abuja.* (Unpublished B.Sc Project, Department of Sociology University of Abuja, Abuja).

Odekunle, F. (2010) "Corruption: I support life imprisonment and special court" *Our Milestone* Vol. 1 No. 1, May 2010 pp. 74.

Odey, J.O. (2001) The Anti-corruption crusade: The Saga of a crippled giant Enugu; Snap Press.

Ogbunwezeh, E.F. (2006) "EFCC and cyber crimes: The true lessons" Accessed on 14/6/2011 from http//www.nigeriavillagesquare.com.

Oji, C. (2011) "scan: Police rescue Saudi bizman from 'kidnappers" *Daily Sun,* Thursday October 20th 2011. Accessed on 21/10/2011 from www.sunnewsonline.com.

Olakami, J. & Co. (2011) Evidence Act 2011: synoptic guide (1st ed) Abuja, Lawlords.

Olusesi, M. (2008) "cyber crime in Nigeria: A sociological Analysis" Accessed on 14/6/2011 from http://profgave.blogspot.com.

Oni (2009) "Nigeria" Accessed on 03/10/2011 from http://opennet.Net/research/profiles/Nigeria.

Osuji, K.C. (2005) *Cyberlaws: its Application and Enforcement.* (Unpublished LL.B Project, Faculty of Law University of Abuja, Abuja).

Oyesanya, F. (2004) "Nigeria: heaven for terrorist internet communication" Accessed on 7/10/2011 from www.nigeriavillagesquare.com/acticles/femi-oyesanya/nigeria-heaven-for-terrorist-internet-communication?

Oyesanya, F. (2007) "Nigeria internet 419 on the loose" accessedon14/6/2011 from www.dawodu.com/yesanya.1htm.

Peace, (2010) Common wealth internet governance forum from www.commonwealthconnectsprogramme.org.

Rittinghouse, J.W. and Ransome J.F. (2005) IM: Instant messaging security. USA: Elsevier Digital press.

Sagay, I. (2010) "EFCC has given us Hope" An interview granted to Our Milestone vol. I, No. 1, May 2010, pp. 48.

Shelly, G.B., Cashman, T.J., Waggoner, G.A. (1996) *Using Computers: A gateway to Information: World Wide Web Edition. Canada,* Boyd and Fraser Publishing Co.

Siegel, L.J. (2007) Criminology: Theories patterns and Typologies (9th ed) U.S.A Thomson wadsworth.

Ubani, D. (2011) "Dan Ubani, Abia State Commissioner for Information Says Abia state University rape video, a ruse" in www.nesz.onlinenigeria.com.

Uzor, B. (2011) "new Evidence Act paves way for electronic evidence in courts" accessed from www.businessdayonline.com.

Voigt, K. (2011) "Analysis: the hidden cost of Cybercime" accessed on 7/6/2011 from www.edition.cnn.com.

Waccs (2010) "The 1st West African Cybercrime Summit (WACCS 2010): The Communique" Published in www.waccs.web.officeline.com.

Watch Tower (2011) "what should I know about social networking? Part 1" Awake July 2011 :pp. 24.

Waziri (2008) "Anti-graft war: Expect revolution" *Zero Tolerance* vol. 3 No. 2 August 2008: pp. 28.

Waziri, F. (2011) "Towards increasing capital flow to Africa: EFCC's reforms and way forward". Paper presented at UN conference on least developed countries, Istanbul Turkey. Published in our Milestone Vol. 2 No. 1, May 2011. Pp. 34.