THEORETICAL ANALYSIS OF THE FACTORS INFLUENCING CYBER CRIME IN NIGERIA BANKING SECTOR.

Iguodala-Cole, Hope I.
(ATAC)Abuja Graduate School,
No.1 Ikeja Close,Oyo street,
Garki 2, FCT, Abuja
hopecole420@gmail.com.

Anto, Jacob B.
Department of Sociology,
Nigerian Army University, Biu.
PMB 1500, Borno State.
jacobantobidda@gmail.com

Jawondo Abdulhamid I.
Department of Sociology,
Nigerian Army University, Biu.
PMB 1500, Borno State.
&
Ishaya, Daniel L.
Department of Sociology
Faculty of Social Sciences
Nasarawa State University, Keffi
danishayal@gmail.com

Abstract
Over the years, there has been a global distressing growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria to- day, several internets assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, identity theft, hacking, cyber harassment, spamming, piracy and phishing. Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Therefore, this paper focuses on the prominent cybercrimes carried out in the banking sector in Nigeria and presents a brief theoretical analysis of the factors influencingcybercrimes in the banking sector in Nigeria.It attempts to provide an overview of Cybercrime and Cyber-security. The paper also attempts to name some challenges of cybercrime and present practical and logical solutions to these threats. The study strongly relies on secondary sources of data drawn from existing literatures. In conclusion, detection and prevention techniques are highlighted in order to combat cybercrimes in Nigeria.

Key Words.Cybercrime, Phishing, Plagiarism, Security.

Introduction

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which may totally destroy an organization. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola, 2013). This term is used for crimes such as

fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. Cybercrime is a relatively new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories: 1. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, mal-ware and so on. 2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare. The risk associated with cybercrime is immense, and the banking sectors uses approximately $67 billion per Annum (Association of Certified Fraud Examiners, 2016).

Financial institutions all over the world play significant roles in the development and growth of the economy of that country. The effectiveness and efficiency in performing these roles, particularly the intermediation between the surplus and deficit units of the economy depend largely on the level of development of the financial institutions (Ofanson, Aigbokhaevbolo & Enabulu, 2010). In this 21st century, the banking sectors operate in a complex and competitive world which is characterized by changing conditions and highly unpredictable economic climate. Information Technology (IT) is at the center of this global change curve in e-banking system in Nigeria today. The major players in the financial market are the banks and discount houses. The banking sector play the intermediate role of ensuring the mobilization of idle funds from the surplus units to the deficit sector.Globally, cybercrime is a major problem to the Nigerian banking sectors.

Conceptualization of cybercrime

Modern study of sociology focuses on application of traditional sociological concepts in analyzing dynamics in contemporary human society. This marks a departure from the traditional approach of centering on social relation concepts, themes and issues, (Scheim, 1990). It is on this premise that this paper is designed to examine the varied views, models and concept of cybercrime.Cybercrime is a criminal activity that involves a computer network device or a network. In Nigeria, the three-pronged advent of the Internet, computers and the mobile phones gave rise to massive outbreak of cybercrimes.

Scope of the study

The issues of cybercrime has posit a threats to the banking sectors and this has affected the customers trust and perception of their banks, the recent spate of cybercrime in Nigeria, especially the arrest of individuals who are involves in hacking banks websites and also duping foreigners on the internets has posits a threat to the National security, one might be tempted to ask how possible was it for them to have access to the bank details of their victims and even having their phone numbers to the extent of calling them and even sending them message at times, if this problems is not well handle then it will be difficult for individuals to have confidence in the financial institutes. It is against this background that this study is interested in the dynamics of cybercrime in the banking sector in Nigeria, particularly in the light of the fact that its presence is making it difficult for firms and individual customers to have necessary confidence in the financial institutes. This study covers the theoretical analysis of factors influencing cybercrime in Nigeria banking sector from the period of 2014 to 2019.

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime (Hassan, 2012) a. Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival. b. Quest for Wealthis another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to startsmall hence they strive to level up with their rich counterparts by engaging in cybercrimes.

c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crimeknowing thatthey canalways go uncaught.

Cybercrimes in the e-Commerce Sector

The Nigerian economy, includingthe enormous amount of e- businesses, are greatly threatenedby the rapidincrease of e-crimes. E-commerce refers to the use of technology, particularly the Internet, to buy, sell and market goods and services to customers (Michael, 2014). In a recent article by This Day and Vanguard, Senator Iroegbu estimated the annual cost of cybercrime to Nigeria at about 0.08% of the county's Gross Domestic products (GDP) which amounts to approximately 127 billion Naira (Ewepu, 2016).

Effects of Cyber Crime

Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals. Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them. Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity. Vulnerability of their Information and Communication Technology (ICT) systems and networks.

Challenges facing the war against cybercrime in Nigeria

The Executive Chairman/Chief Executive Officer, Nigeria Communication Commission (NCC), Prof. Umar Garba Danbatta has pointed out various challenges involved in the fight against cybercrime in Nigeria. He said the absence of comprehensive and reliable demographic and database; insufficient expertise in the area of Cyber and information security; insufficient inter agency, regional and international collaboration and lack of effective and functional forensics labs, techniques and manpower to match the speed, anonymity and fleeting nature of evidence in cybercrimes investigation are the numerous challenges encountered in cybercrime management in Nigeria. Speaking at the 4th edition of Cyber Security Experts Association of Nigeria (CSEAN) yearly conference, Danbatta stated that the commission's roles and efforts in combating cybercrime and cyber security development is to ensure relevant regulations are created to support security agencies such as, regulation on lawful interception; implementation of national cyber security strategy among others.

Poverty Rate: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries. Corruption: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria. Lack of Standards and National Central Control: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse. Lack of Infrastructure: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices. Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

Proliferation of Cybercafés: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced. "Security professionals and the security industry will have to change as well. Cyber security must become an enabler of business, of lifestyle, of healthcare and of a better society.The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example,

communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents.

This raises very significant problems in terms of jurisdiction, availability of evidence, coordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context. New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that Involve new computational concepts.

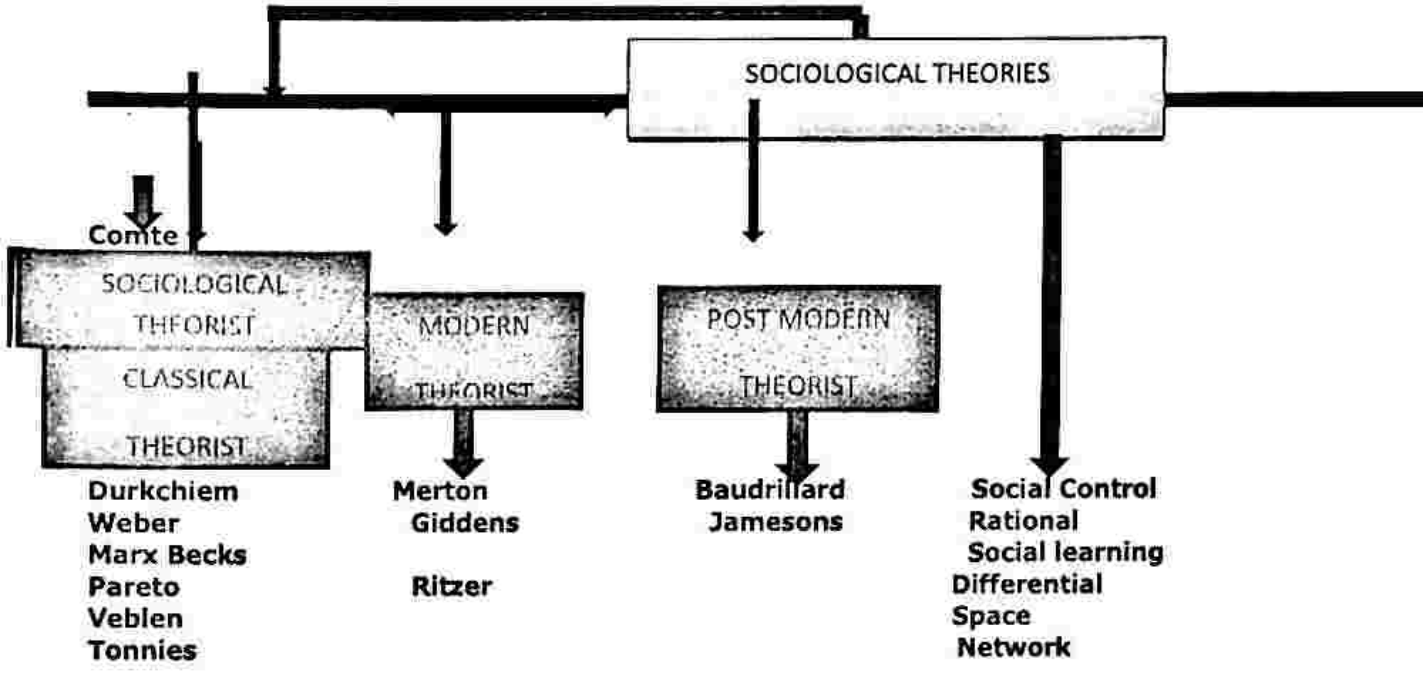
Review of Literature

So many crimes are committed every day in the Nigerian cyberspace. A recent report in the Daily Trust, (2010)by the Internet Crime Complaint Centre, which is a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, revealed that Nigeria is now ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9. 9%).Criminals that indulge in the advance fee fraud schemes (419) are now popularly called „Yahoo Boys" in Nigeria. The country has therefore carved a niche for herself as the source of what is now popularly called 419-mails, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that forbid advance fee fraud. For instance, Nigeria is ranked first in the African region as the target and origin of malicious cyber activities; and this is spreading across the African sub-region,impliedly, the heavy economic impact of cybercrime on the country, (either in financial terms or otherwise), will have an adverse consequence on unemployment rate, social services and international reputation. Therefore, a detailed introduction of cybercrime needs to be presented with the view to fully analyze the indices that make up this crime so that our government and society will be aware of this crime and its implication on the economy.

Theoretical Framework

Model of sociological theories and categories of some sociological theorist whose empirical research explicitly offer a theoretical framework to the understanding of the factors influencing cybercrime.

Theoretical Framework



SOURCE; Secondary Data Survey 2020

Several criminological and psychological theories and their empirical support for explaining cybercrime are reviewed.

Classical Sociological Theorists

Comte's (1865) positive philosophy is his real contribution to social and political philosophy. For him Positivism is the last stage of intellectual development. Reason and objectivity is the basis of positivism of his philosophy. Comte gave more importance to analysis, experimentation and observation. According to him positivism is not only responsible, but inevitable for social reconstruction. It is essential for bringing a new society and new social order. Even though Comte did not talk about crime, but reason which is the basis of positivism has a strong foothold in conduction of crime. Many of the crimes are organized and planned reasonably so that least of the suspect is left behind. Criminals use their brains as much as intellectuals so that no footprints are left behind. They are objective and use reasoning and observation for criminal acts. Even cybercrime has a logical basis as it involves analysis, objectivity, technical knowledge, experimentation and observation.

Durkheim (1893-1933) emphasizes the fact that as the society advances and industrialization progresses, division of labour not only becomes important but also inevitable. Division of Labour is associated with specialization of labour. It is with the help of division of labour that society becomes more efficient, which in turn results in social progress. Progress gives rise to many new vocations and new inventions. Since there is division of labour and specialization, everyone does only a limited job with the result that there is dependence on others who are specialized in their own fields. Durkhiem gave the notion of social solidarity and identified its two major types – Mechanical and Organic. Mechanical solidarity is based on shared beliefs and sentiments while organic solidarity means the integration that result from specialization and interdependence. It is a consequence of moral and material density. Material density denotes a rise in population while moral density refers to the rise in interactions amongst people in society.

Weber (1991) introduced 'rationalization' to explain societies of west who have shifted from traditional orientation to rational and scientific orientation. Rationalization is a process which replaces traditional and subjective thinking with reason and objectivity. He believed that history has seen societies with traditional mode of thinking and modern society is rationalized. Even though rationalization results in technological advancement, weber feared that it would lead to dehumanized and alienated element. Rational society is based on social actions with "rationally pursued and calculated ends", where "the end, the means, and the secondary results are rationally taken into account and weighed". They involve an actor's calculation of the best means of achieving a given end (example how to make maximum profit by online theft) or even a consideration of different end. Weber notes that the utility of each end is considered and there is a ranking of the utility associated with each end and therefore, ends having greater utility are pursued first in comparison to less important ends. All these features are suitably applicable for crime and cybercrime as well.

Marx's (1844-1932) concept of Alienation can be aptly used as a tool for understanding contemporary society. Technology has become a part and parcel of present society and Marx has referred to production as a technical process as it involves technology. Man has attempted to gain control over nature by means of technology. Great success is achieved and man has obtained large degrees of control over nature, time and distance. However, the control and order exercised by technology seem to extend over man himself. It is as if man has lost control over his own instruments. It is the dynamics of technology because humans have engrossed themselves in this all powerful social fact. According to Marx, alienation renders Powerlessness. Indiscriminate use of modern technology has alienated man from himself and people around him. Man has himself become an object or material in the organization of modern technology leading to powerlessness; an aspect of new technological culture that has deprived man from face-to-face relations.

Modern Sociological Theorists

Merton, (1938) opines that gap between approved goals and they creates strain. In contemporary society, success is primarily measured in terms of material achievements and social standing. In a mixed shape of economy such as India, and Nigeria individuals have to choose their own path and work hard to earn living. This leads to competitive nature of careers and employment. Merton used anomie theory to apply specifically to deviant behaviour in various societies. In the contemporary society, success is probably rated a lot higher than virtue. His theory proposes that those individuals, who are underprivileged, may end up as taking honest and socially acceptable path to meet financial success and yet not end up as successful, as those who are not in the same position. This would lead them to question why they would take the honest path when they could be more successful through deviant behaviour. Cyber criminals come from a very diverse background. Those who are in higher schools or colleges are most likely to fit into these theories. They may see how they put a lot of hard work into their studies and development of skills and yet realize that it is unlikely that they could achieve the financial success. As a result, they may see crime as a means to achieve enormous financial success. Any individual would see computer crime as a way and means to make large sums of illegitimate money. Modernity recognizes the advantages of technology and sees risk as its inevitable feature.

Differential Association Theory of Crime

Edwin Sutherland's (1947) Differential Association theory was instrumental in bringing the sociological perspective of crime to the forefront. The Differential Association theory asserts that delinquent behaviours are learned in an environment where interactions exist. Differential association refers to direct association and interaction with others who engage in certain kinds of behaviour or express norms, values, and attitudes towards such behaviour, (Akers, 2006). The

process of differential association explains how normative conflict produces individual acts of crime.

In views of Veblen (2003) process of social change is more or less constant, and one change results in another change. Whole process of change cannot be resisted. For him social change indirectly reflects our technological advances and vice versa. The use of internet has established online communities which have brought new kind of social relationships. Relationships on networking sites also turn real when people are seriously involved. It is through the use of technology that people learn more about worldly affairs. Use of mobiles and internet for instant communication have become commonplace. However, technology has also given rise to a new type of crime such as cybercrime.

Giddens (1991) describes the modern world as a 'Juggernaut 'which is a runaway engine of enormous power which, collectively as human beings, we can drive to some extent but which also threatens to rush out of control and which could render itself asunder". Internet is a product of modern technology moving along through time and over physical space. Digital netizens are the agents who steer it in their directions. Distanciation which is close linkage between time and space is broken through net. In this sense, both time and space are devoid of content and have become pure forms. Thus, with modernization, time is standardized and the close linkage between time and space is disappearing. Relationship with those who are physically absent and increasingly distant are more and more likely. Time and space distanciation is important in modernity for several reasons; first it links local and global domain, second, modern world is able to mould the present, and third, such distanciation is a major prerequisite for the source of dynamism in modernity such as 'Disembedding'.

Beck, (1992) calls modern world as a 'Risk Society'. The emerging new modernity and new technologies are associated with the risk society. The contemporary world has elements of both. Beck labels the new or better yet newly emerging form as reflexive modernity. A process of individualization has taken place in the west. The agents of modern era are free of structural constraints and as a result better able to reflexively create not only themselves but also the societies in which they live. Beck recognized a strange paradox in late modern society; risk is increasing due to technology and science rather than being abated by technological progress.It is not a world which is less prone to risk, but it is "world risk society' In the case of cybercrime one is unaware of the risk that can occur with a single click of mouse.

Postmodern Sociological Theorists

Postmodern society has seen the dawn of sentiments and emotions. In the postmodern era, the disadvantages of technology are recognized. While in modern society individualism was important, in postmodern era, emphasis is on collectivity or groups.

Baudrillard, (1984) believes that there was a time when signs stood for something real, now they refer to little more than themselves. Distinction between what is real and what is fabricated is the cornerstone of the postmodern world. The distinction between signs and reality has imploded. It is characterized by such implosions as distinguished from explosions (of production system, of commodities, of technologies so on). Therefore, just as the modern world underwent the process of differentiation, the postmodern world can be seen as undergoing dedifferentiation, in a world where signs no longer have a natural meaning and are instead manufactured to take on symbolic meaning. According to Baudrillard 'We live in the age of simulation'. It leads to "reproduction of objects or events". Software Piracy or the counterfeiting and distribution of products intended to pass for the original is done by illegal downloading. In photo morphing, a face can be morphed with someone else's body; it is difficult to distinguish real from the duplicate.

Social Control Theory and Cybercrime

Social control refers to the effort of a group or society to regulate the behaviour of members in conformity with established norms. As a result, there are sanctions, or externally imposed constraints. Some of these are informal sanctions and unofficial pressures to conform. When informal sanctions are not enough, formal sanctions come into play. These are officially imposed pressures to conform, such as fines or imprisonment. Through socialization and internalization of cultural norms and values, most people learn to purse socially accepted means even without external sanctions. However, when this learning is faulty or incomplete, it results in deviance.

Space Transition Theory

"Space Transition Theory" is proposed by Jaishankar, (2008). It explains the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical spaceand virtual space. Virtual space provides an individual with such space where he can express his feelings and even vent out his outrage against anyone. Cyber stalking and Cyber defamation are instances where offenders use online space because of its anonymity and widespread approach. It also argues that people behave differently when they move from one space to another. One of the important postulates of the theory is that 'People with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position'.

Network Theory

This theory focuses on a wide range of micro to macro structures. Links occur at the large-scale, social-structural level as well as at micro level. While sociologists talks about 'strong ties', network analyst talks about 'weak ties. Social networking sites preserve culture of maintaining weak ties. Weak ties prevent isolation and allow individuals to better integrate through Social networking sites. However, such integration also gives rise to deviant behaviour on social networking sites, because networks are transitive. If there is a tie between A and B and B and C, there is likely to be a tie between A and C. This link between A and C is weak and therefore could lead to some form of crime in cyber space like Identity theft and hacking of account.

Summary

The dynamic character of the contemporary society is regarded as a result of alarming alterations in social environment. Introduction of new cultural traits into society bring new social changes. Present society is dominated by a complex culture of networking and informationalism. The Information Technology Revolution has brought many changes in the social structure. People rely on technology for many needs. However, it is noted that abuse of technology has given rise to a new variant of crime online such as cybercrime. Emergence of virtual society has associated risks with it. It is characterized by instant communication with anonymity, deception and disguise. Various Theoretical explanations provide an answer to an in-depth curiosity about use and abuse of technology and how it has given rise to cybercrime. The classical theorists relate emergence of crime to the development of science and technology. The modern theorists, on the other hand discuss the effect of technology on contemporary society which they characterize as risk society, encouraging anomie, dehumanization and distanciation. The postmodern theorists see the world as 'hyper real' and 'virtual', full of simulations and technological intensities facilitating spatial interactions and providing anonymity to cybercrime.

Conclusion

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world.

Recommendation

The following recommendations were put forth by this study.

A combination of comprehensive reliable demographic database and technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.Government should make every effort to harmonize laws on cybercrime in such a way as to facilitate international cooperation in preventing and combating these illicit activities.

Reference

Abdulrasheed, S., Babaitu, D., & Tinusa, G. (2012) *Fraud and its implications for bank Performance in Nigeria.* International Journal of Asian Social Science, 2(4), 35-45.

Adebusuyi, A. (2008): The Internet and Emergence of Yahooboys sub-Culture in Nigeria,International Journal Of CyberCriminology, 0794-2891, Vol.2(2) 368-381, JulyDecember

Amaka Eze,Adepoju, A. & Alhassan, G. (2010) *Challenges of automated teller machine (ATM) usage and Fraud occurrence in Nigeria*: A case study of selected banks in Minna metropolis.Journalof Internet Banking and Commerce (JIBC), 15(2), 2-10.

Akindele, R. I. (2010).*Fraud as a negative catalyst in the Nigerian banking industry.* Journal of Emerging Trends in Economics and management Sciences (JETEMS), 1(11), 77-90.

Anderson R Barton C, Rainer B, Clayton R, Michel JG, Eeten M L, Moore T & Savage S. (2012). *Measuring the cost of cybercrime. Rainer B¨ohme, ed., Econ. Inf. Security.* Springer Berlin,Heidelberg, 265–300.

Boateng R, Olumide R, Isabalija S., & Budu J (2011). *Sakawa - Cybercrime and Criminality in Ghana.* Journal of Information Technology Impact Vol. 11, No. 2, pp.85-100.

Britz T. (2009). *Computer forensic and cybercrime.* New Jersey Pearson Education.Cohen LE, & Felson M. (1979). *Social Change and Crime Rate Trends: A Routine Activity Approach.* American. Sociology. Rev. 44(2):588-605.

Gibson, W. (1984), Neuromancer, Pg.4, Ace Hardcover, New York.

Giddens A (2001). Sociology. UK: Blackwell Publisher's pp.306-501.