Journal of Social and Development Sciences
Vol. 5, No. 4, pp. 258-265, December 2014 (ISSN 2221-1152)

Cyber Risks and Fraud in the Nigeria's Business Environment: A Postmortem of Youth Crime

Jegede Ajibade Ebenezer, Olowookere Ibukunoluwa Elizabeth
Covenant University, Ota Ogun State, Nigeria
Ajibade.jegede@covenantuniversity.edu.ng

Abstract: This article examines the opportunities and the negative impacts associative of the use of Internet technology in the era of E-Business. Contextually, it zeroed on the activities of youths as they engage in online fraud as a means of survival in Nigeria. It further postured that the Internet medium tremendously promoted e-commerce and simultaneously created a new form of socio-economic insecurity that is highly unprecedented in the world history. The magnitude of vulnerability and concomitantly the monetary loss often attendant of wireless transaction cross culturally engenders fear, skepticism and disillusionments among Internet users in the cyber environment. In order to minimize this trend, the authors were of the view that a special inbuilt security mechanism attachable to the Internet technology hardwires be provided for the censorship of online monetary related interactions. This unique configuration is expected to serve as checks against fraud and other maladaptive uses of the technology by cyber predators.

Keywords: *E-Business, Fraud, Cyber, Internet, Youths*

1. Introduction

The introduction of new technology into business or commercial arena often offers the promise of a better world, thereby challenging, in the process, our imagination and enhancing human expectations. In this sense, the internet revolution was construed to be an era that would usher in an unprecedented social transformation: new economy, new politics, new world order, indeed a new and advanced species of human beings whose personalities will be dependent on the computer and whose expertise would be transported across the borders of space and time by the power of the internet (Carey, 2005). The motive for the use of internet has variously been attributed to the gratification required by the user (Ferguson and Perse, 2000; Paracharassi and Rubin, 2000; Valkenburg and Soeters, 2000; Perse and Greenberg-Dunn, 1998). Nayar (2004) also asserts that users rely on digital technology to some degree. The users expect to derive some gain from the manipulation of the internet either in the realm of personal communication or in global business. Lupia and Sin (2003) also assert that the technology is seen as a facilitator of development. Internet use is implicated in actualizing economic, social, political, religious, ethical goals. Therefore, the basic factors explaining increase in the use of the internet can be examined from the institutional framework of modern society.

Beyond this general view that the internet will facilitate the much desired development across the world, it has clearly shown that the relationship between technology and society has proved not to be metaphysical but quite materialistic instead (Kalathil and Boas, 2003). The optimistic appraisal of internet technology often overlooks or excludes the possibility that the varied uses can constitute a threat to its rightful employment (of technology) thereby making social relationship harder to maintain and easier to destroy. By implication, the celebrated optimism about the varied opportunities the new technology offers clearly neglected the negative consequences of the medium within the context of group and institutional relationships (Carey, 1988). Just as the growth of cyber technology increases the population of users; it equally expanded risk related factors. The ontology of security remains virtually displaced in the operation of global trade. The probable cause of risk was succinctly captioned by Carey (2005) when he posits that the 'new' man and woman of the 'new internet age' strike one as the same mixture of greed, pride, arrogance, and hostility that history and human experience are yet to comprehend. In an attempt to adjust to the capitalism that characterized the world economy, people especially the youth have resorted to dubious means via the internet to make ends meet. The danger linked to various usages in the internet community is closely tied to the difficulty of securing expected outcomes in group and institutional interconnectivity. Internet technology can be either beneficial

or detrimental to the development of any nation. Cyber-crime represents the negative fallout of internet technology and e-commerce. If left unchecked, it may constitute major setback in national growth and development. This is because nations with high rate of cyber fraud could be blacklisted and estranged from international trade and relations. It is imperative to explore the expressive aspect of crime under conditions of late modernity to better understand the nature of cyber-crime (the major point of emphasis in internet crime involves fraud and related forms of criminality) and identify pragmatic measures to be taken to forestall this menace in the society.

This study therefore, investigates the major factors generating a high rate of cyber fraud in Nigeria especially among youths and also examines this in the context of prevailing socio-economic problems, value displacement and the changing roles of the family which create avenues for experimentation and concomitantly giving birth to negative innovations among a significant section of the Nigerian youths. As part of locating the problem of cyber fraud in its global context, the study investigates the role played by modern internet technology as a facilitator of both legal and illegal businesses. It also considers cyber-crime as a reflection of the continual fall in human condition of living occasioned by the world economic system with its grave consequences on most Third World nations. Also, the current study identified solutions to the problem of cyber related fraud in Nigeria. This has implication for the government, internet users and internet service providers in maintaining secured trade and healthy relations among individuals, institutions and nations.

2. Theoretical Conditions of Nigerian Youths in the New Economy

The 'climatic condition' of the new economy environment can best be described as less predictable and highly vulnerable. The pervasiveness of risks and quantum of monetary loses often occasioned by the use of Internet technology for trade relationships remained appreciable in the newly evolving capitalist economy. It may be of interest to know that current age have been variously characterised as typifying an advanced stage of capitalism (Giddens, 1990). Capitalism today is viewed as intrinsically unstable, restless and depicted by high consequence risks. It is a lived experience for individuals. And in terms of its structure, the ownership of private property under this framework represents a condition of existence for varied number of people. Consequently, survival becomes an individual's sole responsibility. The occupation of this newly evolved stratum in the hierarchical arrangement of capitalism by significant portion of human population globally then presupposes the attendant likelihood or the actual existence of conditions pressuring men toward the adoption or application of both licit and illicit methods in heckling a living under this consistently non-predictive environment. Ironically, research has earlier reported that criminal enterprises which developed with the new economy are economically marginal compared with the productive power of modern industry (Hirst, 1975).

Regrettably, this argument is not valid for all known continents. No matter what the picture painted may seemed like, it is here suggested that one should exercise some level of skepticism on this espoused non parity argument which affirms that the population of those adapting illegal means for survival may appear minimal and has insufficient effect for industrial growth (Cowling, 2008). The advocacy for skeptic attitude in this regard borrows extensively from the measurable impact of crime for most countries in Sub-Saharan Africa. Considering the cost benefit analysis of fraud on investment decision globally therefore, one should rarely know that there is a persistent inverse relationship between the prevalence of fraud in any environment and the attraction of investible capital. The higher the magnitude of investment vulnerabilities projected by global media affecting a target continent, the higher the avoidance of potential investors to participate in trade on one hand and to commit capital for investment in the dreaded arena on the other hand. The net cost of cyber and other related frauds potentially represented in the overall output of diverse crime often injected into the Nigeria's economy environment and the multifaceted secondary impact of criminality most times inhibit the smooth take-off and sustenance of modern e-business in Nigeria. Regarding the socio-economic conditions of Nigeria, it is important to note that significant number of youths has experienced incredible traumatic lives which have hampered their life course and promoted their embracement of crime as one of the options for survival. Cyber fraud then becomes one of the best options toward cushioning the effects of myriad of economic precipitated vulnerability among the youths since Nigeria's environment is economically bad and the current cyber environment can be said to be equally supportive of youth's negative

innovations (Jegede, 2010). In other way round, youths are ill-fated and can be described as victims of the precarious nature of Nigeria's economic environment.

It is on this basis that the life course analysis of the Nigerian youths becomes relevant in this context. The increasing dirt of investment capital promotes the disruption of the life course of youths in this regard. Expectantly, youths are in the stage of transition from schooling into a phase of career selection. The absence of transitional tools (industrial capital) required for soft landing of youths into the employment markets explains to a large extent their involvement in fraud activism. Most unfortunate also is the one sided benefits promotable by the new capitalist order which is practicably impacting positively on the advanced capitalist nations and consistently recorded to be generating the negative impact affecting the developing nations in Sub-Saharan Africa. The absence of required infrastructure and the industrial base needed for the absorption of youths into various productive capacities nurture disillusionment and hopelessness causing the drove of this segment of Nigeria's population into crime. This condition explains more on youths-crime nexus in Nigeria. There is a constellation of factors entrenching and sustaining this segregatual consummation of benefits attendant of the new economy when drawn from both past and present experiences of Nigerian peoples.

There are cumulative life event that impinged upon attainable development and the visible or quantifiable progress reached by the country thereby making the situations of the youths extremely precarious. As a matter of fact, Wall (2001) was quick to point attention to the relationship between youths lived environment and the development of crime related habits. The symbiotic relationship existing between Nigeria's economic situation and the youth's socio-economic condition is best captured in the observation of Giordano et al. (2002). It was viewed that with the existence of socio-economic deprivations, youths acquire more personal deficits, thus raising their chances of acquiring additional acumen for anti-social behaviours. In their various transitions, youths are deprived of the soft landing presopposedly embedded in the global economic environment. They are basically at risk of socio-economic problems and their situation is further compounded by unfriendly political administration lacking in youth welfare promotion in Nigeria. In essence, there are multiple pathway to crime and as well as multiplicity in the classes of youths into crime. Cyber fraud participation only formed an aspect of plethora of crime related activities endemic in Nigeria. In summary, Siegel (2010) gave a vivid picture of the trend in Nigeria when he posited that criminal careers that are rife among the youths constitute a passage and their manifestation draw from personal, social and national/environmental factors traceable to worse economic conditions jointly faced by the citizens and the youths alike. In this case, developmental factors located in bad economic condition, corruption pandemic, high level of unemployment and hopelessness affecting the world of youths explains to a large extent the cyber fraud involvement among Nigeria youths. The up-shoot of this trend is attributable to influences or forces beyond their control and which occasioned a rise in their participation in cyber fraud (Patemoster et al., 1997, cited in Siegel, 2010).

3. Increasing Risks in the Cyber Business Environment

The central concern of this section involves the exploration of the danger deducible from the compromise of private or otherwise sensitive information valuable to the Internet users. It further addresses other challenges touching on the wellbeing of users. The attempt at explaining the former requires the interrogation of the problematic inherent in the Internet-risk affinity in the arena of the global economy. Correspondingly, interrogating the field of cyber interaction, to what extent can one divulge sensitive information online? How can one guarantee the safety of such information without becoming a victim of cyber fraud or other crimes? These entire questions are explained with the view of situating the cost implication of cyber risk in online relationship. Basically, a thorough examination of the nature of risks in the e-commerce environment will warrant making a holistic juxtaposition on the configuration of Internet technology in part, varied uses and their attendant impact on the expansion or contraction of volume of trade relationship globally on the other part. Marshall (2004) was quick to draw attention to the existence of different types of cyber technologies, gamut of uses and which in the process helped broadened our experiences in the cyber environment. Positively cyber technologies enhance the global socio-economic progress in all spheres of endeavours and it antithetically nurtures risks. There are gamut of risks but the one most central to the current discourse is cyber fraud.

Bishop and Hydroski (2009) reported that the speed at which fraud risks evolve is accelerating and will likely continue to do so. A lot of media attention has been drawn to the risks often posed by the Internet (Van Loon, 2008:121). Risk closely linked to cyber fraud has close affinity with anonymity and identity faking in on-line socio-economic interaction. In considering the desirability of exploring risk and youths on-line criminality, therefore, Van Loon (2008) strongly believes that this can only become meaningful when one looks at the role of association (sense of connectedness) and its consequences for social relationship. In a real sense, the Internet usage is about associating with others in the global community for the purpose of achieving a desired end. He views associations of this kind as involving relationships with different degrees and modalities of affect (e.g., trust, solidarity, sacrifice). To grasp the basis for crime in Internet use therefore, we need to explore how such modalities of effect are modulated through interfaces. One must examine how people get into the web of interaction and how trust in all facets of social interaction forms, builds, sustained or otherwise betrayed.

We equally need to understand how trust work in interfaciality. Carey (2005) equally describes this association as a state where today's youths develop the ethic of 'being affected' 'concerned' and at best 'compulsed' by the opportunities the Internet offers. In essence, the awareness of one's friend being Internet compliant compels one to follow suit. This compelling force presents the youths with the opportunities to either align with conventional uses or made the Internet medium amenable to unanticipated uses. Both situations carry implications for e-commerce interaction and as well as the trust needed to remained connected. The Internet is conceived as placing immense pressure on the existing notion of trust prior to the era of cyber mediated interaction. The reason for this is not farfetched, the economic climate that has continued to batter the hope of today's youths can be said to be responsible. Excruciatingly, youths are consistently forced to eke out survival in the face of daunting challenges in the modern world. The affective component driving brotherliness or being one's brother's keeper is rapidly decomposing, thus, diametrically creating exposure to risks. According to Van Loon (2008:122) the lack of affective charge regulating interactions undermines the possibilities to engage in trust. Indeed, all it offers one in its stead is 'blind trust', a form of abandonment to chance with high levels of risk consistently revealing in the magnitude of victimization. It is a well known fact that fraud victims in most cases are innocent people who often suffer because of their altruistic sense of trust. For instead of receiving commensurate treatment based on trust, what they often get in return is disappointment or disillusionment and loss of resources. They suffer from the hands of threat inducers. Who are they? They are both institutions and the cyber predators which each having its own target in the cyber arena.

Mostly affected in e-business environment involve a line of target consisting of funds, products or services often transferred by the Internet users. These threats are consistently posed by e-commerce institutions and the 'opportunists' who manipulate the Internet for both licit and illicit gains. Considering institutional related threats, there are instances where privacy intrusion have been linked to domestic institution such as banks, e-commerce firms and mobile telecommunication network etc. thereby constituting the source of vulnerabilities. When one evaluates the activities of threat inducers locally, experience has shown that Nigeria's youths scavenge and track such information for the purpose of manipulating same to defraud e-business customers and business firms. In most cases where little or no security measure is in place in most of the outlets within which private information are compromised, cyber predators (youths) have the capability to intercept and modify via rewriting, the data that are central to the financial and private lives of their victims through hacking. This exemplifies itself in identity theft that is capable of increasing vulnerability and raising liabilities of customers and e-business organizations simultaneously. Theft encompasses the collection, retention and the invariable use of information relating to name, home address, telephone number, bank details including credit card and private account information of targets of fraud. In the context of information, the aspect of our lives that can be made vulnerable dramatically spans the limit often independently evaluated by the vulnerable groups in the class of Internet users.

There are multifaceted aspects of the lives of cyber users that are readily available to those in need of one information about them or the other; the information which they hold so dear to their existence. This can succinctly be evaluated from the account of Henderson (2006), who rightly observes that the surfing of the Internet for product selection, financial transactions and information sharing in most cases make private information flow outwardly where it is either accumulated in the data base or intercepted by those in dire

need of it. Notable among the 'cyber interjectors' are those who need these information for positive purposes such as product marketers, business speculators and public policy makers. While this group needs virtual information for business promotion and growth, several other jostle for the same to make the cyber space chaotic. Information seeking in the context of the latter follows predatory principle and assumes a dangerous dimension for the e-business environment. Information hijackers who needed Internet consumer information include scammers, cyber fraudsters, cyber terrorists, hackers and a host of others. This information serves a dual purpose. First, such information is needed to facilitate entrant and participation in the e-commerce sites and second it constitutes resource to cyber predators that often used same to defraud Internet users. Consequently, there is a significant unintended effect on the practice of e-business globally as result of the sharp practices which often culminate into loss of money and resources either at a personal level or at the corporate realm. Once the information about what the users hold dear remains vulnerable on the e-business sites, there is the high tendency that they may desist from using the medium for transacting business. This may lower e-participation and e-trust needed to expedite the use of the opportunities on the web.

Due to the risk inherent in cyber business activities, it is important for stakeholders to engage the analysis of risk factors and must therefore take necessary steps to checkmate several threats to transaction often emanating from cyber fraud (Beck, 2006). Risk is the likelihood that a negative outcome will occur in the course of developing or operating an e-commerce relationship. As Beck (2006) notes, risks are real only to the extent that they are anticipated and once they are anticipated, they 'produce a compulsion to act' due to the obligation to 'have to control something even if one does not know whether it exists.' Risk in the world of cyber business is projected as a result of Internet related transaction. Wall (2001) identifies four sources of international business risk. These include competitive risk, transaction risk, customer induced risk and business partner risk. Looking at the current concern, competitive risk is mildly applicable as it has no direct bearing with fraudulent activism in e-business environment. Although, there are cases of hackers outwitting each other for superiority in the cyber space, this level of competition may not carry significant effect for global business when one measures the magnitude of risks that are attendant to the e-business arena in the late modernity.

However, the future implication of competitive risk in the cyber environment has the potential of assuming a negative dimension. The use of the services of 'cyber enemies' to run against the interests of other competitors has the probability of occurring at a higher scale in the foreseeable future. While transaction and customer related risks are sacrosanct to fraud in e-business, business partner risk also portends third party vulnerability induced risks which seldom occurs. Both transaction and customer risk project consequences for distribution channel and business processes thus affecting payment delivery. Globally, individuals, groups, organizations and nations are faced with the challenges of business drive and risk management. They both engage in economic interaction with others having similar interest and strive to attract the gains achievable through the auspices of e-business. Just in the same way, business organizations are eager to attract potential customers with the purpose of increasing sales and maintaining profitability needed to sustain the life of business ventures. However, such transacting agencies or institutions operate in a dilemmic environment where the identity of potential customers remains difficult to know, complex to understand and at its best indescribable. The exposure to the Internet environment increases our levels of vulnerability and raises a lot of skepticism on the probable outcome of most economic transactions.

4. Risk Implication in Cyber Relationship

To establish the risk implication for e-commerce promotion in today world, researchers must of necessity capture, analyze and report the cost involved in the myriad of risks available in the cyber space. There is an amalgam of monetary, socio-psychological and broad spectrum of economic cost attainable in the Internet environment. A survey report released by Cybersource in 2004 gave a rough estimate of the cost of risks in the e-commerce arena. In a study comprising 285 merchants, it was reported that the percentage revenue loss per merchant was relatively flat for the years surveyed. However, the total dollar to fraud increased substantially from S1.9 billion in 2003 to S2.6 billion in 2004. The rise in dollar loss over this period was attributed to the exponential increase in the volume of Internet transactions that rose from 25 per cent to 30 per cent in the same period reviewed. In 2004, merchants estimated that an average of 1.3 percent of their orders were fraudulent. 15 per cent of the merchants indicated that the average of fraudulent orders were

more than 20 percent of the total orders for the period. The median value of these fraudulent orders was S150 or 50 per cent above the average value of all valid orders. 58 per cent of merchants surveyed confirmed acceptance of orders outside the USA and Canada where the transaction and study took place. The fraud rate for these orders was approximately 49 per cent or 3 times higher than fraud rate affecting domestic orders. The Federal Trade Commission (FTC) of the United States also reported that there were nearly 25,000 cases of reported identity theft in 2006 (Mitra, 2010). The above report espouses the interaction between organization offers, consumer orders and the risks induced to the flow of trade in its global context. The cyclical relationship existing between investment and fraud activities is thus explained in the report. Risk is ever present in business but its nature, extent and implication is largely determined by the volume of trade, its financial implications and the profit and loss incurable. The Internet increased the magnitude of global trade exponentially, and it simultaneously created a loophole where cyber criminal exploits for their selfish interests. The danger involved in this regard is transnational in nature. As a result, Guerra (2009) argues that the world is closely heading towards a cyber storm. This vulnerability is made more real by the existence of recession globally. Apart from the effect of recession, the availability of malware needed to intensify the operational frontiers of cyber fraud is ridiculously accessible at give away prices. He gives three reasons why cyber crime remains astronomically high. First, he identified low barrier of entry as a factor.

Second, he considered the prospect derivable from cyber crime profession as a teaser generating youth's involvement. This is hinged on availability of e-gold riches obtainable through expenditure of less stress endemic in cyber environment. Lastly, this involves the guarantee of virtually no risk of getting caught and prosecution. Van Loon (2008) corroborates that cyber criminal can now acquire advanced malware capability for as little as $300 in the open market. This is capable of increasing the number of jobless youths that may embrace the prospect inherent in cyber fraud. Considering the future trend of cyber fraud, Guerra (2009) projects that three important indicators could best explain what may likely happen to spatial interaction. First, he opines that more people are likely to become vulnerable because of the continued complexity of cyber crime environment. Second, desperate people with technical know-how requisite to cyber technology manipulations are more likely to turn to fraud as a way out of excruciating effects of economic down-turn globally. Finally, he was of the view that mitigating the consequences of cyber crime may likely be low owing to reduced income received by both private and public corporations due to low resources sustained by unabated recession. In conclusion, Guerra draws attention to the fact that abysmally low focus and investment may be directed towards the prevention or amelioration of cyber risks. Looking at the projections, the posturing of Guerra seems ethically wrong especially when evaluating his last submission on cyber security intervention. This position is antithetical in so far as insecurity breeds spontaneity and active resistance from the parties exposed to risk. It will be suicidal for an organization at the brink of collapse to express less concern to those things that are likely to salvage his continued existence. In a view, more resources may be galvanized to succor those under threat and diverse measures or strategies may be devised to arrest the trend. In a way, low focus and de-investment constitutes a form of withdrawal syndrome which may arrest the tide of cyber risks on a temporary basis while the future implication remained unattended. It is our opinion that a far more reaching strategy be adopted to solve the problem of cyber risks globally.

5. Arresting the Tide of Cyber Risks in E-Business Environment

In addressing the challenges of cyber risks cum Internet fraud, the nature of fraudable events must be considered. At the centre of cyber risks lay both the Internet medium and the gamut of uses (including human treachery) in accomplishing trade transaction. The porosity of the Internet technology have been widely reported in research (Wall, 2001; Biegel, 2001; Goldsmith and WU, 2006; Graham, 2009; Asokhia, 2010; Mitra, 2010). Apart from the fact the technology facilitates fraud and promotes cyber risks, the use of the Internet has often generated threat to personal and financial information of the transacting parties. In this wise, a comprehensive approach to checkmating cyber risks and fraud is hereby proffered. These will involve inputs from the technology manufacturers, e-business and other allied institutions and the complimentary roles of the e-customers and private users. First in the line of solutions involves suggestions in the class of anticipatory precautions. This requirement is believed to be essential to nipping of risks and fraud at the bud. The special concession advocated here represents the need for the manufacturers of technologies to be security conscious or make up their minds to configure the machines so as to prevent fraud on one hand and to protect their customers on the other hand. The component of precautionary method required of

technology manufacturers involves the installation of spywares and other measures in the computer that will be able to notify e-customer or any other beneficiary of computer technology if their information have been infiltrated or compromised. A third party user or hackers outside the permissive range of e-commerce discussants should completely be blocked out. This can be done by the use of codes whose meanings are offline. In this regard, hackers can gain access to the software of a computer, assess little information but will be unable to unravel coded data whose password only exist offline. For instance, the frequently asked questions (FAQ) can be coded and adapted to this method. The next level of anticipatory precautions affects the Internet service providers (ISP) who takes charge of server related insecurity. They are expected to guarantee the security of the flow of the e-commerce interaction and develop the capacity to arrest the presence of malwares. Making clarifications from their clients (access control) on the authenticity of the identities of the users will also help checkmate the challenges relating to identity theft. ISP group can also fortify their base by installing security gadget such as Secure socket Layer (SSL) in addition to other Internet protocol (TCP and IP) to minimize cyber threat or risks.

Second, e-commerce and their subsidiary institutions must consistently engage risk assessment on a regular basis. Detected security risks must be addressed to discourage secondary effects leading to vulnerabilities affecting the status or life of the institution and as well as the well being of the customers. Apart from installing technologies such as capable of arresting threat, such institutions must endeavour to reinenforce the atmosphere of trust. They owe their customers the duty to get them informed about the existence of real and probable risks emanating from the online environment on a timely basis. Protective measure must be taken to forestall a compromise of personal information essential to the financial and domestic survival of the clients and the acquisition of consent is quite important in this regard especially when such information is requested for secondary uses. Institutions are expected to intimate users on basic security practices that will safeguard them from becoming a victim. Locally in Nigeria, profitability is quite low because of high cost involved in the production of goods and services and this may hinder most e-commerce institutions to engage the purchase of softwares that will checkmate the insurgence of identity theft or at best such organization may lack the abilities to undertake a form of insurance policy indemnifying the loss likely to occur in e-business transaction. Nonetheless, it is advisable that e-commerce institutions in any part of the world should strive to engage the admix of these suggested precautionary methods. Finally, e-customers and other users are advised to guide the confidentiality of the information that is so dear to them. They are not totally insulated from the complicities involved in both exposure to risks and loss of resources. Customer's precautionary role is therefore sacrosanct to the sustainability of the e-business in today capitalist market.

References

Asokhia, M. O. (2010). Enhancing National Development and Growth through Combating Cybercrime/Internet Fraud: A Comparative Approach. *Journal of Social Sciences*, 23(1), 13-19.

Beck, U. (2006). Living in the world risk society. *Economy and Society*, 35(3), 329-45.

Biegel, S. (2001). Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyber Space. U.S.A.: Massachusetts Institute of Technology

Bishop, T. J. F. & Hydoski, F. E. (2009). Corporate Resilience: Managing the Growing Risk of Fraud and Corruption. Hoboken, New Jersey: John Wiley & Sons.

Carey, J. W. (1988). The Mythos of Electronic Revolution', in J.W. Carey (ed.) Communication as Culture: Essays on Media and Society, New York: Unwin Hyman pp. 113-140

Carey, W. J. (2005). Historical Pragmatism and the Internet. *New Media and Society*, 7(4), 445-455

Cowling, M. (2008). Marxism and Criminological Theory: A Critique and a Tool Kit. New York: Palgrave, Macmillan.

Ferguson, D. A. & Perse, E. M. (2000). The World Wide Web as a Functional Alternative to Television. *Journal of Broadcasting and Electronic Media*, 44(2), 155-174.

Giddens, A. (1990). The Consequences of Modernity. Cambridge: Polity Press.

Goldsmith, J. & Wu, T. (2006). Who Controls the Internet: Illusions of A Borderless World. New York: Oxford University Press.

Graham, J. (2009). Cyber Fraud: Tactics, Techniques and Procedures. New York: Taylor and Francis Group, LLC.

Henderson, H. (2006). Privacy in the Information Age. Revised edition. New York: Infobase Publishing.

Hirst, P. Q. (1975). Marx and Engels on Law, Crime and Morality' In Ian Taylor, Paul. Walton and Jock Young (Eds.), Critical Criminology, First Edition, London: Routledge and Kegan Paul, Pp. 203–32.2.

Giordano, P., Cernkovich, S. & Rudolph, J. (2002). Gender, Delinquency, and Desistance: Toward a Theory of Cognitive Transformation? *American Journal of Sociology*, 107, 990–1064.

Guerra, P. (2009). How Economics and Information Security Affects Cyber Crime and What It Means in the Context of Global Recession. BlackHat Turbo Talk Whitepaper

Jegede, A. E. (2010). Globalization, Media Culture and Socio-Economic Security in Nigeria. In Ralph A. Akinfeleye (ed.) Mass Communication: A Book of Readings. Nigeria: Platinum Printing and Packaging Limited.

Kalathil, S. & Boas, C. T. (2003). Open Networks, Closed Regimes: The Impact of Internet on Authoritarian Rule. Washington, DC: Carnegie Endowment for International Peace.

Lupia, A. & Sin, G. (2003). Which Public Goods are engendered? How Evolving Communication Technologies affect the Logic of Collective Action. *Public Choice*, 117, 315-331

Marshall, P. (2004). New Media Cultures, London: Arnold.

Mitra, A. (2010). Digital Communication: From E-Mail to the Cyber Community. New York: Infobase Publishing

Nayar, P. K. (2004). Virtual Worlds: Culture and Politics in the Age of Cybertechnology. New Delhi: Sage.

Paracharassi, Z. & Rubin, A. M. (2000). Predictors of Internet Use. *Journal of Broadcasting and Electronic Media*, 44(2), 175-196.

Perse, E. M. & Greenberg-Dunn, D. (1998). The Utility of Home Computers and Media Use: Implication for Multi-Media and Connectivity. *Journal of Broadcasting and Electronic Media*, 42(4), 435-456.

Paternoster, R., Dean, C., Piquero, A., Mazerolle, P. & Brame, R. (1997). Generality, Continuity, and Change in Offending. *Journal of Quantitative Criminology*, 13, 231–266.

Siegel, L. J. (2010). Criminology: Theories, Patterns and Typologies. Tenth Edition. United Kingdom: Wadsworth, Cengage Learning.

Valkenburg, P. M. & Soeters, K. (2000). Children's Positive and Negative Experiences with the Internet. *Communication Research*, 28(5), 653-676.

Van Loon, J. (2008). Media Technology: Critical Perspectives. New York: Open University Press.

Wall, D. S. (2001). Crime and the Internet: Cyber Crimes and Cyber Fears. New York: Routledge