MEDWIN PUBLISHERS
Committed to create value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Cyberspace and Crime Engineering: A Sociological Review

Jegede AE[1]*, Ovia E[2] and Idam SC[3]

[1]Department of Sociology, Covenant University, Nigeria

[2]Department of Languages and General Studies, Nigeria

Review Article

Volume 1 Issue 1

Received Date: July 28, 2016

Published Date: August 17, 2016

***Corresponding author:** Ajibade Ebenezer Jegede, Department of Sociology, Covenant University, Nigeria, Tel: +234 805 303 9200; E-mail: ajibade.jegede@covenantuniversity.edu.ng

Abstract

The complexity of cyberspace and its benefits to modern economies have been substantially accentuated in literature. Cyber environment permits different shades of activism and it as well coalescences myriad of application, pursuits and users both converging in space with the absence of censorship or control. This expanded patronage of space presents gamut of threat to lawful utilization and sufficiently promote insecurity to both financial and information concerns of users consequently, this paper engages a review of the rising rate of vulnerabilities in the cyberspace and contextualized this within the framework of modernist theory of space. It also establishes affinity between space, modern crimes and resultant victimization. Finally, the paper proffer solution to the challenges of cyberspace induced crimes.

Keywords: Cyberspace; Cyber fraud; Victimization; Internet; Vulnerability; Environment

Introduction

The empirical facts portraying the cyberspace as both enabling and disenabling on account of its potentials for accelerating development and inhibiting social progress remained non-contestable. When assessed positively, it should be noted that the medium has revolutionized both human thinking and human activities and this has also resulted into unquantifiable socio-economic attainments unparalleled in the history of humanity. All over the world, man has made significant progress in his quest for better condition of living and yet he has also retrogressed morally in fixing fair and equitable relationship in the age of Internet borne relationship. All this paradox if puts together have been found to converge within the domain of cyberspace. This environment has been reported notorious for its receptance and concealment of cybercriminals that are unabatedly targeting relational concerns of diversities of users of IT systems in this era of virtualization of relationships. With the adoption of e-technologies on a massive scale and the complexity attendant of interconnectivity in the global context, it is most glaring that the rate of risk within the virtual (spatial) arena has exponentially increased and concomitantly, the probability of becoming the next victim looms very high at each successive key strokes on the computer or with a touch of the mouse and worse still at the manipulation of any other social media platforms. The manifestation of unconventional adaptation of cyber technologies ushered in unintended consequences and creates a dilemma in the mind of users. This ensuing dilemic situation in a way queries the utopia the ICT technologies claim to bequeath the modern man. Engaging the assessment of the virtual arena therefore, the platform presents an admixture of jubilations (optimism) and bewilderments (pessimism) that collectively form the basis of responding to the happenings or vulnerabilities in the cyber environment. The core of vulnerability in this regard is inherent in the manner the medium functions to increase financial victimization and promote reputational damages among

stakeholders in the e-space. Asides the economic and reputational losses attributable to the cyberspace, Baylon [1] equally reports on militarization of the space by states with varying degrees of ideologies and their collective efforts at intensifying the vulnerability level already attained within the space. This form of rivalry tends to promote potential threat to innocent 'comers' to the cyber arena to the end that activism towards outwitting each other raises the level of victimization.

Similarly, Brito & Watkins [2] have earlier notified on the destructive potential of the cyberspace in facilitating the use of weapons of mass destruction. These referential pointers on the character of the cyberspace deduced from empirical studies are clear indicators that the use of cyberspace is fraught with a particular challenge or another and these unanticipated situations are often promoted by the volume of interests booking a place in that arena. However, drawing an inference from the submissions of the above scholars, one should rarely know that the cyberspace is not entirely innocent as often depicted or interpreted in the context of the aggregate viewpoints of majority of technology critics who often construe it to be safe and enabling. Taking this eulogy at face value will make the other side of the workings of the cyberspace to be ignored. It then becomes important that researchers and other stakeholders venture into unraveling the myths behind the operationality of the cyberspace. Achieving this will require the engagement of analytical review of the operationality of the new space and this will be complimented with pragmatic provisions for cybersecurity. In essence, analytical focus should be directed at the assessment of both licit and illicit capabilities and uses of cyber infrastructures in order to arrest the tides of its negative impact on development. Consequently, this review narrows itself to the constructive examination of the configuration of the cyberspace, situates its epistemological foundation and establishes its affinity with modern cyber fraud. It concluded by making far reaching suggestions toward the alleviation of vulnerabilities and ultimately the eradication of cybercrimes.

The Configuration of the Cyberspace

The information need, absorption and the production of affinal society informed the construction of the spatial environment. Within this environment, there exists gamut of spaces in which the cyber technology gained expression. Cyberspace represents a global electronic medium [3], and can be described within the collective and descriptive term from everything from the Internet and the World Wide Web, and the imaginary or metaphorical space that it exists in [4]. It represents the point where the information is, an experiential, but also an imaginary space, the imaginary site of the e-mail conversation and space of the chat-room [5]. This medium consists of a wide range of technically constituted environments in which individuals experience a location not reducible to physical space and that which allows the free flow of interaction across different territories [6-8]. It entails an existence of a community thus as it were creating virtual reality. Cyberspace is both an extension of social relationship as well as capable of generating new relationship hitherto unknown in the field of communication. It is a point where the messages, words and instructions that a user sends through the Internet and other medium utilizing the cyberspace and the answers resulting from such conversation or interaction meet, interact and change tracts from one destination to another [9]. The cyberspace constitutes a medium where myriads of conversation translated into stream of codes sent by radio and text and wired messages take place in space. It is a medium which allows for shared appreciation of media event, life conditions and social progress.

Cyberspace is that imagery space that exists in, on and between computational devices. It encompasses technologies, uses and users, experiences, stories and images [10]. This field is viewed by Thieme [11] as the host or hive of much memetic and viral diffusion and infection. Brown [12] also views the space as an unregulated and irregulable space. It is peopled and people driven environment and intricately connected to human agency; it is a medium which constantly reminds us when we sit in front of the computer terminal that we are simultaneously…relocating ourselves in the space behind the screen, between the screens, everywhere and nowhere [13]. Cyber exists within a very real social, economic and political context. It is a created virtual community consisting of diverse users, operating in a world without boundaries; facilitating anonymity and bridging the gap in socio-economic interaction amongst interested parties (human-machine interface) [14]. Bankowski & Mungham [15] conceive of virtual 'as largely a term used to obfuscate, through connotation of oneness and togetherness, the real divisions in society. The advent of the cyberspace instantiated the Internet and as a matter of fact the two is quite synonymous as presented by several scholars [16,17]. There are number of challenges closely knitted with the use of cyberspace implicating both the macro and the micro structure of the human society. Considering the macro level analysis of the cyberspace, one will notice that global governance (eroding the scope of the nation state), group behavioral

censorship and interactional control are continually mitigated or puts in another way obstructed by extraterritorial, complicating and unregulated attributes of the cyberspace. At the micro level, the cyberspace both enhances and inhibits institutional efficiency. Just as it creates the opportunity to reduce time and space, the cyberspace equally move further away from the customary appreciation of unraveling global event and ultimately dislocating the ability to predict with some level of exactitude the method that is appropriate for arresting the trend if laden with negative cues.

Although, there are gamut of areas affected by the current development, this paper will limit its scope to thematic review of cyberspace implication for understanding crime activism, social vulnerability and control. It has earlier been noticed that apprehending and prosecuting cyber criminals is complicated because of the intercontinental nature of the cyberspace [18,19]. In essence, beyond the optimism about the role that cyberspace plays in the global interaction, the medium presents a little prospect for criminalizing illicit behaviors. Kohl [20] argues that the cyberspace poses qualitatively new problems operating outside the traditional comprehension and prosecution of crime. Its derivative, the Internet is implicated in crime multiplication on a global scale. What makes the Internet amenable to crime uses involves its attributes. The medium is inherently open and extremely dynamic and by nature allows attacks in general to be quick, easy, inexpensive, and often times difficult to detect or trace [21]. The porosity of the Internet to attack and manipulation by the criminals was also supported by Campbell et al, [22]. Crime activism is made easy at the click of a button and made concealable by its virtualness. The consequences of these puts together affect nations, organization, individuals and thus requiring scholarly attention.

The Description of the Cyberspace

One at the outset must admit that traversing the history of cyberspace will be a herculean task for two obvious reasons. First, the space is a metaphoristic construction and second, it portends a state of technological utopia [23]. Exploring its metaphoric existence, Holeton [24] contends that the cyberspace is by no means a finished product, or some complete thing "out there" that is visibly accessible to any commoner. It is an intangible space accommodating information of various magnitudes. Similarly, ISO/IEC [25] accounts that the cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. The development which ushered in the cyberspace is closely linked with the era of the late multinational capitalism identified by which is basically depicted by nuclear power and electronic machines. It also coincided with the era of science identified by Giddens and era of informational capitalism reported by Manuel Castell. Its fundamental features is represented in machines of symbolic reproduction—cameras, computers, video, movies, tape recorders, fax machines collectively functioning to remove the direct connection between human production and its symbolic representation [26].

Cyberspace embodies all other operations taking place in the virtual community. These involve cybercrime, cyber war, cyber terrorism, cyber espionage, cyber security and host of others. William Gibson introduced the world to cyberspace, a vast, geometric, limitless field bisected by vector lines converging somewhere in infinity, permeated by the data systems of the world corporations [27]. The Internet, cell phone, e-mail, text messaging and social networking sites are important and valuable in rendering account on the origin of cyberspace. The space is often account for as the super highway powered by wired or wireless capabilities of telephones and networked computers with cable and satellite TV's capacity to transmit thousands of programs via the system of the Internet [28]. Stratton [29] also locates the origin of the cyberspace in the advent of the telegraph which occurred in the first half of the nineteenth century. He argues that it is not the emergence of the computer and the microchips that ushered in the cyberspace but rather the pragmatic attempt at speeding up information circulation time causing the separation of communication and transportation. By Stratton's assertion therefore, the development of global telecommunication and that of cyberspace are inextricably intertwined [8]. The role of the new electronic technologies in the advent of cyberspace was earlier accentuated by Bukatman [27]. Its origin is drawn from a sort of computer simulation of the future, or the possible, within the framework of the real.

A comprehensive conceptualization of the cyberspace was engaged by Rajnovic [30] via the engagement of cross-national definition of space. From Canadian perspective, cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship [31]. German perspective views cyberspace as the virtual space of all IT systems linked at data level on a global scale. The basis for

cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks [32]. The UK Cyber Security Strategy [33] also conceives of cyberspace as an interactive domain made up of digital networks that are used to store, modify and communicate information. It includes not only the Internet, but also the other information systems that support our businesses, infrastructure and services. The US National Security Presidential Directive described cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

Modernist Theory of Space

In the real sense of it, the cyberspace defied any substantive sociology theoretical explanation since its ramifications extend beyond all existing classical ideological domain. The realization of this limitation spurred Giddens & Sutton [34] to assert that the next stage of action for sociologists of the media will be to study the new digital media and this may as well mean devising new theories that will take account of the Internet. The most comprehensive ontological explanation of the cyberspace is offered within the modernist and postmodernist tradition of sociological theorizing. Within the context of the postmodernist view of Brown's symbolic realism for instance, the cyberspace just as the universe is seen as existing for human through communicative action. The search for the ultimate reality of the cyberspace in the same light of the universe, constitutes a fruitless effort, hence it forms one of the symbolic construction in the world of interactive communication. Cyberspace represents a conglomeration of functioning to mediate communication. These technologies foster the development of social spaces of virtual reality that combine sociability and experimentation [35]. It is fundamentally part of the products of modernity. The theoretical cues required in the field of cyberspace therefore are embedded in the emergence of new society birthed by revolution in informational technology as theorized by Manuel Castells. The network society developed by Castells is within the framework of modernist theories which engage the critique of the problems posed by the modern world. It rest solidly on its account of social change in the communication age and it functions to capture the period of massive social and technological transformation of today. Castells posits that advances in information technology, and especially the rise of the Internet, are fundamentally transforming the core structure of networks in our own time [36].

The core of Castells argument in this tradition of sociological theory lies in what he conceptualized as information technology paradigm comprising of five unique characteristics that are both portraying the features of modern information technologies endemic in the cyber environment as presented by [37]. First, informational technologies consist of technologies that act on information. Experientially, the cyber environment is the hub of interactional activity both social and economic coupled with myriad of interests often channeled through the super Iway [38,39]. Second, their functioning is central to the continuity of human interactions and hence they are pervasive in their effects. The information technologies have consistently promoted the flatness of the world by making information on virtually all subject matter of human material life available at relatively no cost to the end users. Third, the systemic uses of such technologies are defined by networking logic, enabling them to affect a wide variety of processes and organizations. The superlative quality of this medium surpasses those that preceded it in term of coverage, precision and timeliness. Fourth, in its configuration and adaptability, these media technologies are highly flexible thus permitting their easy applicability and reconfiguration in response to change. They are collapsible, potable, and configured for mobile operationality. Finally, the specific technologies associated with information are merging into a highly integrated system. There is amazingly interlocking or connectivity of new media technologies with a single medium possessing the capacity to perform the roles of several others. The birth of cyberspace therefore lies in the revolution of the merger of mass media and computers thus producing real virtuality [40,41].

Contrary to the past, mediatic experience of space represented as 'the space of places', there arose new mediatic space which is 'the space of flows' that is made up of networked places [36]. There is the instantiation of the world dominated by processes and which simultaneously substitutes the world requiring physical contact and interaction in a specified location. Castells argues that modern man has entered an era of 'timeless time or flows' helping information to be available anywhere and everywhere without the barriers of physical space in an instantaneous manner made possible through the cyberspace. This is in line with time-space

distanciation of Giddens; time-space compression of Harvey [42] and Virgilio's [43] annihilation of space. The new space is made up of network linked by interconnected nodes with the resultant implication of making the modern world a network society characterized by 'virtualism' and 'informationalism' [37]. The cyberspace promotes convergence thus creating massive increase in the number and types of opportunities to connect with others in the boundariless space of the cyber world [44]. It offers power to those who can create publish and manipulate information (p277). These enormous advances in communication technology, especially the Internet and spread of mobile telephone that are facilitated within cyberspace, have unleashed decentralized networks that facilitate communications on the move and de-sequenced social interaction at great distances from the physical. The realm of the cyberspace is that of the juggernaut that stands outside the control of men [45].

Affinity between Cyberspace and Crime

Quite often, research has shown that the cyberspace is the most modern way to communicate. The expanded patronage of the medium cannot underplay the gamut of threats inherent in its domain. Dilbert [46] espouses that for several years now, it seems that not a day has gone by without a new revelation about the perils of cyberspace. In using the cyberspace, there is something else to keep in mind and this is implicative in the vulnerabilities promoted by diverse crimes existent in the virtual community. Cyber incidents are becoming more frequent, more organized, more costly, all together more dangerous and encompassing a variety of participating actors and methods [47,48]. The cyberspace is a medium habiting wide range of problematic conducts that are consistently posing challenges to the flow of socio-economic interaction on a global scale [49]. It has been described as a place that is rife with ambiguity, paradox and contradictions. Fundamentally, it was conceived as the domain of crimes.

It is a forum capable of bringing the complete transformation of crime in the information age thereby posing a threat to both consumers and other virtual users. Contextually, cyber borne crimes are those crimes that are likely to emanate from modern technology and computers which tends to have a greater implication for the global community [50-55]. Under the cover of the cyberspace, the advent of advanced technology (Internet) has produced a new breed of criminals: criminals who are well organized, well-resourced and have technological savvy. These cyber criminals commit their crimes with great speed, in an environment of cyber anonymity and in most instances, in multiple legal jurisdictions [56]. Cyberspace therefore encompasses all the odds in the real world. There is fraud, pornography, obscenity, stalking, information theft, money laundering, bullying and gamut of crime existing in the cyberspace. These cyber related crimes are committed by some disgruntled and economically displaced people in this world who are capable of causing insolvable problems. But who are they? They represent those lurking in the dark corners of the cyberspace as predators eagerly waiting for their prey. They are the down trodden personalities in the consistently deteriorating economies concertedly looking for a way out of economic lockjam. Cyberspace remains a crime syndicates dream environment for making a lot of money with little to no risk [3] thus as it were, encouraging the illicit uses of the medium.

The Dynamics of Cyberspace and its Implications for Crime Victimization

Cyberspace in view of its complexities requires a comprehensive examination and its resultant analytical product will pave way to the arresting of most crimogenic trends. Attention in this section of review will be directed at the potential and uses of the cyberspaces Bell [13] puts it succinctly that cyber study is quite necessary to comprehend the ways in which cyberspace as a socio-cultural phenomenon is currently being experienced and imagined and very importantly, how it affects victimization. Describing the nature of cyberspace, Clark [57] posits that the understanding of the medium will require the articulation of its purposes which include processing, manipulation and exploitation of information, the facilitation and augmentation of communication among people, and the interaction of people and information. The infectious effect of the cyberspace carries both positive and negative connotations located in diverse or varying types of uses. He was also quick to draw attention to the existence of different types of cyber technologies, gamut of uses and in the process, broadened experiences in the cyber environment.

The potency of its infectious influence lies in the variety of uses that are basically shaped by socio-economic factors and locating the latent function of the cyberspace, this often becomes manifest in the context of uses in local spaces. Positively, cyber technologies enhance the global socio-economic progress in all spheres of endeavors and antithetically it nurtures risks [58]. Both behaviors in the cyberspace can be rationally described as cybercultures. More importantly, the concept cybercultures gained its existence from the postulation of Dery [59] as

encompassing visionary technology, fringe science, avant-garde art and pop culture. It is a way of thinking about how people and digital technologies interact, how we live together. It connotes ways of life in cyberspace, or ways of life shaped by cyberspace, where cyberspace is a matrix of embedded practices and representations. It produces another strand of culture (sub-culture) best described as criminal sub-culture which is quite distinct from the generalized culture having potentials or capable of destabilizing cyber harmony. Part of these destabilizing effects perfectly aligns with cybercrimes, a major concern of this paper. A closer look at this dimension will give us an objective outlook on what the cyberspace is capable of generating. Dant [60] argues that for us to know the workings of the cyberspace that is producing cybercultures, we must appreciate the materialized relationships between users of the Internet and the technologies facilitating the interaction. In essence, to comprehend users culture, Internet uses (licit and illicit), and the interactional flow (both reinforcing trust and the otherwise), the articulation of the thoughts and feelings of the two category of people booking their presence in the cyberspace become crucial.

The exploration of this is firmly located in the dual role of the cyberspace as both enhancer and demobilizer of social progress. Reflecting on its enhancing attributes, most observed indicators explain that the advent of cyber technology and its virtualness create a flight from the ontological insecurity of late modernity and thus limiting the isolation of major communities of the world [14]. However, the existence of this medium and the oneness it offers is not without implications. Concerned by the nature of its negative effect on social relationship, the social implications of cyber technology have attracted a lot of interest across diverse academic fields especially from the point of view of the transformation of societies and whether or not this is predictable in human relationships [61-63]. The significance of cyberspace for crime study then lies in the way in which the technology produces both anticipated and unanticipated consequences for social interaction in the global community. In cyberspace interaction, the virtual/real distinction is blurred and becomes somewhat meaningless, thus affording the criminals the opportunity to conceal their intentions and manipulate tips known about the victim or rely completely on guesses as they presents a bate to the victim. There are cases of the circulation of illegal material online and, pornographic clips. The cyberspace/crime affinity has been linked to ignorance often displayed by most victims on the workings of virtual transmission. Calce & Craig [64] for instance, assert that nearly forty years after the internet's invention, many people still don't understand that sending an email is like mailing a postcard. In succession, user's message travels from server to server on its way to the delivery point and during the trip it can be read or intercepted by people other than the intended recipient. The point of interception of messages by cyber intruders and attackers constitutes the rendezvous of vulnerability in the use of cyberspace in group interaction. Computer Emergency Response Team Report reveals that "the Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. It is also a domain of hate crimes [65]. Basically, becoming a victim of cyberspace induced crimes is a function of the use of cyber product—Internet. The spaces and places of the cyber are crime prone and with the novelty of the physical and material force of the hitherto known crime and the real fear of traditional crime being replaced by other forms of victimization. Victimization of the body is replaced by victimization of the virtual subject [12].

Human exposure to risk associated with virtual community becomes or appears much greater and more pervasive. Discussing current levels of victimization, Brown (2003) [12] argues that when considering the power afforded by the human-machine interface, there is a value-added –edge to victimization (since men are no longer dealing with physical body, and the space of interaction is transcended or mediated by the cyber technology hence who is to be held for one's predicament). More people are at risk of being affected either simultaneously or at different intervals and the possibilities of detection are immeasurably reduced so also is the potential of legal regulation. The potential gains of certain crimes (fraud, hacking etc.) are huge and the resolution of their impact on victims appears difficult. Majorly, victims are left with nothing than the drudgery of reporting and frequenting crime detection units. The pain of victimization can equally be colossal. The gravity of pain is a factor of the loss incurable by any victim in the course of interaction with diverse virtual impostors.

Locating the Core of Vulnerabilities in the Cyber Environment

The whole idea about the cyberspace or on-line communication is not dangerous or evil all by itself; however, happenings in the cyber environment lend credence to the fact that the magnitude of risks associated with this new technology remains incomparable to other risks that preceded it. The cyberspace accommodates all forms of snoops hanging around the cyber environment. These ranges from habitual fun seekers to genuine users

and the arena is also crowded with obsessive criminals who are poised to steal money, ruin the reputation of other users or cause personal harm. The locus of harm resides in the processes which often commence from the activation of interaction by cyber interlocutors and with such communication basically reduced to electronic messages that are mostly transmitted, then intercepted and acted upon by intended or unintended receptors and thus ending in either positive or negative outcome.

When instant messages or e-mails are sent through the Internet, the message disappears as the sender clicks the send button. However, it is important to note that the original message bounces from place to place in the cyberspace and in the process get to the reach of those who do not need to know its content. Such messages are manipulated by cyber criminals to further their pecuniary interests. This they do by gleaning from the content of the message valuable information that may be of vital interest to or affect the privacy of the sender. The exclusivity of such messages cannot be guaranteed due to the volume of interactors in the cyber arena. Because the Internet has expanded so quickly in the past 15 years, the number and types of conversations occurring have increased exponentially [66]. Part of these conversations that appear germane to current discussion involves the use of Internet as a medium of fraudulent business or an instrument of economic victimization. The development of cyber fraud arose concomitantly with the growth of cyber payment system done through complex encryption technologies which facilitate movement of cash (smart cash or digital cash) from both the issuer and receiver. Sloan [67] rightly observes that electronic fund transfer systems are the fundamental building blocks for both the legitimate and illicit movement of money domestically and globally.

This is not a perfect world, it is not always a honest and fair place. We are surrounded by posers, people who put forth a ―package that is not always true. In most cases, victimization is instantiated through deceptive advances often floated by scammers. Technically, scamming involves an appeal or an allurement to share in a fortune mostly coming in form of baits. It necessitates an advance demand for fee or expenses needed to handle a transaction. This equally entails a request for bank account details or credit card number and online password to facilitate transfer of either fund or investment dividends or other gratification or reward for eliciting cooperation from the respondent. Cyber criminals are relatively smart young people obsessively toying with some pranks in a way to fool Internet users into giving them money or information, or unlocking the online door to bank accounts and credit cards. It involves appetizing potential victims on the existence of a medium of financial breakthroughs requiring no effort except cooperation.

Cyber scammers jump start potential victims and at any case in point fire their salvos in form of pushes directed at victims to act promptly just to avoid missing an offer or avowed benefits. Characteristically, scam content is embodied often in anonymous e-mail messages, strongly worded and consistently painting either a gory, terrible or pathetic story of an unfortunate individual lacking heir or relatives or who circumstantially left behind substantial wealth and the secret of which at the moment remained hidden from any other third party but only in the person floating the offer. Evaluating the magical nature of scam messages therefore, victims are portrayed as trustworthy and capable of helping out in such worse situation. Ironically, such mails are couched as if directed to a single recipient but in its actual sense, dozens of people may receive it simultaneous through the use of bot senders. This method often expands the scope of coverage of the scammer and capable of broadening of net needed to capture the attention of vast majority of people. Wealth sharing formular is given in advance to assure the victim on the term of agreement upon which the cooperation is solidly based**.** The gimmick consists of the promise to send money into the account of the victim with the view of repatriating the agreed portion meant for the fraudster. This may necessitate you giving them your account details thus resulting in financial harm in the long run. Every year hundreds or perhaps thousands of people send money or information to one of these scammers. A handful has been convinced to travel to a foreign nation to meet in person with the people involved; some have been threatened, beaten or even murdered [9]. The danger associated with this innovation is the birthing of transactions which reduce the traceability of the beneficiary in case of cyber fraud [68,69]. Money can be circulated between parties in cyber mediated fraud around the world without detection because the cross-border movement of such money is very difficult to ascertain and the effect of dispossessing cash owners of their hard earned cash can be very grievous. Major money transfers between the parties concerned in cyber fraud often by pass central choke points, which regulators of lawful transactions have relied on for monitoring purposes.

It skirts the raft of the reporting requirement normal in legal trade and departs from the expectation of know your customer rule. Peer to peer or partner to partner Internet transactions may provide cyber fraudsters or launderers

with an alternative to electronic transfer systems, thus avoiding the choke points located on cash flow monitoring systems within or outside national boundaries [70,71]. The form of money transfer applicable to cyber fraud involves what can be described as anonymous electronic cash transfer under the purview of which the senders 'and recipients 'identity remains concealed. Fraud proceeds are processed through traditional banks and other financial institutions across diverse countries of the world. These banks and financial institutions act as facilitators of money transfer and play a major role as sponsors of emerging cyber payment systems [72].

The current discussion centers on the role of electronic fund transfer in fraud operation. Considering the volume of payments carried out through several financial institutions in Nigeria for example, the cyber technology has made it easy for transactionary fraud. With several millions of cash processed along the counters of major banks under the medium of money transfer, it is pretty difficult to detect funds with questionable standing. Computerization and the Internet facility make fraud easier to commit, difficult to detect and increases the vulnerability of investors, consumers and other users of Internet technology. The accuracy and the certainty of the yield and remote detection of fraud, provides an impetus to potential fraudsters. Rahn (2000) [73] opines that a close or tight monitoring of these institutions may generate resistance on the part of those in fraud-related and other non-legal businesses. He further believes that the prohibition of anonymous electronic cash transfer will reduce or eradicate the prevalence of fraud globally. Apart from the role of banks and other financial institutions in the facilitation of fraudulent transfer of money, the last step in the process of the consummation of fraud proceeds is that of integration. Money collected from victims all over the world are integrated into the mainstream financial world or used to purchase choice properties that satisfy the taste of the fraudsters. Typical integration of fraud proceeds into the financial systems may involve the purchase of financial instruments (like stocks, bonds, or other credit instruments such as investing in real estate of legitimate business. Equally important is the shadiness involved in the fraudulent transaction because of greed for gain. In Nigeria, resources often procured through cyber fraud are rarely integrated. Research has shown that most of the fraudsters adopt ostentatious living and thereby squandering most of fraud proceeds.

Cyber security challenges and Risk mitigation

The cyberspace related security challenges are more potent today than when cyber technologies were released for commercial uses globally. The colossal loss attachable to the threats posed by illicit uses and outright attacks on Internet communicative technologies in the cyber environment portends quantifiable insecurity to both private and corporate trust. No wonder that Hollis [74] alarmed that "cyberspace is in trouble." The trouble consist of gamut of threats emanating from the incremental rate of malware, computer error, online displaced trust, computer borne viruses, cyber fraud and attacks that are systematically introduced by hackers which collectively require the urgent attention of cyber threat analysts and scientific experts. The existence of this trouble portends danger for the relational life of cyberspace users and this remains a matter of concern in recent times. Fortunately, in a swift reaction to the danger inherent in cyberspace interaction, Shackelford & Kastelic [75] were very apt to report on the growing consensus over the need for nations in the e-environment to bear increasing responsibility for enhancing cybersecurity. The area of focus involves the adoption of long term strategic plans to assist and insulate those within the web of risk in the spatial environment. And in term of component, the strategic plans involve the empowerment of users with skills and information on how best to detect fraudster gimmicks and how to respond to vulnerable advances or situations through adequate mastery of computer know-how, and Internet cum ICT security related expertise to safeguard organizations, intergovernmental entities and nations via deterring, protecting, defending and possibly defeating or eradicating the upsurge in cyber related threats. The effort directed at achieving all these is commonly referred to as cybersecurity.

Consequently, cybersecurity is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and organizations and users assets [76]. The need for cybersecurity hinge on the fact that IT systems are vulnerable to a variety of disruptions from a variety of sources such as natural disaster, human error and hackers attacks, hence the need to engage cybersecurity [77]. According to Nojeim [78] cyber security operated on a national scale will help protect consumers and businesses and guarantee availability of critical infrastructures upon which national economy gains strength and this will invariably translates into national security. The evolution of cybersecurity has been a movement from the relativity in secret concealment engrafted in Internet resources, to the use of security

systems to monitor, repair and defend personal and organization computer systems and networks. In recent times, efforts aimed at guaranteeing cybersecurity focus on data execution prevention (DEP) and address space layout randomization (ASLR) often adapted to mitigate data vulnerabilities [79]. However, with the rising sophistication in threat dimensions located in the evolving cyber-attacks and cyber exploitations, more and more efforts are required to arrest the spate of attacks in the cyber environment. Just in the same way as threat is increasing, it is vividly clear that the web of vulnerability is also growing at par with the level of danger encapsulated in the cyberspace. With the increase in number of criminal networks, cyber forces and hacktivists, there is an unabated introduction and persistence of newer fashion of cyber security threats which calls for special attention [73]. This will entail the use of effective censorship of interactional flow within the cyberspace and the engagement of a deliberate reformation of Internet architecture in order to cut down on the number of users operating anonymously and generating cyber insecurity. Other precautionary measures are identified in the concluding part of this paper.

Conclusion and Recommendation

In assessing the cost implication of the vulnerabilities linkable to cybercrimes, it is quite revealing that the probability of becoming a victim is substantially high. Judging the unprecedented rate of connectivity needed to accomplish myriad of socio-economic concerns of network users, the stage is set for an encounter of both positive and negative outcomes. Redeeming the situation will require IT systems experts looking inward through the re-engagement of network security. The need for increased cybersecurity alertness and the provision of comprehensive cybercrime mitigating measures cannot be underplayed in our attempt at arresting the tide of the ugly orchaotic occurrences now characterizing the cyberspace environment. Security suggested here involves that aptly puts by Pipkin [80] as a process of minimizing risk, threat, or the likelihood of harm. This may equally involve the consideration of adopting measures relating to costing of vulnerability. In terms of cost, individuals, organizations and national entities should endeavor to make provisions for forensic cost, incident and crisis management response cost and litigation cost alongside expenses and settlements needed to insure cyberspace related threats [81]. Given the state of emergency created by the challenges relating to threat to security of information, transaction and other interactions via the web, the concerted efforts of the inter-governmental institutions, cyber technical experts, legal professionals, cyber breach investigators, cyber luminaries and enforcement personnel's and invariably the larger public will be of immense value to checkmating the surge in modern technological (ICT) crimes. By its nature, the typology of acts denoting cybercrimes demobilizes the potentials and the capacity of traditionally known legal provisions and makes crime definition, investigation and prosecution difficult.

Consequently, nations across the globe are therefore compelled to fashion out appropriate legal instruments that will capture the peculiarities of modern crimes and this should be engaged in a bid at neutralizing its effects on most potential victims. Legal regime must take cognizance of the technicalities involved in defining the variations in cybercrimes and responding to it by embedding into the legislations those unique attributes that will assist the justice system to interpret and prosecute cyber related cases accordingly. Equally important is the creation of trained specialize units within national enforcement groups: a section that will be thoroughly equipped in the art of cyber uses, detection of technology driven crimes, investigation expertize in virtual related breaches and ultimately the prosecution. The combination of these will help nip or at best arrest and reduce the incidence of cybercrime perpetration. Information sharing and the dissemination of best practices in technology crime control among law enforcement organization at the level of the international community will reasonably cut down on the activities of cyber criminals and bring them to speedy justice. In achieving the latter, the institution vested with the authority to formulate law must be proactive in reconciling all the nuances needed to obtain the conviction of the cyber criminals. In this regard, modern laws should contain provisions suitable for the presentation of evidences, judicial interpretation and the establishment of culpability or otherwise of any perceived or the actual breach of cyber related laws. The public also owes the duty of keeping abreast the existence of vulnerability posable by cybercrime and the likelihood of becoming a victim if precautionary measures are not adequately taken to forestall the occurrences of such crimes. In all, cybersecurity must be seen as a collective responsibility and efforts at eradicating the posable vulnerabilities must be fully engaged by the stakeholders in the IT environment.

References

1. Baylon C (2014) In challenges at the intersection of cyber security and space security: Country and

international institution perspectives. Research Paper: International security: Chatham House.

2. Brito J, Watkins T (2011) Loving the cyber bomb-the dangers of threat inflation in cybersecurity Policy. Harvard Law School National Security Journal 3: 39.

3. Carr J (2010) Inside Cyber Warfare. USA: O"Reilly Media Inc.

4. Chatterjee BB (2001) Last of the Rainmacs: Thinking About Pornography in Cyber Space. In David Wall (Ed.) Crime and the Internet. London: Routledge.

5. Lessig L (1996) The Zone of Cyber Space. Stanford Law Review 48: 1403-1411.

6. Escobar A (1994) Welcome to Cyberia, Current Anthropology 5(3): 211-231.

7. Ostwald M (1997) Virtual urban futures in D Holmes Virtual politics: identity and community in cyberspace London: Sage.

8. Homes D (2005) Communication Theory: Media, Technology and Society. California: Sage Publications Inc.

9. Sandler C (2010) Living with Internet and online dangers. New York: Word Association Inc.

10. (2008) United States Cyberspace policy review.

11. Thieme R (2000) Stalking the UFO meme, in Bell D and Kennedy B (Eds) The cybercultures Reader, London: Routledge.

12. Brown S (2003) Crime and Law in Media Culture. London: Open University Press.

13. Bell D, Kennedy BM (2000) Cybercultures Reader: A User's Guide, The Cyberculture Reader. London: Routledge.

14. Heim M (1998) Virtual Realism. Oxford: Oxford University Press pp: 162-167, 171.

15. Bankowski Z and Mungham (1981) Lawpeople and Laypeople. International Journal of the Sociology of Law 9: 85-100.

16. Poster M (1995) The second media age. Cambridge: Polity Press.

17. Biegel S (2001) Beyond Our Control? Confronting the Limit of Our Legal System in the Age of Cyberspace. USA: Massachusetts Institute of Technology.

18. Kahai P (2008) Tracing Cyber Crimes with a Privacy-Enabled Forensic Profiling System. In Hamid Nemati (Ed.) Information Security and Ethics: Concepts, Methodologies, Tools, and Applications. UK: Information Science Reference (IGI Global). Pp: 3938-3952.

19. McConnell BW (2014) (Forward) A Measure of Restraint in Cyberspace: Reducing Risks to CivilianNuclear Assets. Policy Report. Munich Security Conference. Munich: EastWest Institute.

20. Kohl O (1999) Legal Reasoning and Legal Change in the Age of the Internet: Why the Ground Rules are Still Valid. International Journal of Law and Information Technology 7(2): 123-151.

21. Quimbo RNS (2008) Cyber-crime and security Policy Issues. UNESCAP.

22. Campbell P, Calvert B, Boswell S (2003) Security +Guide to Network Security Fundamentals. Boston: CISCO Learning Institute, Thompson Course Technology.

23. Goonewardena K, Kipfer S, Milgroom R, Schmid C (2008) (Eds.) Space, Difference and Everyday Life: Reading Henri Lefebvre. Madison Ave, New York: Routledge.

24. Holeton R (1998) Composing Cyberspace: Identity, Community and Knowledge in the Electronic Age. USA: McGraw-Hill.

25. ISO/IEC, ISO/IEC FCD 27032- Information technology- Security techniques- Guidelines for cybersecurity, Oct-2011.

26. Turner JH (2013) Theoretical sociology: 1930 to the present. Thousand Oak, California: Sage Publications, Inc.

27. Bukatman S (2000) Cyberspace. In Daniel Bell and Barbara M Kennedy (eds.) The Cybercultures Reader Second Edition. Madison-Ave, New York: Routledge. Pp: 80-105.

28. William BK, Sawyer SC, Hutchinson SE (1999) Using information technology: A practical introduction to

computers and communications. New York: McGraw-Hill.

29. Stratton J (1997) Cyberspace and the globalization of culture, in D Porter (ed.) Internet Culture, London: Routledge.

30. Rajnovic D (2012) Cyber space-what it is.

31. CCSS (2010) Canada's Cyber Security Strategy.

32. CSSG (2011) Cyber Security Strategy for Germany.

33. (2011) The UK Cyber Security Strategy.

34. Giddens A, Sutton PW (2014) Essential Concepts in Sociology. Cambridge: Polity Press.

35. Castells M (2009) Communication Power. New York: Oxford University Press, Inc.

36. Elliot A (2014) Contemporary Social Theory: An Introduction. Second Edition. New York: Routledge.

37. Ritzer G, Stepnisky J (2014) Sociological theory Ninth Edition New York: McGraw-Hill Education LLC.

38. Juris JS (2008) Networking Futures: The Movements against Corporate Globalization. Durham, NC: Duke University Press.

39. European Commission (EU) (2013) Cyber Security Strategy of the European Union: An Open Safe and Secure Cyberspace. Brussels: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

40. McChesney RW (2007) Communication Revolution: Critical Junctures and the Future of Media. New York: New Press.

41. Cowhey P, Aronson J (2009) Transforming Global Information and Communication Markets: The Political Economy of Innovation. Cambridge, MA: MIT Press.

42. Harvey D (1990) The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change. Cambridge, MA: Blackwell.

43. Armitage J 2000 (ed.) Paul Virilio: From Modernism to Hypermodernism and Beyond. London: Sage.

44. Edwards A, Edwards C, Wahl ST, Myers SA (2013) The Communication Age: Connecting and Engaging. Thousand Oaks, California: Sage Publications, Inc.

45. Giddens A (1990) Consequences of Modernity. Stanford: Stanford University Press.

46. Dilbert RJ (2015) The Geopolitics of Cyberspace After Snowden.

47. Cavelty MD (2012) The Militarization of Cyberspace: Why Less may be Better. In Czosseck C, Ottis R, Ziokowski K (Eds) 4th International Conference on Cyber Conflict. Tallinn, Estomia: NATO CCD COE Publishers.

48. Theohary CA, and Harrington AI (2015) Cyber operations in DOD Policy and Plans: Issues for Congress. USA: CRS Report.

49. Greenfield DN, Davis RA (2002) Lost in Cyber Space: The Web @ Work. Cyberpsychol Behav 5(4):347-53.

50. Castells M (1996) The Rise of Network Society. Malden, Mass: Blackwell.

51. Grabosky P, Smith R (2001) Telecommunication Fraud in the Digital Age in Wall D (ed) Crime and the Internet, London: Routledge pp: 28-43.

52. Lyon D (2001) Cyberspace: Beyond the Information Society? in Armitage J, Roberts J (eds) Living With Cyberspace, London: Continuum.

53. Symantec (2006) Symantec Internet Security Threat Report, Volume X.

54. Wall D (2007) Cybercrime: The transformation of crime in an information age, Cambridge.

55. McGuire M (2007) Hypercrime: The New Geometry of Harm. Madison Ave. New York: Routledge Cavendish.

56. Fick AJ (2009) Cyber Crime in South Africa: Investigating and Prosecuting Cyber Crime and the Benefits of Public-Private Partnerships. South Africa: Price Water House Coopers.

57. Clark D (2010) Characterizing the Cyberspace: Past, Present and Future. MIT: CSAIL.

58. CSIS (2008) Securing Cyberspace for the 44th Presidency A Report of the Centre for Strategic and International Studies. Washington DC.

59. Dery M (1992) Cyberculture, South Atlantic Quarterly 91: 508-531.

60. Dant T (2005) Materiality and Society, Maidenhead: Open University Press.

61. Castell M (2001) Internet Galaxy: Reflections on the Internet, Business, and Society Oxford: Oxford University Press.

62. Jewke Y, Sharp K (2003) Crime and Deviance and the Disembodied Self: Transcending the Danger of Corporeality. In Yonne Jewke (ed.) Dot. Cons: Crime Deviance and Identities on the Internet. Cullompton: Willan.

63. Cunneen C, Stubbs J (2004) Cultural Criminology and Engagement with Race, Gender and Post-Colonial Identities. In J Ferrel, Keith H, Wayne M, Mike P (Eds) Cultural Criminology, Unleashed, London, Sydney and Portland: Glasshouse Press.

64. Calce M, Craig S (2008) Mafiaboy. New York: Penguin Group (USA) Inc.

65. Citron DK (2015) Hates Crimes in Cyber Space: Introduction. University of Maryland Francis King Carey School of Law Legal Study Research Paper No 11.

66. Enteen BJ (2005) Siam Remapped: Cyber Intervention by Thai Women, New Media & Society 7(4): 467-482.

67. Sloan JF (2000) Financial crime enforcement network, testimony before the US House Committee on Reform, Subcommittee on Criminal Justice, Drug Policy and Human Resources, 23 June.

68. Mussington DA, Wilson PA, Molander RC (1998) Exploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies, Santa Monica: CA: RAND Corporation.

69. Rueda A (2001) The implications of strong encryption technology on money Laundering, Albany Law Journal of Science and Technology 12(1): 1-42.

70. Helleiner E (1998) Electronic Money: A Challenge to the Sovereign State? Journal of International Affairs 51(2): 387-409.

71. Weimer WJ (2000) Cyberlaundering: An international cache for microchips money, DePaul Business Law Journal 13(1): 199-245.

72. Group of Ten (2000) Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues.

73. Rahn RW(2000) Testimony on the Future of Electronic Payment in H Rheingold (Ed.). The Virtual Community: Homesteading on the Electronic Frontier. Reading, MA: Addison-Wesley.

74. Hollis DB (2011) An e-SOS for cyberspace. Harvard International Law Journal 52(2).

75. Shackelford SJ, Kastelic A (2015) Toward a state-centric cyber peace: Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. New York University Journal of Legislation and Public Policy 18: 895-915.

76. Von Solms, Van Niekerk J (2013) From information security to cyber security. Computer and security 38: 97-102.

77. Schaeffer BS, Chan H, Chan H, Ogulnick S (2009) Cybercrime and cyber security: A white paper for franchisors, licensors, and others.

78. Nojeim GT (2010) Cybersecurity and freedom on the Internet. Journal of National Security law & Policy 4(119).

79. Cyber Security Report (CRR) (2016) HPE security research. Hewlett Packard Enterprise.

80. Pipkin DL (2000) Information security: Protecting the global enterprise. Upper Saddle River NJ: Pretence-Hall.

81. Ferrilo P (2014) Alert Cyber security, cyber governance and cyber insurance: What every public company director needs to know. New York: Weil G and Manges LLP.