

YOUTH CRIME AND THE ORGANIZED ATTRIBUTES OF CYBER FRAUD IN THE MODERN TECHNOLOGICAL AGE: A THEMATIC REVIEW

JEGEDE, AJIBADE EBENEZER (Ph.D)
Department of Sociology
Covenant University, Ota, Ogun State,
Nigeria.
Phone No: 2348053039200
E.mail: ajibade.jegade@covenantuniversity.edu.ng
Babatayo4sho@yahoo.ca ,

&

OYESOMI, KEHINDE. O. (Ph.D)
Department of Mass Communication
Covenant University, Ota
Nigeria.
Phone No: 2348034628510
E:mail: kehinde.oyesomi@covenantuniversity.edu.ng

&

OLORUNYOMI BANKOLE ROBERT (Ph.D)
Department of Political Science
Covenant University, Ota, Ogun State,
Nigeria.
Phone No: 2348033638029
E:mail: Robert.olorunyomi@covenantuniversity.edu.ng

Abstract

This paper establishes a link between the hitherto known traditional organized crimes and modern cyber fraud. The transnational context of fraud in the e-business environment promotes exclusive anonymity, transactional secrecy and unprecedented vulnerabilities relatively higher in impact and far above any documented assessment of organized crimes that preceded it. Mostly implicated in this emerging trend considered in this criminological discourse are the youths, commonly referred to as the Net Generation. Uniquely, these categories of people are doubly victimized. Just as they suffer acute deprivation socio-economically, they are also systemically made representable under the criminal justice arrangement of most nations due to their incessant involvements in illicit activities. Finally, the paper made an advocacy for prompt state intervention towards arresting the precarious situations impressing it upon the youths to adopt unconventional means to attain survival.

Keywords; Organized crime, Fraud, Modernity, Internet, Economy, Youth

Introduction

Youth's crime is one of the great preoccupations of late modernity. Indeed the notion that youths crime is a uniquely modern phenomenon, that it wasn't like this in time past and that, things are getting worse are not uncommon (Goldson, 2004, p.221). Conventionally, most youths crimes are directed against property but the trend is however changing in the new global environment (Home Office, 2002). Basically, current wave of effort in research revolves around the location of youth's deviance in the organized category. Unfortunately, attempts at locating the exact point and attributes of the organized structure of youths crime has become an herculean task. Albanese (2007) best captured the core of this dilemmic scenario when he puts it in this way 'organized crime remains one of the most fascinating manifestations of criminal behavior, yet it remains one of the least understood'.

The inability to grasp what organized crime entails particularly in the context of youths criminality is made more complex by the role currently being played by emerging networks of cyber technologies which has continue to bring to fore relatively unknown crimes. Apart from the difficulties involved in locating youths-organized crime nexus, its implications on socio-economic interaction globally cannot also be underestimated. The effect and threat attributable to organized crime according to Poole-Robb and Bailey (2002) are to be considered extremely real. Its real nature carries both financial and resource implicated consequences for modern economy. It is on this basis that the complexity in understanding the final relationship between traditionally known organized crime and the modern evolving cyber technology driven crimes becomes important. This paper therefore approaches the organized nature of cyber fraud under three thematic sections which run through this discourse. First, it establishes a conceptual affinity between traditionally known organized crime and the emerging cyber fraud category. Second, it reports on the involvement of Nigerian youths in cyber fraud and further attempts a review of literature to link the complexity of their operation in extant practice of organized crimes. Finally, using Nigeria as a case study in all through the body of the paper, it further identifies major predisposable factors that are both nurturing youth's involvement in the modern cyber technology driven crimes. It however, presents some recommendations to reduce the scourge of cyber fraud in the global arena.

Conceptualizing Organized Crime

Despite long and continuous debates on what organized crime is and the cost of its threat to modern economy, it remains a vague concept (Newburn, 2012, p.438; Siegel, 2008, p.85; Paoli, 2002). Conceptually, the FBI conceives of organized crime as — any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales, region, or the country as a whole. It was further averred that organized crime is a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or the corruption of public officials (Albanese, 2007, p.4; 2011, p.231).

Similarly, a current idea views organized crime as any significant criminal activity planned and carried out for profit by a cohesive group of conspirators (Newton, 2011). Consequently, looking at the various perspectives on what organized crime is all about, few fundamental facts run across both definitions. One, it can be comfortably deduced that organized crime tilts toward acquiring or obtaining money, properties, services and the like illegally. Two, it also implicated a category of people joining together to accomplish crime related operation and are capable of evading if not neutralizing arrest completely. This gave us a vivid summary involving five important elements: conspiracy, planning to commit crime, dealing in illicit or non-existing goods (Van Duyne, 1996), infiltration of legitimate business, taking property through the use of threat or harm and racketeering (Albanese, 2007, p.26).

All these elements are made present both in traditionally known organized crime and modern cyber fraud as explained in this paper. In establishing the organized status of cyber fraud, a few scholars have argued that most organized crimes are transnational in their identities. Quite a number take the position that cyber fraud falls consistently into the category of transnational organized crime which is an offshoot of the known conventional organized crime. Bossard (1990) used the concept of transnational organized crime as representing acts which violate the laws of more than one country. In the same vein, Passas (2002, p.52)

further stresses this definition as he considers transnational organized crime as crimes prohibited by international criminal law, especially those laws deriving their strengths from either the 1994 draft code, multilateral treaties or customary practice by all nations. Equipped with these various positions, this discourse reveals that majority of acts or infringement perpetrated through the Internet often span a geographical boundary in terms of impact. The operation of cyber crime leaves no geographical space untouched and hence can be described as a global organized crime.

Locating Definitional Gaps and Establishing Cyber Fraud—Organized Crime Nexus

There are diverse affiliations between hitherto known attributes of organized crimes and the emergent cyber fraud. Beyond the limits provided in the several conceptions explained above are other impacts recordable in its transnational context and mostly represented in different dimensions of crimes that are not inclusive in the definitions of organized crime (Levi, 2012, p.454). This non-inclusion is due to the fusion of structure of association and structure of activity in most organized crime's conceptual framework often put across by scholars. The gap attendant to the conceptual framework given by the FBI consist of omissions of significant types of crime in the category of organized crime and most especially the area of crime affecting today youths-cyber technology relationship. Reporting on definitional gap, Siegel (2008) laments that sizeable number of scholars held the view that cybercrimes fall short of the distinguishing features of conventional organized crimes. This appears baffling since the word cybercrime have been used interchangeably with other related words by different scholars.

The word is often replaced by other words such as computer crime', computer related crime' or crime by computer' (Sieber, 1998); high technology or information age crime (Brenner, 2004); Internet or Net crime (Morris, 2004); other variants include digital', electronic' (or e-'), virtual', IT', high-tech' and technology enabled' crime (Clough, 2010, p.9). Wall (2001) denotes that the term cybercrime signify the occurrence of a harmful behaviour that is somehow related to a computer. Within the context of these various conceptions, it is clearly evident that modern organized crimes are inextricably linked to one or more of the concepts used by these scholars in terms of current structuration of crimes in today world. Just as we are constantly registering at a mild level cyber intimidations and at the extreme occasionally, we are rather envisaging or at best experiencing cyber terrorism.

Progressively, later observations educate on the existence of newer activities that share the attributes of organized crime. Conklin, (2007, p.319) reports that in recent years, ethnic and national groups other than known Italian Americans have developed organizations to pursue profits through illegal means. McCarthy (2011) equally observed this trend along their mode of operation when he posited that more organized groups are emerging, they are emerging from more countries, and the activities of all organizations are diversifying across national borders. It has also been predicted that sources of cybercrime will become increasingly organized and profit driven in the years ahead (GTISC, 2009). This projected or anticipated evolution of cyber fraud into a more complex networked typology of crime spanning several geographical boundaries in its effects constitutes one of the preoccupation of this discourse. Drawing from the organized-complexity bracketing, the INTERPOL conceives of organized crime as —any enterprise or group of persons engaged in a continuing illegal activity which has, as its primary purpose, the generation of profits regardless of national boundaries. It includes surfing the Internet for the purpose of generating illicit money and also embraces activities spanning a sizeable number of geographical boundaries.

Equally paraphrasing the conception of the U.N.O. about the organized trend in crime, one may view it as a confederation of criminal individuals or groups that come together because of economic needs, and whose operation is backed by the hierarchical coordination of a number of persons in planning and execution of illegal acts, or in the pursuit of legitimate objectives by illegal means. It also includes such sophisticated activities as money laundering through legitimate business and computer manipulation (requiring electronic communication) and it further encompasses the infiltration of many kinds of profitable, legal endeavours driven by predatory tactics, such as intimidation, violence, and corruption.

These tactics may be sophisticated and subtle or crude, overt, and direct. Flowing from this insight, there is gradual acknowledgement of the emergence of a new form of organized crime that takes advantage of electronic communications (Schaefer, 2005, p. 189). The medium of electronic communications (basically the Internet) offers the needed opportunity for both modern criminals and youths in their quest for economic advancement. Exploring the emerging versions of crime that are lately assuming the structure of organized crime therefore, the most complimentary definition to that given by the FBI on organized crime

which best captures the affinity between the traditional and newly evolving crime in the organized category is that remotely given by Michael Maltz, (1976, p.346). He defines organized crime as —a crime in which there is more than one offender, and the offenders are and intend to remain associated with one another for the purpose of committing crimes. This was further made explicit by Schaefer (2005,p. 188) when he views organized crime as the work of a group that regulates relations between various criminal enterprises involved in illegal activities, including prostitution, gambling, smuggling, sales of drugs and lately Internet fraud. Further corroboration by Valdez (1997) reveals that the electronic media, most especially the Internet, is a domain of cyber and credit card fraud with significant organized attributes. Without any doubt, cyber-crime is one of the growing scourges of global organized crime and representing one of crime diversifications. Its form is loosely registered when compared to the well-known types of traditional organized crimes. This position will become clearer as further explanation will show more on the attributes of cyber fraud which qualify it as a form of organized crime.

Primarily, cyber fraud constitutes an attempt to obtain money by scamming or tricking fraud victims. In its secondary nature, the cyber arena occasions money laundering and the establishment of dummy business networks to cover the sources of illicit capitals. Additionally, cyber fraud operation requires different types of expertise to get to maturation and within its compelling attributes are often performed by different segments in the chain of crime. There are significant attributes demarcating modern cyber fraud from most traditionally known crimes. McConnell International (2000) identified four of such important attributes which make modern cyber fraud differs from the hitherto known traditional crimes. These include, first, simplicity involved in learning the tact and operation of crime and invariably the easy access to engage in the practice of cyber crime and second, the relatively low resources required to engage in cyber crime. In most Third World countries like Nigeria for instance, the investment outlay only requires the purchase of air time from various cyber cafes to enable crime perpetration. Third, flexibility in the manipulation of the jurisdiction of crime. Spatially, Internet technology affords fraud perpetrators to reside in a geographical boundary and project crime toward a different socio-economic boundary. Finally, most cyber crime portend some insulation from prosecution. Legal arrangement of modern nations preclude cyber crime from existing legislations (especially in Nigeria). This often makes cyber fraudsters to remain unperturbed about the threat, possibility and consequences of arrest. In further establishing the basis of the organized nature of cyber fraud in this discourse, most emphasis will be geared towards its determinants as well as its entrenchment in Nigeria.

Review on the Organized Nature and Operationality of Cyber Fraud

Criminal behaviour in the new millennium involves more sophisticated and remote ways to steal (Albanese, 2007). A plus to this trend is added by modern cyber technology which often facilitates illicit practices in an unprecedented manner. Notably, one outstanding practice in this area that is attracting attention in the global community involves cyber fraud with its attendant organized nature. Organized crime differs in all respect from other crimes through its structuration. This involves its durability and complexity of syndicates implicated in crime, which have some of the traits of formal organizations, a division of labour, a hierarchy of authority structure, and coordination among various statuses (Conklin, 2007:315). In explaining cyber fraud organized attributes therefore, the role of power cannot be ruled out.

Research has shown that power helps in the recruitment of others into fraud. When a fraud takes place, the conspirator has the desire to carry out his or her own will, influence another person to act and do as the perpetrator wishes, regardless of resistance (Albrecht et al, 2012, p.53). Besides, the perpetration of fraud also assumes the form that fitted exactly into the five variables that French and Raven (1959) found in the course of their research on the role of power in fraud profession. One, Internet fraud presents its victim with reward power. Through the dissemination of scam letters, fraudster convince a potential victim of benefits that await him or her peradventure he or she complies with fraud tricks presented via the net. Two, coercive power regularly comes into play when the fraudster paints the gory situation that will ensue if the initial solicitation, warnings and expectations to gain the avowed benefits are ignored. It involves the infusion of avowed helplessness in part or fear into the victim and in most cases the subject of fraud affects what is crucial to the survival of the victim (for example bank account, investment base etc.). Third, expert power also comes into play. This manifests in the potential of the fraudster to manipulate his or the victims web page or simulate other genuine web pages of organizations or banks where the interest of the victim lies. Perpetrators present fake websites, disguise their identity and lure their victims into believing their bait.(Albrecht et al, 2012:53).

Fourth involves the use of legitimate power. In this, the fraudster assumes a legitimate posture by giving pieces of information that are closer to the private data held by the victim thereby making the demands exactly real and quite appealing. The fraudster presents before the victim a legitimate organization having something to do with the private life of the victim. The final element of power often adopted by the fraudsters is that called referent power. The perpetrator of fraud uses available intelligence within his capacity to gain the confidence and participation of the victim. This may take the use of other genuine leads to get the victim fixated and willing to play along. Establishing the global impact of cyber fraud, Iannacci and Morris (2000) lamented the scourge of credit card and cyber-related frauds.

It was argued that cyber fraud crime is a major threat to the modern global economy because of its attraction to criminal elements ranging from those committing simple fraud crimes to major organized crime activity. Quite unfortunate, most organized criminal groups that were once national in scope, can now employ global networks to further their illicit dealings. Information technology has enabled criminal groups to interact with other criminals on a global scale to traffic illegal goods more effectively and anonymously and to identify potential victims at a click of a button (Williams 2006, p.17). Criminal groups have no border concerns, in their minds. They seek opportunity and prey on whatever is most accessible. The group traverses state to state and country to country unmolested in their course of operations. They do this in an often futile attempt to evade detection and/or prosecution.

Further review on the organized potential of cyber fraud drawing from the context of Nigeria, few scholarly works confirmed that the existence of organized crime in the country is no longer news. Lame (2002) for example, lamented the business like nature of crime in Nigeria. He posits that like most business ventures, crime generally is now opened in groups, solely with the objectives of making profit. He further reiterates that the major weapon of organized economic crime in Nigeria consists of the ability to evade existing national laws without the use of violence to achieve one's objectives, that is, financial or material benefits. On the basis of the pervasiveness of crimes in most developed and developing nations and the evolution of few of such crimes into organized category, Abadinsky (2010) attempts a differentiation between conventional crimes and those within the category of organized crime. He argues that perpetuity is a crucial variable that distinguishes both crimes. In terms of organization, the structure of organized crime permits criminals in this category to commit a large scale variety of crimes spanning a large geographical space. Such crime engenders affiliation that is non-existent in other crimes. Ojomo (2002) also made an allusion to this latter fact as she claims that the escalation of cyber fraud in Nigeria underscores the development of the execution of fraud schemes at the syndicate-organized level, often with representative cells in targeted countries.

Apart from its spread, organized crime also creates a forum for entering into an agreement, negotiating a contract and sub-contracting a specified number of tasks needed to accomplish a crime.

The avenue for affiliation in essence offers opportunity for credentialing. Criminals often make expertise available in a cyber-market environment (across diverse countries) which simultaneously instantiate negotiations for the purpose of affordability and utmost trust thus representing a form of bonding ritual which serves as the basis for parting with crime choice resources. Simply put in the words of Abadinsky (2010, p.7), —the degree of sophistication characterizing a criminal organization can be measured by the degree to which it provides contract and arbitration services to criminals and sometimes legitimate entrepreneurs looking for a swifter, more reliable form of justice. Crime expertise is ultimately both tangible and intangible economic goods capable of application in legal and illegal terms. Technical knowledge is mostly handy in the international arena and in all known fraud environment. It is within the context of availability of skills that cyber fraud jobbers draw lifeline in the process of operating either as individuals or in their various syndicates globally.

From another angle, few research works attempt the explications of unique determining factors affiliating cyber fraud with related organized crime. According to Siegel (2008:85) the major indicator of the organized nature of any criminal group in any crime environment lies in its mode of operation. It is purely male gendered in which women are marginal actors or incidental victims (Turner and Kelly (2013, p.693). He lists the following attributes as necessary for any crime organization to be called organized: —its ability to keep its activities hidden, absence of written contracts or agreements in order to prevent the production of evidence of illicit transactions and it is an ability to own internal system for solving conflicts. Some form of affinity can be drawn between the structure of modern cyber-related crimes and

what obtains in conventional organized crime outfits as cyber fraud perfectly aligns with most identified attributes. Considering the first criterion, for fraud activities to operate securely in the e-business environment, fraudsters are apt at making their activities hidden from both immediate acquaintances and the law enforcement agencies. The second exemplifies that the virtual nature of cyber fraud creates anonymity and most interactions are done via the cyber space devoided of the establishment or discernment of the locations of the interacting individuals. Evidence is often deceptive and prosecution quite costly if not impossible. Thirdly on internal system of conflict resolution, it is clearly evident that the level of trust in cyber fraud business is quite rare to obtain in other forms of business. Once a deal is struck, parties to such agreement fulfill each other's part without any form of policing and the betrayal of trust rarely happens despite the parties into the deal having their locations thousands of miles apart. Comradeship and assumption of utmost trust form the driving principle upon which fraud experts enter into negotiations and simultaneously, efforts are made to sustain the secrecy of the 'business' concerned.

Another scholar further discussed the affinity between cyber fraud and traditional organized crimes as a factor of entrenched globalization. Cyber fraud is subsumed under the general environment of globalization (Galeotti, 2004), and ultimately as part of the globalization process (Fijnaut and Paoli, 2004). The latter term denotes the boundariless nature of socio-economic interactions affecting nations of the world. Galeotti (2004) intensifies our understanding on the connectivity between globalization and modern organized crime. He locates this connection in five drivers: technological; political; economic; enforcement and internal. Technological drivers heralded the spread of globalization on a larger scale; political drivers exhibit the national will to book a slot in the global arena; economic drivers promotes trade interactions; enforcement drivers function to moderate local and international relationships and while finally, internal drivers determine the structure to diverse approaches to global opportunities. All these drivers are germane to the sustenance of globalization.

A departure from the positive angles to these drivers lies in the existence of cyber fraud. With regard to the roles of these drivers in the cyber fraud operations, five major drivers listed by Galeotti (2004) seem perfectly aligned with the objectives of this discourse. The technological domain represents the locus of cyber fraud trade (in this the Internet technology becomes a suitable medium) while the economic drivers pre-supposes the inherent contradictions pulling so many youths in Nigeria into fraud activism. The latter involves acute unemployment, value displacement, absence of industrial base, dirt of infrastructure, corruption, religious fanatic and host of other anti-developmental stimulus. Borrowing from existing knowledge, earlier research has clearly shown that more and more people will commit fraud when a nation economy goes bad (Singleton and Singleton, 2010). The current trend in technological driven fraud in our world has a correlation with the state of nations economy and in the same vein, the incidence of fraud can be adjudged to be overtly propelled by the experiential situations of considerable people globally.

Youth crimes in most Third World Nation are directly linked with deteriorating economies. Basically, it is survival instincts that promote youths-crime correlation. Further expatiating on the political driver, it is manifestly clear that the participation of significant Nigeria's leaders in the global arena solidly rests on the utilization of the international platform for the intensification of corrupt related practices. This is evident in the volume of money laundering taking place in the e-domain involving Nigeria's political officials and their practices of utilizing the opportunities e-space offers to move fraud or looted treasury resources to their choice international financial institutions. This singular act of the political leadership promotes the level of corruption in the country and invariably represented the magnetic point attracting Nigeria's youths interest in their involvement in myriad of illicit activities. Finally, the enforcement drivers are both inhibitive and supportive of cyber fraud in the Nigerian context. Considering Nigeria's situation, the essence of enforcement is constant but in its desired effect, it lacks its potency.

Cyber anti-fraud law is conspicuously absent and law enforcers in their various levels lack the capacities to arrest its tide. The internal driver only supports a loose structure of collaborations among youths in cyber fraud trade.

Similarly, quite a number of scholars explore the role of technology operatable in the modern global environment as the major factor making cyber fraud assume its recent organized posture. The distinguishing feature of this novel catapult is implicated in the late modernity (Giddens, 1990: Bauman, 1998; Beck, 2000) with its manifest closely linked with revolution in communication technologies (Eriksen, 2003). There is a gamut of revolutions inherently submerged under the broad base of

communication revolution. One of such revolutions is that which thus affects the world of computers and its affiliates. Within the realm of computer revolution itself, the mostly used of the affiliates is the Internet, a technology which operates virtually in the global economic environment. This technology offers the youths the opportunity to reach out to distant lands, know different people and enables the utilization of new methods of doing and gaining things which may both be legal or illegal. Consequently, cyber fraud offenders are diverse and so also are the victims of fraud. The operation of this crime shares many things in common with most hitherto known organized forms of crime.

Causal Environment and Cyber Fraud Involvement among Youths in Nigeria

Many scholars have pointed out that there is a strong symbiotic relationship between organized crime and the legitimate environment in which it flourishes (Siegel and Nelen, 2008, p.2). Creating a link between environment and organized crime, Benson (2008, p.14) argues that the modern organized crime emerged primarily in the early twentieth century. Its precursors in the earliest period include poverty and joblessness with its catastrophic effect culminating in hopelessness in most societies where organized crime flourished. Sociologically, organized crime can be interpreted most readily in terms of anomic theory (Brown et al, 2013, p.473). It is an alternative mode of advancement to the segment of any society who found legitimate routes blocked by the inflexibility of the normative society. Organized criminals come from the lower echelon of the society and are handicapped by poor education or other barriers to social mobility. Other preconditions identified with the growth of organized crime include the existence of official corruption and the possibility of infiltrating the law enforcement unit that will enable bribery and covering of criminal activities. It is a well-known fact that blackmail, bribery and corruption are essential strategic tools of organized crime (Hagan, 2013, p.380). There is no significant difference with what occasioned the advent of organized crime and the climate which birthed and nurtured cyber fraud today both in Nigeria and in other part of the world.

Scholars in the ideological school of crime-society affinity have also blame a unique character of society akin to that of Nigeria as that capable of enhancing the status of conventional and enabling emerging crimes to possess organized structure. This is in line with what was earlier identified by Benson, (2008) as factors promoting the origin and sustenance of the organized potentials of most crimes in different societies. Gelles and Levine (1999) equally argue that this crime exists primarily to provide, and profit from illegal activities and it often manifests in societies where blocked legitimate career is predominant. In this case, legitimate means needed to secure livelihood is very scarce in Nigeria and the majority of Nigerian live below a dollar per day consistently. Consequently, organized crime dominates the world of illegal `business just as large corporations dominate the conventional business world. It serves as a means of upward mobility for Nigeria's youths struggling to escape poverty and it is characteristically global in nature (Schaefer, 2005; Gelles and Levine, 1999).

Crimes in this category are in part, a product of social arrangements that create a high risk, but high profit medium for fraud and other related deviance. Nigerian environment in this context entrenches social arrangement that limit opportunities for some groups, mostly youths that are stifled of breathing space to engage in legitimate business or career. In this regard, the historical origin of fraud groups in Nigeria is consistent with the attributive factors inherent in the community. The possibilities and dimensions organized crime assume in many environments can be blamed on the roles of governmental, social, economic and cultural contradictions existent in these kinds of society. These factors determine to a large extent the formation, intensification and sustenance of crime prone groups in Nigeria. Research also supported this view when it traces the root of organized crime to some inherent factors in Africa (Abadinsky 2010, p.202). There are several variables that make the development of criminality more attractive in Africa and these variables include wide inequality in wealth, unchecked population growth, high rate of poverty, governmental inefficiency and corruption and finally, rapid and uncontrolled urbanization. Organized crime thus becomes an option for individuals seeking to break out of poverty and thereby spontaneously banding together in form of gangs in order to achieve their life goals.

When examined from the precarious situation Nigerian are forced to contend with, one may observe that youths prone fraud activity exists in a web of interactions akin to a gang structure. Gang-like groupings of youth in the Internet environment assume a variety. Borrowing from Covey (2003), Nigeria's organized crime group come under both compressed and specialty gang categories. In its compressed form, cyber fraudsters are widely dispersed in terms of age and the fraud environment presents and nurtures both old

and young cyber fraudsters. There is no remarkable difference in the structure, cohesion, organization, methods of operation, membership/group permanence and control that is mostly dominant among the internationally acclaimed organized crime groups in the world of drug and money laundering and the organized fraud bonding that is common among the youths. In some cases, this group is commonly referred to as youth gangs. However, their attributes are not in any way different from those of other forms of organized crime groups but only in their recognition as one to be classified as such. It is clearly evident that the economic environment of Nigeria promotes the experimentation with diverse illicit activities directed at allaying the fear of survival challenges and which remains pronounced among considerable Nigerian youths and causing them to band themselves in deviance to normative standards.

There are diverse fronts where survival driven crimes can be observed in the country and one of such areas relates to youths involvement in all shades of crime including modern technology conditioned fraud. The successes often recorded in fraud activism are traceable to the regime of bribery that has been perfectly institutionalized and thus forming a subculture. In most cases, cyber café owners work hand in hand with the law enforcement officials to forestall the disruption of fraud activism and in the event of arrest, big guys are always on the standby to get the affected fraudster off the hook from the various police cells. There exists a perfect connivance with both law and criminals. This was rightly observed by Benson (2008, p.16) as he reported the role of law in the intensification of organized crime. He lamented that “The officials whose job it was to investigate and arrest the criminals were always —on the payroll, employees of those very criminals.”

There is also consistency in the operation of fraud because of its mutational capabilities. For instance if one part of a fraud organization is apprehended and its members put in jail it is simply replaced with a new part, and the fraud organization continues to function without interruption. In the organogram of cyber fraud business, there is the easy to capture and convict boys’ known as the small fry’ in organized crime parlance. Slightly above the fry are the major figures known as the Kingpin’ or the hubs connecting the diverse activities of different loose groupings of fraudsters.

This set of persons does not only facilitate business direction and determine the operation of the network but also helps in securing bails for the boys in case of arrest or prosecution. They are often insulated from arrest and prosecution and this is made possible by tight control over information concerning the set-up of the network. The flexibility of fraud gang replacement is a function of the availability of jobless youths on the one hand and the flexibility involved in cyber fraud participation on the other when considered from Nigeria’s context.

Just as other forms of organized crime portend risk, vulnerability and insecurity to social groups across diverse societies so also is cyber fraud in the e-environment. The effects of fraud are often felt by all and sundries cross culturally. The victims of cyber fraud are often referred to as maga’ or mugu’ symbolizing a fool. The web of victimization involved in cyber fraud business remained large. This is nurtured by the increase in the global participation of nations in e-commerce or socio-economic interaction globally. Potential victims abound in the cyber space and unabated cyclical operation pervades the e-environment. With a success recorded in defrauding a victim, another round of illicit venture is often put in place by the fraudsters. In cyber fraud, criminals are constantly on the look-out for new victims and in most cases consider this form of activity as profession in known poor countries. There are diverse areas of specialty in cyber fraud trade and this is often complemented by accurate and timely delivery of services (writing programmes, production of softwares, loading cards, routing proceeds, picking up of fraud proceeds, covering the tracts, etc.).

These practices have assumed an alarming magnitude across diverse geographical boundaries. Gunter Ollmann, Chief Security Strategist for IBM Internet Security Systems subsumed this dimension of the modern fraud group thriving through the lapses inherent in Internet technology as an international conglomerate of professionally trained actors motivated by high profit (GTISC, 2009). He established the affinity between the typology of criminals in Internet fraud and other forms of criminals that are traditionally known in organized crime arena. He divided the cyber-crime industry into three tiers. These include low-level criminals who use kits to create the specific malware required for their targeted victims; skilled developers and collectives of technical experts creating new components to embed within their commercial malware creation kits and finally top-tier managed service providers that wrap new services

around malware kits to increase propagation and enable organized fraud on a global scale, feeding gains back into existing money laundering chains (GTISC, 2009). With growing ingenuity in computer manipulation recently noticeable among Nigeria's youths, there is the correspondence between Ollmann's categorization and the major practices prevalent in the country. Youths in Nigeria parade different types of expertise needed to facilitate cyber fraud and yet they often record successes in Internet fraud business on a regular basis. The transient nature involved in the operation of cyber fraud occasions a break in transmission once a particular task is accomplished which simply demarcates this form from the hitherto known organized crime structure. This is in consonance with what Glenny (2009) identified as the entrepreneurial nature of organized crime in the late modernity. There is a high sense of trust with little or no in-fighting among youth fraudsters in Nigeria as they conduct their businesses in a conducive atmosphere. Apart from the existence of gangs, the Nigerian cyber fraud type also shares transnational connections in its operation.

The symbolic representation of the cyber fraud group is consistent with the character of other groups in the organized environment of crime. Both thrive by illicit behaviour to earn a living. While most known organized crime syndicates offer both tangible or intangible items in exchange for money or other choice items, cyber fraud thrives on trickery and scamming their victims through the offer of deceptive advances. In the utilization of crime proceeds, there exists no remarkable difference in the diversion of resources to legitimate investments. Similarly, a considerable amount of proceeds are used to live a luxurious life, ward off arrest, secure freedom if arrest occurs and to buy the conscience of law agencies. Research also shows that the interconnectivity between legitimate and illegitimate economic activities determines if a crime assumes an organized dimension (Siegel and Nelen, 2008). Considering this in the light of cyber fraud activism, funds are generated through scamming and proceeds are transferred and retrieved through legitimate banks. Promotionally, a substantial portion of these funds are invested in legitimate businesses which serve as a cover against public scrutiny and insulate fraudsters from molestations from the legal arena. The role of bankers in facilitating the successful transfer and disbursement of fraud proceeds in cyber fraud trade gave credence to the organized nature of Internet fraud.

In Nigeria, despite the existence of provisions stipulating the identification of client, record keeping and the mandatory notification of the Central Bank of Nigeria on diverse specified amounts of deposits and withdrawals, experience has shown that bank officials have a way of smoothing out difficulties in the settlement of illegal transactions. In this wise, a ratio of fraud proceeds is parted with to smooth out such difficulties. The practices of the banks in giving a soft landing for illicit fund transfer perfectly help reinforcing the cyclical nature of crime operation required by most organized crimes. Cyber fraud benefits from the cooperation of all stakeholders in the crime environment and in a way increases its perpetuity in both global scale and in myriad of local arena.

Conclusion and Recommendation

Examining the various positions of scholars on the rating of cyber fraud as a newer version of organized crime, this discourse authenticates that the operations of cyber fraud participants in Nigeria share some forms of affinity with modern organized crime. This entails the existence of simple gangs operating mainly in a transient manner. Organized structure of fraud in Nigeria appears loosely and with semi-autonomous fraudsters operating on fraud need basis. The structure is consistent with what Hobbs and Dunningham (1998) earlier reported on cyber fraud structures. Both argued that organized crime increasingly involves individuals in loose knit networks, who treat their criminal career rather like they would a business career. Fraudsters create their markets and products through surfing the Internet and maintain complex relationship within the web through spatial interactions globally. It is therefore suggested that the adoption of measures mostly appropriate to censuring the operations of organized crimes seemed appropriate and specifically desirable.

Apart from prosecuting offenders and the attendant application of severe punishment on crime associated with organized crimes, spontaneous recovery and seizure of fraud proceeds will help reduce the trend in the newly evolving organized crimes. Forfeiture of fraud asset and money will undermine the fiscal structure of the fraud rings and may equally diminish the likelihood of survival of the group involved in fraud. Increment in efforts geared toward protecting potential victims of fraud will also help reduce the complexity and surge of fraud organization in this era of the new economy. Most complimentary to the aforementioned is the required concerted efforts of governments across diverse regions of the world to

engage mutual legal agreement treaty to address the challenge of organized crime at the international arena and the use of far reaching economic reforms locally to address the perennial problem of unemployment and poverty linkable to current period of late capitalism. Promotion of citizen centred economic policies will go a long way in eradicating the challenges of organized cyber fraud.

References

- Abadinsky, H. (2010) *Organized Crime*, Ninth edition. Belmont: Wadsworth Cengage Learning
- Albaneze, J. (2007) *Organized Crime in our Times*. Fifth edition. Newark, New Jersey: Matthew Bender & Company, Inc.
- Albaneze, J. S., (2011) Transnational Organized Crime. In Mangai Natarajan (Ed.) *International Crime and Justice*. Cambridge: Cambridge University Press.
- Albrecht, S. W., Albrecht, C. O., Albrecht, C. C. and Zimbelman, M. F. (2012) *Fraud Examination*. Fourth Edition. South-Western: Cengage Learning
- Bauman, Z. (1998). *Globalization: The human consequences*. New York: Colombia University Press.
- Beck, U. (2000). *What is globalization?* Cambridge: Polity Press.
- Benson, M. (2008) *Criminal Investigations: Organized Crime*. New York; Infobase Publishing.
- Bossard, A. (1990). *Transnational crime and criminal law*. Chicago: Office of International Criminal Justice.
- Brown, S. E., Esbensen, F., and Geis, G. (2013) *Criminology: Explaining Crime and Its Context*. 8th Edition. London: Elsevier Inc.
- Clough, J.. (2010) *Principles of Cybercrime*. Cambridge: Cambridge University Press.
- Conklin, J. E. (2007) *Criminology*. London: Pearson Education, Inc.
- Covey, H. C. (2003) *Street Gangs Throughout the World*. Springfield, IL: Charles C. Thomas
- FBI (2000) U.S. Department of Justice, Federal Bureau of Investigation, *Criminal Victimization in the United State*. Government Printing Office, 51.
- French, Jr., J. R. P. and Raven, B. (1959) The Basis of Social Power." In D. Cartwright, ed., *Studies in Social Power* Ann Arbor, MI: University of Michigan Press.
- Galeotti, M. (2004). Introduction. Global crime today. *Global Crime*, 6(1), 1-7.
- Gelles, R.J. and Levine, A. (1999) *Sociology: An Introduction* Sixth Edition, New York:

- McGraw-Hill Companies Inc., 251-252.
- Giddens, A. (1990) *The Consequences of Modernity*. Cambridge: Polity Press.
- Glenny, M., (2009) *McMafia: A Journey Through the Global Criminal Underworld*. New York: Vintage Press.
- Goldson, B. (2004), 'Youths Crime and Youths Justice'. In John Muncie and David Wilson (eds.) *Students Handbook on Criminal Justice and Criminology*, Great Britain: Cavendish Publishing Limited, 221-234.
- Hagan, F. E., (2013) *Introduction to Criminology: Theories, Methods and Criminal Behaviours*. Thousand Oaks, California: Sage Publication, Inc.
- Hobbs, D. and Dunningham, C. (1998), 'Glocal Organized Crime: Context and Pretext' In V. Ruggiero, N. South and I. Taylor (eds.), *The New European Criminology: Crime and Social Order in Europe*, London: Routledge.
- Home Office (2002) *Criminal Statistics*, England and Wales, London: Home Office.
- Iannacci, J. and Morris, R. (2000) *Access Device Fraud and Related Financial Crime*. Florida: CRC Press LLC
- Levi, M., (2012) Perspectives on Organized Crime. In Tim Newburn (Ed.) *Readings in Criminology*. Abingdon, Oxfordshire: Routledge.
- Maltz, M. D. (1976) "On Defining 'Organized Crime.'" *Crime and Delinquency* 22 (July): 338-46.
- McCarthy, D.M.P. (2011) *An Economic History of Organized Crime: A National and Transnational Approach*. Abingdon: Routledge
- Morris, S. (2004) The Future of Netcrime Now: Part 1 - threats and challenges, *Home Office Online Report* 62/04, p. 20.
- Newburn, T., (2012) (Ed.) *Key Readings in Criminology*. Abingdon, Oxfordshire: Routledge.
- Newton, M. (2011) *Chronology of Organized Crime Worldwide: 6000 B.C. to 2010*. North Carolina: McFarland & Company, Inc. Publishers.
- Ojomo, A. J. (2002) "Advanced Fee Fraud and Nigerian Image" In *Proceedings of the First National Seminar on Economic Crime*. Abuja: CBN. 96-115
- Passas, N. (2002). Cross-border crime and the interface between legal and illegal actors. In P. Van Duyne, K. von Lampe, & N. Passas (Eds.) *Upperworld and underworld in cross-border crime*. Nijmegen: Wolf Legal Publishers.
- Poole-Robb, S. and Bailey, A. (2002) *Risky Business: Corruption, Fraud, Terrorism and Other Threats to Global Business*. London: Kogan Page Ltd.
- Schaefer, T. R. (2005) *Sociology*. Ninth edition New York: McGraw-Hill Companies Inc. 337-338
- Scheff, T. (1966), *Being Mentally Ill*, Chicago: Aldine.
- Sieber, U. (1998) Legal Aspects of Computer-Related Crime in the Information Society, *COMCRIME Study*, European Commission. 19.
- Siegel, D. (2008) Diamonds and Organized Crime: The Case of Antwerp. In Dina Siegel and

Hans Nelen (Eds.) *Organized Crime: Culture, Markets and Policies*. New York: Springer Science + Business Media

Siegel, D and Nelen, H. (Eds.) (2008) *Organized Crime: Culture, Markets and Policies*. New York: Springer Science + Business Media

Singleton, T. W. and Singleton, A. J. (2010) *Fraud Auditing and Forensic Accounting*. Fourth Edition. New Jersey: John Wiley & Sons, Inc.

Turner, J., and Kelly, L., (2013) Trade Secret Intercessions Between Diasporas and Crime Groups in the Constitution of the Human Trafficking Chain. In Eugene McLaughlin & John Muncie (Eds.) *Criminological Perspectives*. London: Sage Publication Ltd.

Valdez, A. (1997), "In the Hood: Street Gangs Discover White-Collar Crime" *Police*, Vol. 21, No. 5, (May): 49-50, 56.

Van Duyne, P., (1996) The Phantom and Threat of Organized Crime. *Crime, Law and Social Change.*, Vol. 24, Pp. 341-377.

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

Williams, M. (2006) *Virtual Criminal: Crime, Deviance and Regulation Online*. Madison Ave., New York: Routledge.