Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace

DOI: 10.36108/NJSA/6102/14(0130)

Philip N. Ndubueze
Department of Sociology
Federal University Dutse
Jigawa State, Nigeria
Email: pnndubueze@gmail.com

Abstract
Digital and Computer Mediated Communication (CMC) technologies have altered traditional forms of social relationships across modern societies and have raised critical concerns about social order in the cyberspace. The amorphous and borderless nature of virtual communities have allowed various deviants, criminals and terrorists elements to permeate them. The resultant criminogenic atmosphere has created a new research agenda for the discipline of criminology. This paper examines the emergence of cyber criminology as a twenty-first century field of criminology and argues that its growth is a fall-out of concerns about the increasing rate of crime and disorder in the cyberspace. Cyber criminology seeks to offer explanation to the causation of deviance, crime and terrorism in the cyberspace. The paper which is anchored on Jaishankar's Space Transition Theory and Cohen and Felson's Routine Activity Theory highlights the challenges, prospects and future direction of the evolving field of cyber criminology and its relevance to the quest for order in the Nigerian cyberspace.

Keywords: cybercrime, cyber criminology, cyberspace, social order, space transition theory, routine activity theory

Introduction

The term "Cyber Criminology" was coined in 2007 by an Indian criminologist and founding father of the new field, Professor Karuppannan Jiashankar. Cyber criminology is a multi-disciplinary field that engages researchers from criminology, victimology, sociology, internet science and computer science (Jaishankar, 2007; Jaishankar, 2011). In the past two decades, the scope of criminological researches has broadened to include different forms of technology-enabled crime and the use of traditional theories in their explanation (Holt and Bossler, 2014).

The internet has expanded the idea of community as it is traditionally used in the social sciences (Vance, 2008). It has become a platform for the composition and re-composition of new internet-based identities (Parker, 2008). Electronic tribes which are similar to virtual teams from different geographical locations operate on the internet to accomplish different tasks (Olaniran, 2008). Thus the internet brings together like minds who interface on virtual communities and social network sites using various forms of Computer Mediated Communication (CMC) to pursue common goals. Likewise, various forms of deviance, crime and terrorism are perpetrated in the internet.

"Murderers, sexual predators, blackmailers, thieves, spies and many other criminals have used the Internet to facilitate their crimes" (Casey, 2002: 549). The resultant criminogenic atmosphere has created a new research agenda for the discipline of criminology. This paper examines the emergence of cyber criminology as a twenty-first century field of criminology and argues that its growth is a fall-out of concerns about the growing rate of crime and disorder in the cyberspace. The field of cyber criminology seeks to offer explanation to the causation of deviance, crime and terrorism in the cyberspace with a view to promoting social order. The paper therefore highlights the challenges, prospects and future direction of cyber criminology as an emerging academic field and its relevance to the quest for order in Nigeria's cyberspace.

Conceptual Review

Cyber Criminology

According to Jaishankar (2011, p. xxvii) cyber criminology is "the study of causation of crimes that occur in the cyberspace and its impact in the physical space". He posits that the body of knowledge on cybercrimes should be distinguished from cyber forensics and that there is need for a separate discipline to explore cybercrime from a social science standpoint **(J**aishnakar, 2011). Cyber criminology is the scientific study of deviance, crime and terrorism in the cyberspace and the concerns that they provoke among a wide spectrum of stakeholders such as internet-active users, families, Faith Based Organizations (FBOs), operators, security companies, Internet Service Providers (ISPs), regulators, the criminal justice system, the government and Non-Governmental Organizations. Cyber criminology is a twenty-first century field of criminology that emerged in response to the development of the cyberspace and the super-criminogenic atmosphere it created.

Cyberspace

The term "cyberspace" which was coined by Williams Gibson in 1982 (Wall, 2008), connotes the network of computers linked by the internet (Ince, 2003; Mitra, 2010), and transcends physical boundaries as well as geography (Jaishankar, 2010; Wall and Williams, 2007). Gibson (1984: 51) conceives cyberspace as:

> A consensual hallucination experienced daily by billons of legitimate operators, in every nation… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellation of data like city lights receding.

A decade after Gibson's definition of cyberspace, Rheingold (1994: 5) offers a more vivid definition of the concept as: "the conceptual space where words, human relationships, data, wealth and power are manifested by people using CMC [computer-mediated communications] technology". The cyberspace

creates certain difficulties for law enforcement and prosecution agencies (Smith, 2014). This is because "systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses" (Clarke and Knake, 2010: 31). This is further compounded by the fact that a person may enjoy some level of privacy in cyberspace and can change his or her age, gender, race, and or socio-economic status and assume an entirely different persona to others online (Biegel, 2001). Communities do not exist exclusively in the cyberspace as social groups in the cyberspace spill over into the physical space and vice versa (Kollock and Smith, 2005). It therefore implies that the activities initiated online can have far reaching consequences on the physical world.

Social Order

According to Wall (2004), order refers to the establishment of a reasonable control over the environment within which a system operates to enable its individual entities effectively carry out the tasks necessary for the survival of the system. Horton and Hunt (as cited in Rao, 2012: 642) define social order as "a system of people, relationship, and customs operating smoothly to accomplish the work of a society". These definitions presuppose the likelihood of obstruction and disorder in a system that is devoid of some measure of control. It is argued that "the idea is not only that people ascribe meaning to disorder they see in front of them (i.e. disorder signals a lack of concern for public order and low levels of informal social control), but that ambiguous cues also need to be defined by the observer as 'disorderly' while other individuals in the same environment might not" (Farrall, Jackson and Gray, 2009: 99). Disorder refers to any aspect of the social and physical environment that depicts a lack of control and concern as well as the values and intents of others that occupy the space (Farrall, Jackson and Gray, 2009: 99). An unregulated space may be characterized by disorder and various forms of antisocial behaviour. Arguably, the search for social order influenced sociological thought and theorizing in the nineteenth and twentieth century. Early sociologists were concerned about the disorder that resulted as a push back from the political revolutions, the industrial revolutions/the rise of capitalism, the rise of socialism, feminism, urbanization and religious change (Ritzer, 2008). These forces triggered unprecedented social change and early sociologists were therefore interested in understanding the course, causes and consequences of these changes.

Statement of the Problem

Digital and Computer Mediated Communication (CMC) technologies have altered traditional forms of social relationships across modern societies and have raised critical concerns about social order in the cyberspace. The amorphous and borderless nature of virtual communities have allowed various deviants, criminals and terrorists elements to permeate them. The resultant

criminogenic atmosphere has created a new research agenda for the discipline of criminology.

There is a rise in the spate of deviant, criminal and terrorist activities on the internet (Ndubueze, 2016; Nhan and Bachmann, 2015). However, the emerging discipline of cyber criminology that is concerned about the context, causes, course and consequences of deviance, crime and terrorism in the cyberspace has not received adequate attention from mainstream criminology. There are three major reasons why the new sub-discipline of cyber criminology deserves more academic attention than it is presently receiving. First, the internet revolution is raging across societies of the world and is characterized by mass transition of systems, processes and people from the analogue platform to the digital platform. This transition has some unintended and far-reaching consequences for individuals, organizations and societies at large, of which crime is one. Second, unlike traditional crimes, cybercrimes are technology-enabled and as such difficult to prevent, monitor or prosecute. Third, there is dearth of empirical researches in cyber criminology especially in Nigeria.

The foregoing underscores the dire need for a specialized attention to this emerging sub-field by a team of dedicated researchers within general criminology to interrogate and bring to fore these evolving issues with a view to contributing to the quest for social order. Thus, if not systematically delineated, the fundamental concerns of cyber criminology may be drowned within the discourse of mainstream criminology.

Method

This research employed content analysis. Hence, information was elicited from relevant and related literature (books, journals, and online materials) on cyber criminology and other key concepts. Major consideration was given to literature that reflected the nature and extent of debates and scholarship on cyber criminology which is a new sub-discipline of criminological studies. This exercise highlighted the scope and depth of scholarship in the area and both theoretical and empirical literature were reviewed.

Theoretical Orientation

The paper is situated within the framework of Jaishankar's (2008) Space Transition Theory (STT) and Cohen and Felson (1979) Routine Activity Theory (RAT). Both theories underpins the current discourse.

Space Transition Theory

The Space Transition Theory which is probably the only cybercrime specific theory to date is considered appropriate for the discourse because of its unique insights into the nexus between space transition and online criminality. The theory is premised on the assumption that people bring their conforming or nonconforming behavior in the physical space into the cyberspace. The STT however focuses on explaining cybercrime only. The perspective argues that space transition entails the movement of people from the physical space to

cyberspace and from the cyberspace to physical space. This movement is characterized by a change in behavior which obviously have certain security implications. The theory is anchored on seven assumptions as follows:

1. Those who have suppressed criminal inclinations in the physical space are more likely to commit crime in the cyberspace, which ordinarily they would be reluctant to commit because of their status or position.
2. Certain attributes of the cyberspace such as identity flexibility, dissociative anonymity and lax deterrence facilitates the commission of cybercrime.
3. Offenders may import their criminal behavior in cyberspace to the physical space and may export same to the cyberspace.
4. The unsteady appearance of offenders in the cyberspace coupled with changing spatiotemporal attribute of the cyberspace makes escape pretty easy.
5. (a) Strangers may congregate in the cyberspace to execute crime in the physical space.
   (b) Friends in the physical space may come together in the physical space to commit crime in the cyberspace.
6. People who live in closed society are more likely to commit crime than those who live in open society.
7. The inconsistency between norms and values of the physical space with those of the cyberspace may facilitate cybercrimes.

The physical space is characterized by crime and disorderly conducts. People have always sought to and sometimes ultimately succeeded in circumventing social norms and values way before the advent of cyber technology. The internet age while creating novel kinds of crime and criminality in Nigeria**,** also saw the introduction of traditional crimes such as advance fee fraud into the cyberspace. The new found space (cyberspace) provides a 'safe haven' for those with bottled-up criminal tendencies to launch their crime, remain anonymous or hide their true identity, cover their tracks and avoid detection. This scenario is troubling as it makes the cyberspace a free for all world, where conformists, deviants, criminals and terrorists congregate. This problem is compounded by the fact that social norms and values for the most part seem to be relaxed in the cyberspace. This is evident in e-mails, social media and chatroom communications and conversations. People disrespect constituted political and religious authorities, use vulgar language, share indecent pictures and regress to the state of nature (as it were) without any feeling of guilt. This will hardly be the case in the physical space. Granted that there is a serious breakdown of moral values across all the basic institutions of society, a society should not lose its sense of decency and respect for traditional values. Nonetheless, today, there are good examples of Nigerians who feel a strong need for order even in the physical space. Unfortunately, though, the internet, computer mediated communications and digital technologies are systematically diminishing our value system. Thus, the space transition theory provides an

appropriate framework within which to situate the problem of disorder in Nigerian cyberspace.

In a nutshell, the Space Transition Theory (STT) offers a simple explanation to the complex problem of crime and disorder in the cyberspace. It provides a plausible insight into the nature of transition between the spaces (physical and virtual) and its implications for order in society. Nonetheless, Danquah and Longe (2011), in a study with primary data from Ghana and secondary data from other parts of the world scrutinized the Space Transition Theory and found that its postulates do not completely apply to all categories of cybercrime. Also, the space transition theory, unlike other theories that have been used to explain cybercrime such as the Routine Activity Theory of Cohen and Felson (1979) is focused only on crimes committed online. For a deeper understanding of the current discourse, there is need to complement the Space Transition Theory with a broader theory of crime.

Routine Activity Theory (RAT)

The Routine Activity Theory, a variant of environmental criminology was developed by Cohen and Felson (1979) to explain the dynamics of crime victimization. The theory posits that crime is a consequence of the convergence of three elements: (i) Likely offenders (persons who want to commit crime). (ii) Suitable targets (valued items that can be moved easily). (iii) The absence of capable guardians (persons who have the ability to prevent the crime).

It has been argued that RAT is premised on two ideas. First, for crime to occur, motivated offenders must meet with suitable targets in the absence of capable guardians. Second, the likelihood of this scenario happening is dependent upon people's routine activities such as their family, work, relaxation and consumption patterns (Cullen, Agnew and Wilcox, 2014). Thus, the RAT adequately complements the STT. It has been used by several scholars to explain cybercrimes (Pratt, Holtfreter and Reisig, 2010; Yar, 2005). However, Vito and Holmes (1994) have criticized the theory for not explaining the risk of victimization of females, low-income individuals, single people and the young.

Nigerian cyberspace is besieged by law-abiding persons as well as deviant and criminal elements. In spite of the spirited efforts of law enforcement agencies in Nigeria especially the Economic and Financial Crimes Commission (EFCC) to track and prosecute cyber criminals, many online criminals are still undeterred. This by implication means that there will always be motivated offenders lurking around for suitable targets online and because cybercrime is a complex kind of crime and many internet users in Nigeria are perhaps "internet-naïve" (and constitute the weakest link in the internet security chain), capable guardianship cannot be guaranteed. Therefore, as more people get connected to the internet in Nigeria, so do more people get trapped into the potential cyber victimization net. One way to alter this equation is for individual internet users to reduce their suitability for victimization. This they can do by taking all necessary security precautions during their routine online activities. For example, by using alpha-numeric passwords and being very

mindful of whom they connect with online as well as the personal information they divulge online.

Crime and Disorder in the Cyberspace: An Overview

The cyberspace is characterized by crime and disorder. "For centuries, law enforcement officials have bemoaned the crime-enabling effects of new technologies – and have successfully used this as a rationale to further expand their policing reach" (Andreas, 2013: 55). The internet changed the geographic boundaries of crime and also gave rise to the new forms of criminal activities (Mitra, 2010). Deviance and crime are social phenomena that are rooted in the wider cultural, economic and political context of a given society (Sandywell, 2011). The use of the internet by deviants, criminals and terrorists seems to be on the rise and has elicited serious concerns among cyber criminologists who have attempted to understand their contexts, causes and consequences. Wall (2001) identifies a typology of cybercrime that includes: cyber-trespass, cyber-deception/theft, cyber-pornography/obscenity and cyber-violence.

Criminal, malicious and inappropriate activities online can be classified into three, namely: cyber deviance, cybercrime and cyber terrorism. Holt, Bossler and Seigfried-Speller (2015) explain that cyber deviance refers to the use of technology to carryout behaviours that may not necessarily be illegal but violates the formal and informal norms or beliefs of a dominant culture. However, when activities contravene codified legal statuses they become criminal acts. They consider the political or ideological use of digital technology or computer mediated communication for malicious purposes and for social change as cyberterrorism.

Youth assemble in the cyberspace just like they do on the street to seek illicit fun and illegal profit (Grabosky, 2004). Criminals use the internet to carry out activities that they have done in the past through phone, letters, or in person (Biegel, 2001). Smugglers and traffickers use the internet to organize their network and activities in an effective, efficient and less risky manner (Nicola, 2014). With the digitalization of critical personal information, identity theft is now prevalent (Mitra, 2010), and criminals can use personal information obtained from data leaked publicly or extracted from online databases or from users via social engineering to carry out different kinds of illicit activities (Smith, 2014). Criminal organizations around the world use the internet to communicate and network and do not necessarily have to meet physically (Nicaso and Lemothe, 2005). Cyber stalking can escalate to physical world and result in assault and homicide (Eastton and Taylor, 2011). The internet is also besieged by cyber offenders such as online stalkers and child pornography website operators (Maguire, 2015). The growing influx of terrorists to the cyberspace is well documented in the literature. The cyberspace and the internet is suitable for terrorism and the psyche of terrorists (Rogers, 2003). The internet has been used by terrorists to raise funds, recruit and train (Clarke and Knake, 2010). It has been argued that some governments (or their

proxies) use internet technologies to commit crime (Broadhurst, Grabosky, Alazab and Cohen, 2014).

The spate of crime and disorder in the cyberspace and their real world consequences raise serious concerns about social order in the cyberspace. In February, 2009, in the United Kingdom, Edward Richardson reportedly killed his wife because she changed her Facebook status from married to single (Eastton and Taylor, 2011). Similarly, in 2012, Cynthia Osokogu was reportedly killed by her Facebook friends in a hotel room in Lagos, Nigeria (Usman, 2012). In 2012, an estimated $1.9 million was reportedly generated through "Silk Road" – an online illicit drug trafficking gang (Christian as cited in Bryant, Day and Kennedy, 2014). Recently, a cyber-criminal gang known as "Carbanak" from Russia, Ukraine, other parts of Europe and China allegedly stole about $1b from 100 financial institutions across the world from 2013 to date (Kaspersky, 2015). In 2008, the Central Intelligence Agency reported cyber-attack incidents that disrupted power equipment in several regions outside the United States (SANS Organization as cited in Peshin, 2009). These incidents underscore the need for social order in a space that is increasingly becoming criminogenic and disorderly.

Cyber Criminology and the Search for Social Order

Every technological innovation in human history is tailored towards solving an existing societal problem. Paradoxically, while it solves the identified problem, it often leaves in its wake some unintended consequences for society. As was observed:

> Cyberspace presents myriad potential opportunities for society in the new millennium. In the 1990s, a new era was ushered in, in which Internet technology reigned supreme. However, the increase in the netizens has dwarfed the technology to a mere medium. Additionally, the perpetrators who attacked machines through machines have started attacking real humans through the machines. This radical development led criminologists to address the need for a discipline to study and analyze criminal behavior in the cyberspace (Jaishankar, 2010: 26).

The search for social order in the cyberspace is one of the primary concerns of the young discipline of cyber criminology. Early cyber criminologists such as Bachmann (2007), Brenner (2001), Holt (2003), Jaishankar (2007), Wall (2001), Yar (2005) among others were interested in understanding the contexts, causes, consequences and control of crimes and disorder in the cyberspace. Arguably, some of the crimes committed in the cyberspace are not entirely new, but are transported from the physical space. However, scholars are interested in understanding how such crimes are committed in the new space and the level of impact such crimes have in the physical space. Cyber criminologists are also interested in investigating how virtual communities

emerge, congregate, operate and transit as well as how they dramatically alter the traditional norms of face-to-face communications.

Social order is critical in the cyberspace as it is a prerequisite for the survival of the environment. Jones (2009) in his analysis of cybercrime and Internet security argues that a new social space is emerging and examines the nature of the criminal activity that occur in this space, its mechanisms and motivations and control measures. Lusthans (2013) notes that cybercriminal forums cannot be effectively governed because of the virtual nature of monitoring and enforcement. However, scholars have examined the prospects of establishing some level of control in the cyberspace.

Beigel (2001) contends that digital fences are some kind of new online borders that denote law, order and control. Smith (2014, p.125) identifies the capable guardians of the cyberspace as "computer users, local and international law enforcement agencies, financial and business regulators, government policy and regulatory agencies at local, national and international levels, informational technology industry organizations, including telecommunications carriers, Internet service providers, hardware and software manufacturers; small and large business associations and their members, and a range of public interest groups, including the media, computer user groups, and consumer protection agencies". Ndubueze and Igbo (2014) examined the role of third parties to crimes in policing cybercrime in Nigeria.

Challenges, Prospects and Future Direction of Cyber Criminology

The Challenges

The new field of cyber criminology is confronted with several challenges. Some of these challenges include:

a) *Definitional, Methodological and Theoretical Issues*

Cyber criminology is obviously confronted with the challenge of framing a generally acceptable definition of its concepts, arriving at uniformed methods and widely embraced theories. Nhan and Bachmann (2014: 223) ague that "despite the growth in both cybercrime and cybercrime research, cyber criminology faces challenges as a new paradigm of study in search of a clear definition, generally accepted methods, and theoretical models". Wall (2008: 52) had observed that different group of people attach different meanings to cybercrime, thus "contemporary debates about cybercrime encompasses a range of legal-political, technological, social and economic discourses that have led to some very different epistemological constructions of cybercrime". Hargreaves and Prince (2013) contend that defining cybercrime is a difficult task. Holt and Bossler (2014) opine that most cybercrime studies use aspects of traditional criminological theories such as routine activity theory, social learning and the general theory of crime. However, the first cybercrime-specific theory: the space transition theory was developed by Jaishankar (2008).

b) *Lack of Adequate Attention from Mainstream Criminology*
It has been argued that "cyber criminology is slow to emerge from a niche area that is often marginalized by mainstream criminology to occupy a position of high importance" (Nhan and Bachmann, 2015, p. 223). Cyber criminology is one of the latest sub-fields of criminology. Unfortunately, most criminology textbooks do not appreciate the place of this new field in twenty-first century criminology as they do not have dedicated chapters on cyber criminology. The few that discuss cybercrimes barely make explicit reference to the evolving sub-discipline of cyber criminology. Jaishankar (2007) was one of the early scholars who made serious efforts to promote the new field. He launched an open access journal dedicated to cyber criminology known as: "International Journal of Cyber Criminology" in 2007 and published a book entitled: "Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour" in 2011. These publications brought to fore the increasing state of crime and disorder in the cyberspace and the need for social order which is the primary concern of the new discipline of cyber criminology.

c) *Multi-disciplinary Nature of the Discipline*
Cyber criminology is multi-disciplinary in nature and draws researchers from criminology, victimology, sociology, internet science and computer science (Jaishankar, 2007). This makes the issue of common definition of concepts problematic. Internet science and computer science in their study of cybercrime often use technical terms that are not common in the social sciences. Unfortunately, where concepts are common, they are defined strictly from discipline-colored glasses that leave little room for appreciation by allied disciplines. Sometimes publications on cybercrime emanating from non-social science disciplines are rather loaded with jargons that may not make much sense to the average social scientist. Diamond and Bechmann (2015) recognize this problem and advocates that the next generation of social scientists incorporate technological aspects into cybercrime programs as a way out.

c) *Dearth of Dedicated Researchers and Research Centers*
According to the United Nations Office on Drug and Crime (2013, p. xvii) "In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's population, had access to the internet. Over 60 percent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years." However, there is dearth of dedicated cyber criminologists especially in developing countries of Africa. Most scholars who have researched extensively on cyber criminology such as David Wall, Karuppannan Jaishankar, Marjid Yar, Michael Bachmann, Peter N. Grabosky, Susan W. Brenner, Thomas Holt, Yvonne Jewkes, and the like are not from Africa. Again, most cybercrime research centres are located in the western world. This development is clearly inconsistent with our vision for a "crime-free" virtual operating environment in Nigeria.

e) *Dearth of Reliable and Standardized Data*
There is a dearth of reliable and standardized cybercrime data. Hargreaves and Prince (2013) observe that due to the lack of data collection and continued arguments over cybercrime definition, cybercrime data is currently fragmented. Wall (2008) contends that the primary source of statistical data on cybercrime come from cybercrime security industry and questions the reliability of such data given the interest that they promote. Tcherni, Davis, Lopes and Lizotte (2015) in their work on online property crime highlight the gap in reporting and accounting of online crimes. Wall (2005) notes that some serious online crimes against individuals are not reflected in the crime statistics. Diamond and Bachmann (2015) posit that the source of most cybercrime data are either agency or victimization surveys and that while they offer a base insight into law enforcement efforts to curb cybercrime, they fall short of deep insight on their prevalence**,** official response and offenders' attributes. Similarly, the United Nations Office on Drug and Crime (2013) maintains that police-recorded crime statistics are not useful for cross-national comparisons and that victimization survey provides a better basis for comparison.

Results

Cyber criminology is an emerging area in criminological studies that has created a new research agenda for criminologists. The analysis of the contents of the relevant materials reviewed indicates that the cyberspace is increasingly characterized by crime, deviance and terrorism. Cyber technology is not only embraced by law abiding persons but also by law violators and disorderly people. The internet thus is besieged by deviant, criminal and terrorists. Cyber criminology therefore evolved in response to these developments and the quest for social order in the cyberspace.

The extant literature reviewed reveals a gap in empirical studies in cyber criminology. There is also a gap in generally acceptable definition, methods and revenant theories. Dedicated researchers and research centers are western-heavy. More so, not so much have been done in promoting the sub-discipline in Africa, including Nigeria. Moreover, there is generally a dearth of dedicated textbooks on cyber criminology. Also most criminology textbooks do not have a dedicated chapter on cyber criminology. The foregoing seems to suggest a lack of attention from mainstream criminology. However, there are indications that cyber criminology will gain popularity in the near future as crime and disorder in the cyberspace continue to pose serious threat to social order across modern societies. The literature also indicates that some Nigerian scholars have shown interest in the concerns of cyber criminology.

The Prospects and Future Direction

There are clear indications that the emerging sub-discipline of cyber criminology will in the near future gain prominence in mainstream criminological discourses.

> …Society at large is becoming more aware of the severity and dangerousness of cybercrimes and related issues. The young discipline of cyber-criminology is already benefiting from this increasing awareness. More social scientists are beginning to examine cyber criminological topics and aspects, and it is safe to predict that greater numbers will follow in the years to come. Just as its subject of study, cyber criminology will become more mainstream within criminology. *(Diamond and Bachmann, 2015: 31)*

The above quote underscores the great prospects that lie ahead for the emerging discipline of cyber criminology. This is perhaps for three reasons. First, with the dramatic explosion in internet access across the globe and the growing dependence on computer mediated communication (CMC) technology and the Internet of Things (IOTs), the vulnerability widow of cybercrime will expand. Second, the above scenario will ultimately create moral panic about the rate of crime and disorder in the cyberspace and raise agitations for increased regulation. Third, these developments will stimulate more interest in cyber-related discourses and ultimately attract more attention to the discipline of cyber criminology.

Moreover, in the near future, national governments, regional bodies and international organizations such as the United Nations will show renewed interest in emerging cyber security threats. Many cybercrime and cyber security centers will emerge in the build-up of a global battle cry for order in the cyberspace. More dedicated cybercrime/cyber security fora and academic conferences will be convened. More universities across the world and particularly in developing countries will offer criminology programme with a cyber criminology component at undergraduate level. These milestones will give further impetus to the evolving discipline of cyber criminology. The next decade will no doubt be engaging for cyber criminologists.

Nigeria will not be completely left behind in the movement for the restoration of order in the cyberspace. It is worthy of note that some Nigerian scholars have contributed to emerging cyber criminological discourses over the years. They include Adeninran (2008), Longe and Chiemke (2008), Ndubueze (2012), Ndubueze, Igbo and Okoye (2013), Radda and Ndubueze (2013), Tade (2011), Ojedokun and Eraye (2012) among others.

Conclusion and Recommendations

Although cyber criminology is an evolving field of criminology which has not so far received adequate attention from mainstream criminology, the future holds great prospect for the new discipline. As virtual communities and electronic tribes proliferate the cyberspace and crime/disorder escalate, the discipline of cyber criminology will gain momentum and attention. It will remain active in the search for answers to the fundamental questions of the

contexts and causes of crime and disorder in the cyberspace as well as the quest for social order.

More cyber criminology - specific concepts, models and theories are required in the understanding of the problem of deviance, crime and terrorism in the cyberspace. They must be social science oriented and must take into consideration the growing complexity of virtual communities and online social networks. Above all, more dedicated cyber criminologists are needed to sufficiently explore the traditional concerns and emerging themes of the new field of cyber criminology. The Nigerian government should increase its funding on cyber security researches. There is need for the federal government to set up a re-invigorated National Cyber Security Working Group that will comprise of experts from the academia, law enforcement agencies, research institutes and Internet Service Providers. Nigerian universities should seriously consider the establishment of cybercrime research institutes. This is perhaps one way that order can be guaranteed in a rather increasingly disorderly space.

References

Adeniran, A.I. (2008) The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology,* 2(2): 368–381.

Andreas, P. (2015) Illicit globalization: Myths and misconceptions. In V. Mitsilegas, P. Alldridge and L. Chelitotis (eds.), *Globalization, criminal law and criminal justice: Theoretical, comparative and transnational perspectives,* Oxford: Oxford and Portland Oregon. pp. 45-64.

Bachmann, M. (2007) Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA. *International Journal of Cyber Criminology*, 2(1): 213-227.

Brenner, S.W. (2001) Is there such a thing as "Virtual Crime"? 4 Cal. Crim. L. Rev. 3. Retrieved August 24, 2016: http://scholarship.law.berkeley.edu/bjcl/vol4-/iss1/3.

Brenner, S.W. (2004) Towards a criminal law for cyberspace: A new model of law enforcement? *Rutgers Computer and Technology Law Journal*, 30: 1–104.

Biegel, S. (2001) *Beyond our control.* Cambridge: The MIT Press.

Broadhurst, R., Grabosky, P., Alazab, M. and Cohen, S. (2014) Organizations and cybercrime: An analysis of the nature of camps engaged in cybercrime. *International Journal of Cyber Criminology*, 8(1): 1-20.

Bryant, R., Day, E. and Kennedy, I. (2014) Opportunities and challenges for the future. In S. Bryant and R. Bryant (eds.). *Policing digital crime.* England: Ashgate Publishing Limited. 201–228.

Casey, E. (2002) Cyberpatterns: Criminal behaviour on the Internet. In B.E. Turvey (ed.). *Criminal profiling: An introduction to behavioural evidence analysis*. Amsterdam: Elsevier Academic Press. 547 – 572.

Clarke, R.A. and Knake, R.K. (2010) *Cyber war: The next threat to national security and what to do about it.* New York: Harper Collins Publishers.

Cohen, L.E. and Felson, M. (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 44: 588-608.

Cullen, F.T., Agnew, R. and Wilcox, P. (2014) *Criminological theory: Past to present* (5th ed.). New York: Oxford University Press.

Danquah, P. and Longe, O.B. (2011) An empirical test of the space transition theory of cyber criminality: Investigating cybercrime causation factors in Ghana. *African Journal of Computing and ICT*, 2(2): 1, 37–48.

Diamond, B. and Bachmann, M. (2015) Out of the beta phase: Obstacles, challenges and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology*, 9(1): 24–34.

Eastton, C. and Taylor, J. (2011) *Computer crime, investigation, and the law*. Australia: Course Technology Cenage Learning.

Farrall, S., Jackson, J. and Gray, E. (2009) *Social order and the fear of crime in contemporary times.* Oxford: Oxford University Press.

Gibson, W. (1984) *Neuromancer.* New York: Acc.

Grabosky, P. (2004) The global dimension of cybercrime. *Global Crime*, 6(1): 146–157.

Hargreaves, C. and Prince, D. (2013) Understanding cyber criminals and measuring their future activity. Lancaster University. Retrieved September 25, 2015 from: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf.

Holt, T.J. (2003) Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999-2001.*International Journal of Comparative and Applied Criminal Justice*, 27: 199-220.

Holt, T.J. and Bossler, A.M. (2014) An assessment of the current state of cyber crime scholarship. *Deviant Behaviour,* 35: 1, 20-40. DOI: 10.1080/01639-625.2013.822209.

Holt, T.J., Bossler, A.M. and Seigfried-Speller (2015) *Cybercrime and digital forensics*: *An introduction.* New York: Routledge.

Ince, D. (2003) *Oxford dictionary of the Internet*. Oxford: Oxford University Press.

Jaishankar, K. (2007) Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1): 1–6.

Jaishankar, K. (2008) Space transition theory of cybercrime. In Schmallagar, F. and Pittaro, M. (Eds), *Crimes of the Internet,* Upper Saddle River, NJ: Prentice Hall. 283–301.

Jaishankar, K. (2010) The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology*, 4(1 and 2): 26–31.

Jaishankar, K. (2011) Introduction: Expanding cyber criminology with an avant-garde Anthology. In K. Jaishnakar (ed.). *Cyber criminology: Exploring internet crimes and criminal behaviour,* Boca Raton: CRC Press. xxvii- xxxv.

Jones, R. (2009) Cybercrime and internet security: A criminological introduction. In L. Edwards and C. Waelde. *Law and the internet*. Oxford: Hart Publishing. 601-621.

Kaspersky (2015) The great bank robbery: Carbanak cyber gang steals $1bn from 100 financial institutions worldwide. Retrieved September 16, 2015 from: http://www.kaspersky.com/about/news/virus/2015/Carbanakcyber-gang-steals-1-bn-USD-from-100-financial-institutions-worldwide.

Kollock, P. and Smith, M.A. (2005) Communities in cyberspace. In P. Kollock and M.A. Smith (eds.). *Communities in cyberspace*. London: Routledge. 3-24.

Longe, O.B. and Chiemeke, S.C. (2008) Cybercrime and criminality in Nigeria: What roles are internet access points playing? *European Journal of Social Sciences,* 6(4): 132-139.

Lusthans, J. (2013) How organized is organized cybercrime? *Global Crime*, 14(1): 52–60.

Maguire, M. (2015) Sex crimes. In M. Maguire and D. Okada (eds.). *Critical issues in crime and justice: Thought, policy and practice*, (2nd ed.). Los Angeles: Sage Publications. 181–192.

Mitra, A. (2010) *The digital world: Digital security, cyber terrorism and cyber security.* New York: Chelsea House Publishers.

Ndubueze, P.N. (2012) Regulatory agencies, third parties and cybercrime control in Nigeria. *Bayero Sociologists – A Journal of Sociological Studies.* 1(3): 116-134.

Ndubueze, P.N. (2016) Policing cyber terrorism in Africa: Perspectives, problems and prospects. In J. Ingram (ed.). *Policing strategies, management and potential risks* (pp. 59 – 84). New York: Nova Publishers.

Ndubueze, P.N., Igbo, E.U.M. and Okoye, U.O. (2013) Cybercrime victimization among internet active Nigerians: An analysis of the socio-demographic correlates. *International Journal of Criminal Justice Sciences.* 8(2): 225–234.

Ndubueze, P.N. and Igbo, E.U.M. (2014) Third parties and cybercrime policing in Nigeria: Some reflections. *Policing: A Journal of Policy and Practice.* 8(1): 59–68.

Nhan, J. and Bachmann, M. (2015) Developments in cyber criminology. In M. Maguire and D. Okada (eds.). *Critical issues in crime and justice: Thought, policy and practice*, (2nd ed.). Los Angeles: Sage Publications. 209 -228.

Nicaso, A. and Lamothe, L. (2005) *Angels, mobsters and narco-terrorists: The rising menace of global crime empires.* Canada: John Wiley and Sons.

Nicola, A.D. (2014) Trafficking in persons and smuggling of migrants. In P. Reichel and J. Albanese (eds). *Handbook of transnational crime and justice* (2nd ed.). Los Angeles: SAGE. 149–164.

Ojedokun, U.A. and Eraye, M.C. (2012) Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology,* 6(2): 1001–1013.

Olaniran, B. (2008) Electronic tribes (E-Tribes): Some theoretical perspectives and implications. Where is the Shaman? In T.L. Adams and S.A. Smith (Eds.). *Electronic tribes: The virtual worlds of geeks, gamers, shamans, and scammers.* Austin: University of Texas Press. 36-57.

Parker, J. (2008) Introduction: Where is the Shaman? In T.L. Adams and S.A. Smith (eds.). *Electronic tribes: The virtual worlds of geeks, Gamers, shamans, and scammers.* Austin: University of Texas Press. 1-7.

Peshin, E. (2009). A Pragmatic and floor proof approach for connecting critical/industrial networks to external less secure networks. In U. Gori (Ed.). *Modelling cyber security: approaches, methodology, strategies*. Amsterdam: IOS Press. 79–92.

Pratt, T.C., Holtfreter, K. and Reisig, M.D. (2010) Routine Activity Theory and internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency,* 47(3): 267–296.

Radda, S.I., & Ndubueze, P.N. (2013). Fear of on-line victimization among undergraduate Students: A comparative study of two selected urban universities. *African Journal of Criminology and Justice Studies.* 7, (1 & 2): 35- 46.

Rheingold, H. (1994) *The virtual community: Homesteading on the electronic frontier*. New York: Harper Collins.

Rao, C.N.S. (2012) *Sociology: Principles of sociology with an introduction to social thought* (Revised Edition). New Delhi: S. Chand and Company Ltd.

Ritzer, G. (2008) *Modern sociological theory* (7th ed.). Boston: McGraw Hill.

Rogers, M. (2003) The psychology of cyber terrorism. In A. Silke (ed.). *Terrorists, victims and society: Psychological perspectives on terrorism and its consequences*. England: John Wiley and Sons Ltd. 77-92.

Sandywell, B. (2011) On globalization of crime: the Internet and new criminality. In Y. Jewkes and M. Yar (eds.). *Handbook of internet crime*. London: Routledge. 38–66.

Smith, R.G. (2014) Transnational cybercrime and fraud. In Reichel, P. and Albanese, J. (eds.). *Handbook of transnational crime and justice* (2nd ed.). Los Angeles: SAGE Publications. 119-142.

Tade, O. and Aliyu, I. (2011) Social Organization of Internet Fraud among University Undergraduates in Nigeria, *International Journal of Cyber Criminology,* 5(2): 860–87.

Tcherni, M., Davies, A., Lopes, G. and Lizotte, A. (2015). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*. DOI: 10.1080/07418825.2014.994648.

United Nations Office on Drug and Crime (2013) Comprehensive study on cybercrime. Retrieved September 12, 2015 from: https://www.unodc.org/-documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Usman, E. (2012) How ex-General's daughter, Cynthia, was killed by facebook 'friends'. *Vanguard* Online. Retrieved September 16, 2015 from: http://www.vanguardngr.com /2012/08/how-ex-generals-daughter-cynthia-was-killed-by-facebook-friends/.

Vance, D.C. (2008) "Like a neighborhood of sisters": Can culture be formed electronically? In T.L. Adams and S.A. Smith (eds.). *Electronic tribes: The virtual worlds of Geeks, Gamers, Shamans, and Scammers,* Austin: University of Texas Press. 35-57.

Vito, G.F. and Maahs, J.R. (2012) *Criminology: Theory, research and policy.* Sudbury: Jones and Bartlett Learning.

Wall, D.S. (2001) Cybercrimes and the internet. In D.S. Wall (ed.), *Crime and the Internet*. London: Routledge. 1-17.

Wall, D.S. (2005) The Internet as a conduit for criminals. In A. Pattavina (ed.). Information *technology and the criminal justice system*. Thousand Oaks, CA: Sage. 77-98.

Wall, D.S. and Williams, M. (2007) Policing diversity in the digital age: maintaining order in virtual communities. *Criminology and Criminal justice*, 7(4): 319–416.

Wall, D.S. (2008) Cybercrime, media and security: the shaping of public perceptions of cybercrime. *International Review of Law, Computer and Technology*, 22(1-2): 42-63.

Yar, M. (2005) The novelty of "Cyber Crime": An assessment in light of Routine Activity Theory. *European Journal of Criminology*, 2(4): 407–427.