An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats

Article *in* International Journal of Computer Science and Information Security, · May 2014

CITATIONS
0

READS
4,661

3 authors, including:

Ahmed Alnagrat
Universiti Malaysia Perlis
8 PUBLICATIONS **18** CITATIONS
SEE PROFILE

Shakirat Haroon- Sulyman
University of Ilorin
9 PUBLICATIONS **48** CITATIONS
SEE PROFILE

An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats

By

Samson Olasunkanmi Oluga*

Dr Azizah Bt Haji Ahmad

Ahmad Jamah Ahmad Alnagrat

Haroon Shakirat Oluwatosin

Maryam Omar Abdullah Sawad

Nur Adlya Bt Muktar

Of

School of Computing (SOC)

College of Arts and Sciences (CAS)

Universiti Utara Malaysia

06010 Sintok, Kedah

Malaysia

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Abstract

One thing that has emanated from the development of the internet technology and popular embrace of social networking is the emergence of a second digital world which is a virtual reality world called the cyberspace. The cyberspace users who can be described as the *Cyberians* are attracted to the cyberspace from time to time especially because of the various opportunities/activities available via the cyberspace cutting across many spheres of human endeavor. There are however many threats or challenges which may be inimical to the safety of the cyberspace, the cyberspace assets/resources and the interest of the *Cyberians,* the regular cyberspace users or cyber citizens. This paper, based on extensive examination of contemporary literature on the cyberspace, explores fundamental activities of the cyberspace and explicates various forms of cybercrimes orchestrated by cyber criminals posing great threats to the cyberspace. The basic ideas of the paper are equally captured in vivid illustrative models.

Keywords: Cyberspace, Cyber activities, Cybercrimes/Threats

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Introduction/Background

It is axiomatic that the present age of humankind is a computer technology age where virtually all aspect of human activities are computerized or computer-based and basic tasks in most spheres of human endeavor are enhanced or better executed via the instrumentality of modern or state of the art computer technology. It is also crystal clear that the whole wide world is presently in a state of constant transformation courtesy of the advent of advanced computer technology breakthroughs that are systematically revolutionizing the human society. The interesting thing about today's computer technology advancement orchestrated by competitive wizards, working rigorously, independently or collaboratively, all over the globe but driven by the positive goal of making the world a better place, is the quick succession of contemporary computer-based innovations.

Today, it will be highly unimaginable to think of life without computers or reverting to the pre-computer technology age characterized basically by manual execution of human activities and expending a lot of time, energy, efforts or resources on given tasks only to attract minimal results or outcomes. On the other hand, the minimum input with maximal output that is characteristic of computer technology application makes it exceptionally rewarding and simply preferred especially by those who have chosen to be computer technology compliant and always abreast development. The computer/ICT based internet technologies presently afford numerous end users myriads of opportunities online which are improved replicas or computerized versions of the traditional offline activities. It is in the light of the various online social, political, economic and educational activities as well as many others that computer technology/ICT has provided humankind a second world now described as the cyberspace.

The word/term cyberspace has attracted a number of definitions or semantic interpretations especially by experts and lexicographers trying to shed more light on the meaning of the concept. This is characteristic of topical concepts or contemporary phenomena coming to limelight or arousing research interest. Cyberspace according to Adnan (2010) is an unreal world where information is constantly transmitted through or between computers. It is a web of private cum public computer networks. It is a geographical milieu of online conversations, email exchanges, flame wars, spam attacks and information dissemination or exchange. The cyberspace according to Pfaffenberger (2000) simply refers to the virtual space that computer systems have aided its creation, that is, the computer technology invented world. In a similar

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

vein, McGraw Dictionary of Computing and Communications (2003) briefly describes the cyberspace as the digital realms which include websites and virtual worlds.

It is clear from the above definitions/descriptions of cyberspace that the cyberspace is a computer-technology invented /aid world. It is important to point out the fact that the first definition or description of cyberspace as an unreal world may not be as appropriate as the virtual space and digital realm/virtual world of the second and third definitions or descriptions respectively. This is simply because the cyberspace involves a lot of real happenings and activities similar to those of the physical world, so called the real world, hence there is a close relationship. It is against this background that the second world of the cyberspace is also described as the virtual reality world based on the fact that the lexeme 'virtual' semantically depicts something very close to reality.

This paper presents the outcome of an extensive examination of contemporary literature on the topical concept of cyberspace activities and the challenging cyberspace crimes/threats. The paper articulates fifteen (15) fundamental cyberspace activities that are attracting the attention/interest of several millions of cyber-navigators of different ages, genders, professions or status to the cyberspace, from time to time, day to day and place to place. The paper equally sheds light on some eighteen (18) prevalent cybercrimes/cyber threats that now constitute great challenge to the cyberspace as they can be inimical to the safety of the cyber assets/resources and the interest of the *Cyberians*. It fashions illustrative models to capture the ideas or concepts discussed to aid comprehension.

An Exploration of Fundamental Cyberspace Activities

The cyberspace has been constantly growing in terms of the numerical strength of its various users across nations as well as in relation to the various cyberspace activities attracting the numerous users to the cyberspace the world over. Korchmaros, Ybarra, Langhinrichsen-Rolling, Boyd and Lenhart (2013) corroborate the numerical growth of cyberspace users by pointing out the fact that 95% of United States adolescents aged 12-17 use the internet while 54% of the group text messages on daily basis. This is based on the outcome of their study of some 615 adolescents. Kumar (2013) equally puts the total number of internet users in India at 14.2 million by March 2013 with a total of 164.8 million net connections apart from apart from the numerous users of the popular cybercafés. The situation in other Asian countries like Malaysia, Indonesia, Singapore, Japan, Pakistan and China is not different.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The cyberspace is equally growing in terms of the existing cyber activities which have some similitude with those of the physical world and which tend to be more convenient and with less constraint as they can be done usually anywhere there are required facilities and cyber connection. The most fundamental of the cyberspace activities focused are cyber commerce, cyber learning, cyber socialization, cyber gaming, cyber entertainment, cyber journalism, cyber broadcasting, cyber advertising, cyber politics, cyber tourism, cyber medicine, cyber governance, cyber evangelism and cyber mobilization. These are captured in the diagram below and are discussed one after the other in the light of the views of contemporary cyberspace researchers.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Commerce in the Cyberspace

Cyber commerce, otherwise called electronic commerce i.e. e-commerce, covers all forms of electronic, online or internet business transactions. Vakharia, Mishra and Kumar (2013) describe electronic commerce as that which involves selling and buying of goods and services over the World Wide Web i.e. the internet-based business transactions which are fast becoming the order of the day especially because of their cost, choice, and time advantage among other benefits. They identify four main type of electronic commerce namely Business to Business Electronic Commerce,(B2BEC), Business to consumer Electronic Business(B2CEC), Consumer to Consumer Electronic Commerce (C2CEC) and consumer to Business Electronic Commerce(C2BEC). Specifically, in relation to electronic banking, Usman and Shar (2013) identify some basic electronic/banking services viz electronic fund transfer, electronic cheque version and WEB/ATM services. Rahman and Lacey (2013) observe that the development as well as the popularity of the internet has necessitated the transformation of some aspect in traditional commerce into electronic commerce which many have embraced and successfully implemented. This is simply because it has been realised that to compete in today's business/market, especially in a digital age, key business processes/transactions must have online or internet representation i.e. cyber-representation.

Cyber Learning/Education in the Cyberspace

Online learning and electronic learning are some of the terms used to depict the concept of cyber learning/education. Online learning according to Chiu, Chiu and Chang (2007) cited by Yee (2013) refers to learning done via the internet, intranet or extranet. It is regarded as one of the digital tools for the enhancement of teaching and learning the effectiveness or efficacy of which can be a function of how it is utilized. Yee (2013) identifies and examines the various online learning difficulties of some international students in Australian online learning setting or environment. Adeoluwa, Aboderin and Omodara(2013) equally identify computers and internet as essential media of educational technology that have been successfully utilized in teaching and learning. The study conducted by Zhuhadir,Yang and Lytras (2013) on the impact of the social media systems on cyber learners shows that they can facilitate the dissemination of knowledge and engagement of students in the course of teaching more effectively than the traditional face to face teaching approach.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The cyberspace is therefore providing various means of knowledge acquisition and dissemination for virtually all categories of people at all levels. There are electronic-based learning aids for students at various educational levels, pre-school, primary, secondary and tertiary. Permvattana, Amstrong and Murray (2013) discuss how e-learning can be designed to benefit the vision impaired. There are many courses now available online just as there are many exams now conducted online. Many learning materials are made available online just as there are lecture notes/lectures that can accessed online. Electronic versions of books, journals and magazines are now available online and library materials can be accessed without getting to the library. In fact, cyber learning/education has made the acquisition of knowledge interesting and relatively easy for all and sundry especially students, teachers and researchers. There are cyber fora for people to ask members of the cyber communities what they do not know or what they want to know the more, and those who know usually guide those who want to know or want to know the more.

Cyber Socialization/Relationship via the cyberspace

Naturally, humans are social beings hence socialization is more or less a distinctive human characteristic. The development of the internet–aided social networking and emergence of the cyber community now enhance human socialization potentials beyond expectations. Shahid (2013) observe that the importance of the internet technology is evident in virtually all spheres of human life and many now prefer the use of the internet and the new media for social communication than other traditional communication media. In a similar vein, Misra and Stokols (2012) confirm that cyber-oriented individuals have preference for the social virtual environments especially the chart rooms and there is the possibility that many of their real life/world relationships/marriage partners emanated from the cyberspace virtual world. Cyberspace-enhanced social communication has really revolutionized the seeking/initiation of romantic relationships/partnership as can be seen in growing rate of today's online dating. Finkey, Eastwick, Karney, Rels and Sprecher (2012:49) therefore assert that "it is fundamentally altering the dating landscape, restructuring the romantic acquaintance process and changing the nature of compatibility matching". However, it has been observed that some social Cybarians do abuse cyberspace via excessive cyberspace social communication and therefore end up with cyber-relationship addiction. This results from the addiction to the social relationship networking chart room and messaging to the extent that they now find online relationship/acquaintances more important than the existing real life/world

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

relationships/acquaintances. De Fife (2012) adds that excessive social networking or social network addiction can have negative impact as this can lead to social isolation/disengagement from real life activities/societies which ultimately may degenerate to affect social-psychological health by resulting in depression.

Cyber Entertainment in the Cyberspace

Cyber entertainment (cyber-tainment) can overlap with some other cyberspace activities especially those that can equally serve as good instruments of relaxation, amusement and warding off stress. However, cyber entertainment in this context is specifically in respect of how the internet functions as the mechanism or instrument for the provision of online songs, films, video games etc. for the entertainment or enjoyment of today's more than 1.5millions internet users (Jaff & Chen, 2010). O'Keeffe and Clark-Pearson (2011) identify the YouTube as a key entertainment and communication website that happens to be the favourite of many, especially the youth and the young at heart, as well as some blog, gaming and virtual world sites. They further strongly caution that the use of the internet or cyberspace by children needs to be monitored to prevent any abuse or misuse that could negatively impact on them. Lopez-Fernadez, Freixa-Blanxast and Honrubia-Serrano (2013) also buttress the need for a controlled adolescent online/cyber entertainment use by stressing the fact that researches have reported/established non-substance addition to online entertainment among adolescents. However, the fact still remains that cyber entertainment can be to the benefit of users especially when used to ward off stress or ease tension like playing music while working on the system.

Cyber Gaming in the cyberspace

Cyber gaming happens to be one key cyber activity that is attracting the vast majority of the youths to the cyberspace these days. It is basically supposed to be another means of relaxation for the gamers both contemporary trends show that it is now being abused and misused making it attract attention. An International Conference on Cyber Games (CG2008) held in Beijing, China from 27-30 October, 2008 which is a pointer to the topicality of cyber gaming as a key component of the cyber space or key cyberspace activity. Yee (2007) points out that there is an enhancement of cyber gaming with the Massive-Multiplayer Online Role-Playing Games (MMORPGs) online environment that facilitates the interaction of millions of people on daily basis. Cole and Griffith (2007) point out the uniqueness of the MMORPGs in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that they are used as traditional games and for the initiation of relation and for the exploration of places basically because they have both visual and auditory components for players' use. However, Kapahi, Ling, Ramadass and Abdullah (2013) discuss the issue of excessive gaming identified as a sub type of addictive online/internet behaviour emanating from the creation of interactive environment for games platforms. This provokes a sense of wonder, amazement and awe of the fantasy world making cyber gaming an activity that gives gamers the room for imagination. Massive Multiplayer Online Role-Playing Game (MMORPG) is one of the appealing forms of gaming addiction for problematic internet users.

Cyber Journalism of the Cyberspace

Traditional journalism basically involves news gathering and dissemination by the press via the print media like newspapers and magazines hence to Meier (2007:13) "journalism researches, selects and presents issues that are new, factually correct and relevant. It creates public spheres by observing the society, delivering these observations to the mass audience through the periodic mass media and thus constructing a common reality". The development of the digital/internet technology has brought significant changes to the practice of journalism as the traditional mass media control of news transmission or information dissemination to the public has been neutralised or modified by the advent of the digital media (Kaul, 2013).The public now have the option of reading either the traditional hard copy/printed newspapers /magazines sold at the newsstands or the electronic soft copies/versions which many newspapers now make available online.

Sherwood and Nicholson (2013) in their study of newspaper sport journalists discovered that Twitter, Facebook and Fan Forum are web 2.0 platforms commonly used by Australian newspaper sport journalists in the course of news sourcing/researching, news reporting and interacting with their readings. It is important to point out the fact that the development of digital/cyber journalism has attracted divergent views/opinions as some believe it negatively impact on journalism as the way many opt for the online newspapers /magazines will have sales implication while some believed that the traditional print journalism is enhanced by the digital journalism. Potter (2012) points out that some have therefore jumped to the conclusion that the advent of digital journalism will mark the end of the century of print journalism while some are of the opinion that the advent of digital journalism only marks end the of the 20th century journalism and the rise of the new era of journalism that continues to achieve its fundamental goals in dynamic ways.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Broadcasting in the today's Cyberspace

Cyber broadcasting is the otherwise regarded as webcasting and it is usually in respect of two main forms of online/internet broadcasting, namely, online or internet radio broadcasting and online/internet television broadcasting which involves online/internet audio and audio-visual stations or news transmission or information dissemination respectively. The internet radio is otherwise called web radio, net radio, e-radio or streaming radio simply because it involves the use of streaming technology that employs streaming audio format like Window Media Audio and Read Audio. The good thing is that the internet radio stations/services can equally be accessed and enjoyed from any part of the world where there is a good internet service just as the case of CBS Radio and Citadel Broadcasting. Cover It Live, Blog Talk Radio and U Stream are contemporary web-based news broadcasting media.

Somu and Rengarajan (2012:350) observe that the Internet Protocol Television (IPTV)is becoming more and more important especially because of its live TV broadcast as well as a hordes of other interesting services like Video on Demand (VOD) and Personal Video Recorder (PVR).The IPTV according to them refers to "a system that offers digital TV services through internet protocol over the computer network infrastructure which is now an area of research interest because of the increasing desire of TV consumers for interactivity and personalisation". Hartung, Horn, Huschke, Kampmam, Lohmar and Lundevall (2007) however, argue in support of the hybrid broadcast unicast delivery especially because unicast technology is believed to be sufficient based on resource utilization and users experience in many situations . For example, it can enable users to access content on demand without following any fixed schedule among others.

Cyber Advertisement via the Cyberspace

This can also be morphologically regarded as 'cybertisement' though it is now a registered trade mark just as 'cybertising'. Online advertising according to Ha (2008:31)means "deliberate messages placed on third party websites including search engines and directories available through internet access". According to her, they are not unsolicited listing on third party sites and do not include marketers website for promotional and non-promotional

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

purposes, e-mails and other forms of marketing communications and shopping sites such as Amazon.com. Similarly, Haghirian and Madlberger (2005:) define mobile advertising as "the usage of interactive wireless media such as cellular phones and pagers, cordless telephones, personal digital assistants, two-way radios, baby crib monitors, wireless networking system, GPS-based locators and maps to transmit advertising messages to consumers in form of time and locations, sensitive, personalised information with the overall goal to promote goods and services". Cyber advertisement becomes pertinent now that there is dwindling readership of newspapers, a fundamental medium of traditional advertisement, with many now reading newspapers online just as they opt for the online TVs (Salman, Ibrahim, Abdullah, Mustaffa & Mahhob, 2011). However, the need to properly reward or monetize news media online efforts has been identified to complement the new media development and encourage the internet-facilitated new communication/media technology revolution (Yap, 2009).

Cyber Politics/Politicking in the Cyberspace

This, as the name suggests, simply refers to online/internet politics/politicking or political activities as opposed to the age long traditional face to face, print or broadcast media politics/politicking or political activities. Raves (2013) observes that ICT/internet affords citizens of different nations more opportunities to engage in political discourses/discussions thereby making the people to become politically informed and engaged. She, however, points out the fact that some people abuse this medium of cyber politics by being uncivil and derogatory in their political discussion simply because such online political communication gives room for relative animosity. Aronson (2012) in her study of cyber politics examines the role/impact of the new media on the political activities and electoral process in the United States and discovered that they do influence the electoral process vis-a-vis provision of vital political information, increasing political involvement and participation, setting political agenda and influencing election outcome among others.

The concept of cyber politics has become so germane that some institution of higher learning like Villanova University had to incorporate cyber politics components into their political science/communication studies programmes. Also, the political parties of different countries now seize the opportunities of the new media to reach out to the electorate. The incumbent seeking re-election tries to showcase their score cards to the people via the new media to justify their campaign/ quest for re-election just as the opposition uses the new media as well to present their views on why the incumbent should not be considered by the electorate with

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

reasons and promises. Elections before election even come up via online opinion polls which in many cases reflect political trends and realities. Cyber politics/politicking was quietly but extensively utilized during the recent Malaysian elections as instrument of underground political mobilization just as used in many contemporary elections too. It is therefore not surprising that there have been a number of online opinion polls conducted in respect to the next United States presidential election that is still about a thousand days away. This was presumed to be between the Democrat's former Secretary of State, Hillary Clinton and Chris Chistie the present Republican Governor of New Jersey who secured a land slide second term victory.

Cyber Medicine/Cyber Medical Practices in the cyberspace

Cyber medicine otherwise described as internet health by Segal (2009) refers to the act of "accessing electronic health records, consulting physicians emails, shopping online for pharmaceuticals and blogging about illness experience" among others. The author adds that health information is not only transmitted but equally transformed via the web just as internet health users are not just informed but equally transformed via the web. There is therefore an emerging area/concept of medical practice which involves the use of the internet for certain aspects of medical service delivery especially online medical consultation and online drug prescription by qualified physicians. Cyber medicine, however, is not exactly the same as telemedicine though they are over lapping. The former represents an improvement over the latter. The former is said to be usually applied to diagnostic and curative health delivery with limited participants' involvement while the latter relates to preventive and public health. The latter has to do medical consultation or remote treatment of patients usually through telephone conversation or fax communication. The former has to do with studying application of the internet and global networking technologies to medicine and public health, examining the impact and implication of the internet and evaluating opportunities and challenges for health care (Eysebach, Ryoung & Drepgen 1999).

It is important to point out that cyber medicine is not just limited to medical expert's/practitioner's unseen/unknown patients or virtual treatment of patients via the internet. Rather, it equally incorporates the process of medical training. Cowan, Sabari, Kaprales, Porte, Blackstein, Christancho and Dubrowski (2010) in their work or orthopaedic surgey training present a 3-D serious game that was designed using an iterative test and design method for the purpose of training orthopaedic surgery residents the series of steps

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

comprising the total kneel arthroplasty (replacement) procedure using a problem-based learning approach .The usability test of this is a pointer to the fact that the serious game is simplistic, intuitive and stimulating. There is also the cyber knife VSI (Versatile, Simple and Intelligent) system by Accuracy Incorporated designed to enable unprecedented precision of the system and benefiting patients a great deal.

Cyber Governance/Government via the cyberspace

E-government according to Haque, Memon and Shak (2013) refers to online digital government or internet based government involving the use of ICT for the exchange of information and delivery of services with the citizens, business or other arms of government. This, therefore, can be in form of government to citizen (G2C), Government to Business (G2B) or Government to Government (G2G).They identify efficiency, convenience and accessibility to/of public services as key benefits of e-government. Banday and Mattoo (2013) however, add collaboration, empowerment, timelessness and cost effectiveness as the benefits of social media use in e-government. This, to them, requires good social media policy and security measures due to the susceptibility of the social media/government information system to cyber threats/attacks.

The governments of many developed/developing nations now depend a lot on cyber system of/for governmental administration. Cyber journal (2013) expressly declares that the government of Canada (GC) depends on its wired and wireless network for communications and day to day operations hence any threat to their information assets could be very serious and which usually should be prevented. The same goes for the United State that uses the NSA and other security agencies to guard against national cyber information threats/insecurity that may negatively impact on cyber governmental administration. The website challenge of the Obama health care policy is considered by many as a great challenge of the president Barak Obama administration even though many believe it is doing well in some other areas simply because of the role of cyber governance in the present day American governmental administration. Singapore is another country known for a highly cyber-dependent governmental system of administration which was a major reason why some opponents of the government opted for a cyber-attack against the government recently to drive home some point (The Star, 2013). It is important to point out that even the government of North Korea that restricts the use of the internet /cyberspace by citizens has a government website.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Still on the issue of the social media use in e-government, Banday and mattoo (2013) also explicate this with specific reference to the situation in India. They point out that apart from individuals, business organisations and academic institutions that have been using the social media for information dissemination, social interactions, business promotion etc., government have been opting for the social media tools to revolutionize governmental administration for effective government–citizens communication. They further stress the fact that the United Kingdom, the United States, Australia, and Sweden among many other nations do use social media for digital diplomacy.

Cyber Tourism/Online Tourism via the Cyberspace

Cyber tourism, otherwise regarded as online tourism or E-tourism, according to Singh (2003) cited by Dixit, Belwal and Singh (2006) is "a new form of travel product distribution where a supplier/ service provider offers products/services mainly through the medium of internet to a group of customers irrespective of their physical location". Online tourism according to them is fast becoming a concept of research interest hence its semantic interpretation has gone beyond the utilization of the instrumentality of ICT for the enhancement of the marketing of the business of traditional tourism. Rather, it now involves virtual tourism that brings tourist attraction to virtual tourists where ever they are as opposed to the traditional idea of tourists going to the tourist attraction locations.

One of the recent technologies that have facilitated the actualization of the concept of cyber tourism is the three dimension technology simply called the 3D Tech. This technology is the brain behind the 3Dimension virtual tourism which involved the realistic 3D navigation of virtual reality tourist destinations so as to virtually explore physical places without physically travelling to those places. This is made pretty close to reality with the aid of multimedia support features like sound effects and incorporation of narration mainly with the aid of the 3DVT and usually on the internet. Buhalis and Deimezi (2003) confirm the fact that ICT applications have been positively imparting on global tourism especially in relatively tourism-dependent Greek economic System. They add that some innovative tourism organizations are enthusiastically embracing e-tourism and internet tools to enhance business communication with their clients and other stakeholders. He, however, stresses the fact that there is still the need for better utilization, understanding and maximization of the potentials of e-tourism so as to enjoy its competitive advantages vis-a-vis other tourist destinations.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Evangelism via the cyberspace

This is otherwise regarded as internet evangelism or cyber mission. Edmiston **(**2007) identifies the vital role of information technology as one key means for the fulfilment of the great evangelical mission to mark the beginning of his elaborate discussion of internet evangelism and Cyber mission. He observes that the internet has become a spiritual counsellor where many people now channel their spiritual questions and where they now obtain vital information on personal spiritual matters. This according to Chiluwa (2012c) explains why some religious organisations/institutions, that strongly believe that the internet is a fulfilment of prophecy or last day evangelical instrument, have been maximizing the benefits of the new media for the propagation of religious activities. Chiluwa (2013) adds that some offline worships and practices like healing ministration, anointing/communion services, feet worshiping, tithe and offering are also done online. He points out that the online Christian worship in Africa has become so popular thereby leading to the emergence of the Internet Church.

Edmiston (2007) further observes that the mission agencies need to have good understanding of the cyberspace based on the fact that contemporary trends in ICT have shown that the internet and related tools/devices will soon emerge as the dominant instruments of human religious communication. Some of the key benefits of cyber evangelism/internet mission identified include its low cost, low risk, wide geographical reach, possibility of one to many and many to one communication, media multiplicity, multilingualism, its being always on (unterrupted), preservation of messages, not being location dependent/constrained, not requiring many operation licences, bypass of demotivational restrictions etc. He however, rounds off his discussion by stressing the fact that there will be the need for the development of well-established internet evangelism and cyber mission units by 21st century mission agencies so as to reach the unreachable, access the inaccessible and follow up the young believers.

Cyber Mobilization/Activism and Fund raising on the Cyberspace

This can equally be described as online, digital or electronic mobilization/activism/fund raising which simply involves the uses of electronic communication technologies or tools like Twitter, Facebook, YouTube and email to appeal to some people or canvass for their support in respect of a given cause basically to influence their action in favour of the said

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

cause. The Tunisians and Egyptians would quickly come to mind at the mention of cyber mobilisation. Kuebler (2011) discusses the role of the internet as a relatively free space in the political mobilization of Egypt and Tunisia irrespective of all sorts of censorship in place. He points out that Egypt's blogosphere is one of the best documented in the Middle East which has impacted on the Egyptian politics. Kamis and Vaughan (2012) also confirm how the use of the social media especially Facebook, including Twitter, YouTube and text messages, were instrumental to Egyptian revolution. These were said to have been actively and effectively utilized to mobilize and coordinate the protesters towards supporting the common political goal.

However, Stork (2010) adds that cyber mobilization predates even the Tunisian and Egyptian uprisings or the Arab spring uproar by pointing out that the revolutions of Iran and Moldova which were described as "Twitter Revolutions" preceded even the popular Arab spring. Equally important is the fact that the Arab woman are said to be quietly utilizing the instrumentality of the social media underground to advance their causes now described as cyber feminism. She therefore also stresses the role of social media/networking as a tool for the political mobilization of citizens and the actualization of the cause of pro-democracy movements. Cyber mobilization, however, is not limited to political activism or human mobilization only as this can also be in the form of financial mobilisation which entails mobilization of funds required for the execution of given projects especially a philanthropic projects. Corson-Finnerty and Blanchard (1998) therefore describe cyber fundraising as the utilization of internet tools for the enhancement of fund raising and not as a replacement for the traditional method, in such a way that incorporates/accommodates the socially active/ engaged generation of new internet users.

An Explication of Challenging Cyberspace Crimes/Threats

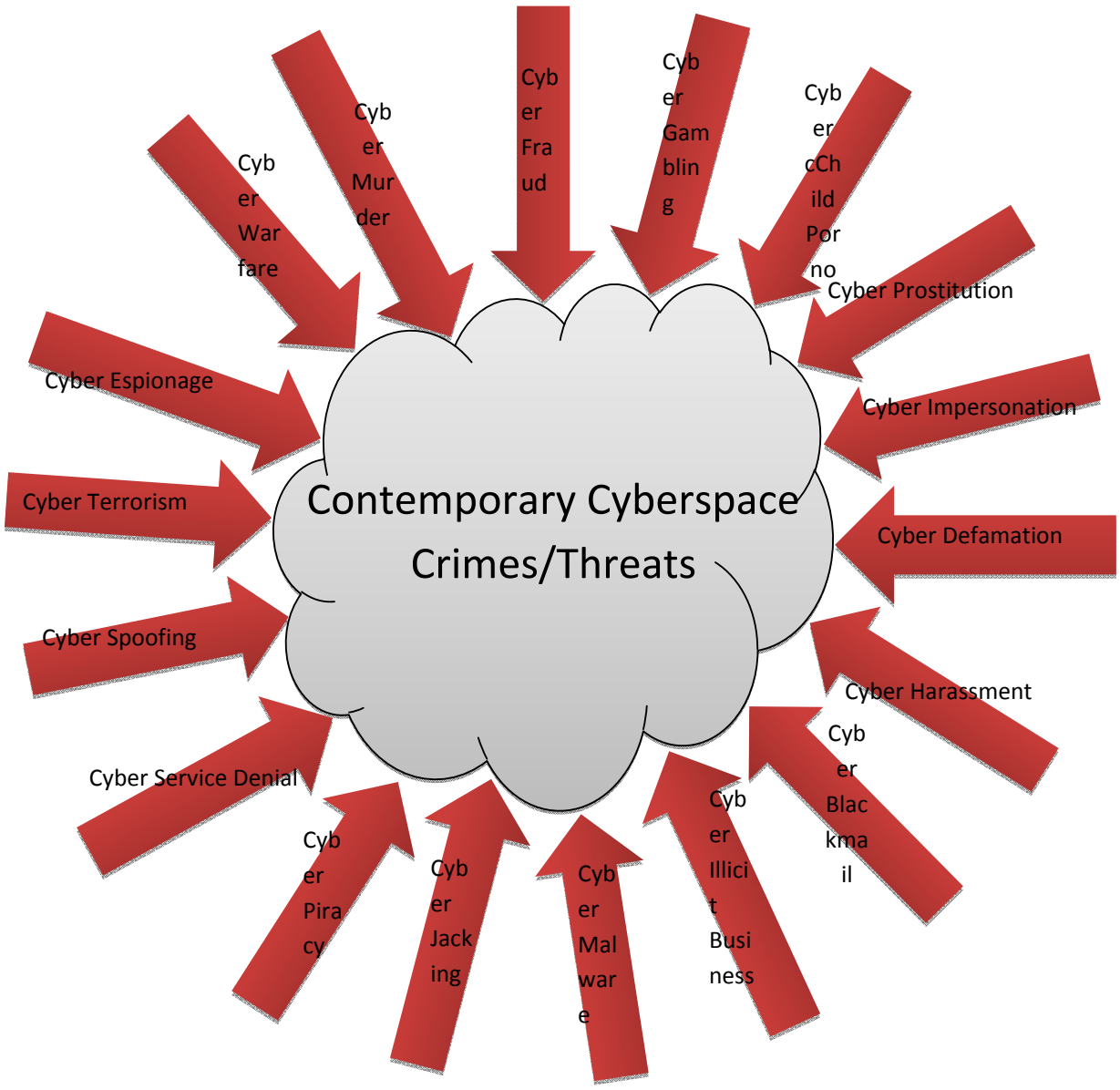
It is disturbing that the cyberspace that is serving multi-dimensional purposes and which is benefitting various people in different ways is now confronted by the preponderance of cyber crimes perpetrated by some, usually unknown, cyber criminals. This unfortunate development has the potential to negatively impact on the life-touching/changing cyberspace activities if not properly and promptly addressed. This means just as we the infiltration of numerous criminal acts or activities in the human society in the physical world, the same is equally happening or experienced in the digital or internet world of the cyberspace. More

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

unfortunately, various types of the cybercrimes keep emerging as existing ones are detected as many innocent and uninformed Cyberians continue to fall victims.

The term cybercrime is otherwise regarded as computer crime, internet crime or web crime and it has attracted various definitions or interpretations by those who have shown interest in this area of study. Nosrati, Hariri and Shakarbeygi (2013:104) first simply describe computer crime as "any crime that involves a computer and a network" and net crime as "the criminal exploitation of the internet". They further comprehensively defines cyber crime in line with Halder and Jaishankar (2011) as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet (chat room, email, notice boards and groups) and mobile phones (SMS/MMS)". Kshetri (2013:118) equally defines cybercrime as "a criminal activity in which computers or computer networks are used as the principal means of committing an offence or violating laws, rules and regulations. To McGee and Byington (2013) cybercrime simply refers to the use of computer in conjunction with the internet for the perpetration of what they describe as White Collar Crime (WCC). There are various cybercrimes presently constituting threats to the cyberspace like cyber fraud, cyber gambling, cyber (child) pornography, cyber prostitution, cyber impersonation, cyber blackmail/extortion, cyber harassment, cyber defamation, cyber malware, cyber illicit business/transaction, cyberjacking, cyber piracy/copyright infringement, cyber denial of service, cyber spoofing, cyber spying and espionage, cyber terrorism, cyber warfare and cyber murder. These are captured in the model below and then discussed one after the other in the light of relevant literature.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Cyber Fraud of the Cyberspace

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

There is prevalence of fraud of various types perpetrated by cyber criminals via the cyberspace just as there are prevalent fraudulent activities in the physical world. Many innocent cyberspace users have fallen victims of the traps of the cyber fraudsters and there is the possibility of many falling victims except precautionary security measures are put in place. Various types of cyber frauds can be identified, namely, financial fraud, email/text message fraud, electoral fraud, airtime fraud, online publication fraud etc. One of the major cybercrimes identified by Nagpal (2008) is financial crime which basically aims at extorting money from targets or victims and which is identified as the key motive behind most crimes. This, according to him includes credit card frauds, money laundering and bank account manipulation. He specifically identifies the "Salami fraud" as an example which involves the insertion of a program into a bank's server to be deducting a token amount from every customer's account which over a period becomes a huge amount of money.

The email/text message fraud is a kind of cyber fraud where the recipient/victim is given a piece of deceptive information aimed at defrauding him or her like saying he/she has been left an unknown inheritance, has won a computer generated lottery or should allow the use of his/her account to lodge a huge amount stolen from some foreign organizations or nations. The cyber electoral fraud relates to the kind of voting fraud or manipulation of results/information where the electronic or online voting system is employed. Cyber fraudsters also advertise and sell some fake products online like those for weight loss and fast money making ventures aimed at siphoning innocent victims' hard earned money. Airtime fraud occurs when somebody's airtime is programmed to be transferred to another person when the victim recharges. On the online publication fraud, Jalahan and Mahboobi (2013) point out how some cyber criminals now create fake websites for journal publications with bogus impact factors just to attract authors who want their work published as quickly as possible and who are ready to pay the exorbitant publication fee charged for the papers that are not usually properly reviewed if reviewed at all.

Cyber Gambling on the Cyberspace

This simply refers to the internet based gambling otherwise regarded as online gambling which according to Wood and Williams (2011) presents the traditional form of gambling in an electronic format on the internet thereby making it accessible to those with internet connection and electronic means of money transfer to participate. They point out that there were 2243 internet gambling websites as of August 2009 with virtual slot machines, pokers,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

horse betting , skill games and casino table games, among others, available online and the number keeps increasing. Although cyber gambling is legalized and regulated in some places especially where traditional gambling is not illegal, it is prohibited in many other places especially where traditional gambling is a crime. Even states like Nevada and New Jersey in the United States only passed laws that allow some forms of online gambling. However, cyber gambling makes it possible for people from all walks of life to gamble freely including those from places where it is prohibited thereby making the cyberspace a free gambling zone.

Griffith and Parke (2002) identify some factors that are likely to be responsible for growth of the internet gambling business like existence of sophisticated gambling software, integrated e-cash system, multilingual sites, increased realism (via web cam gambling) remote wagering and improved customer care systems. They further point out that cyber gambling may not make it easy to control or curb adolescent gambling as those of them who have the credit card information of parents or older siblings can still gamble online. Also, those under the influence of alcohol or drug can gamble away fortune online when they not in the right frame of mind whereas they may be restrained in a non-online gambling setting especially where there are reasonable gamblers or in the company of close friends. The possibility of internet gambling being doubly addictive is however identified based on the fact that internet use and gambling could be addictive. It is in the light of this that Kuss and Griffith (2011) are of the opinion that excessive gaming can result in some of the common symptoms of substance addiction.

Cyber (Child) Pornography of the Cyberspace

Pornography traditionally depicts obscenity and sexually explicit materials. Cyber pornography usually abbreviated as cyber porn and sometimes called web or net porno, according to Desai and Patel (2013) refers to the stimulation of sexual or erotic activities on the internet. They point out that there are free and commercial pornographic sites that offer variety of sexually explicit materials like photos, videos as well as live web cam access that enable those interested to access pornography of all kinds. Cyber pornography happens to be one of the fastest growing online businesses and this is evident in the thousands of pornographic sites in existence. It is important to note that while pornography or cyber pornography is not illegal or prohibited in some countries or societies the case is not the same in many other countries or societies. However, child pornography which involves sexual exploitation of children or involvement/exposure of children to the act of pornography,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

whether online or offline is prohibited in virtually all nations of the world. It is unfortunate that those in the cyber pornography business still engage in this to the satisfaction of pedophiles. This must have informed the recent arrest of 43 men members of an international child porn network with about 140 identified as their victims and several thousands of images discovered in their systems.

There have been a number of researches on the consequences of consumption or excessive exposure to pornographic materials. Owen, Behun, Manning and Reid (2012: 116) observe that "Youth who consume pornography develop unrealistic sexual values and beliefs. Permissive sexual attitudes, sexual occupation and early experimentation have been correlated with more frequent consumption of pornography". They equally point out how researches have linked adolescent use of pornography with increased degrees or levels of sexual aggression just as researches have suggested that those who consume online pornographic materials are prone to low degree of integration/emotional bonding but high level of delinquent/problematic behavior and incidence of depression. In a similar vein, Seigfried-Spellar and Rogers' study (2013) of the effect of consumption of adult-only bestiality and pornography shows that those who started earlier are more likely to be involved in deviant pornography (bestial or child) compared to those who started later.

Cyber Harassment (Bullying and Stalking) on the Cyberspace

Cyber harassment, cyber bullying and cyber stalking are closely related concepts though some have ascribed them slightly different interpretations and classifications. Cyber harassment according to Willard (2007) refers to the act of using telecommunication services to repeatedly communicate unwanted, unpleasant and demeaning messages that are intened to cause emotional distress to the target victims. The two main types of cyber harassment are cyber bullying and cyber stalking. Cyber bullying according to Fraser, Bond-Fraser, Buyting, Korotkov and Noonan (2013:26) involves the use of the internet to denigrate, demean or harass a person with a degree of anonymity and possibly 24 hours a day and 7 days a week. To Belsey (2004) cyber bullying involves the use of electronic communication devices to intimidate, harass and threaten somebody thereby achieving an effect similar to the traditional direct bullying. It is in the light of this that Smith, Mahdavi, Carvalho, Fisher, Russell and Tippett (2008) also define cyber bullying as aggressive behavior of some individual or group executed via modern electronic communication means over a period of time against some defenseless target victim.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber stalking according to Hazelwood and Koon-Magnin (2013) involves repeated pursuit of target individuals by using unwanted electronic communication and by threatening, coercing or intimidating them. Nagpal (2008) also stresses the fact that cyber stalking involves repeatedly harassing or threatening target individuals using the internet, emails or other electronic communication devices. This shows that the basic element of cyber bullying and cyber stalking is harassment or threat hence the classification of both as forms of cyber harassment. The slight distinction lies in the fact that cyber bullying, just as the traditional bullying relates to children and teenagers while cyber stalking is in respect of cyber harassment of adults. This is in line with the position of Chiong (2009) who identifies the case of Megan Meier, who killed herself after being deceived and cyber bullied by a neighbour's mother, as that which popularized cyber harassment .This however, is unlike the categorization of Willard (2006) of online harassment and cyber bullying as two of the identified seven forms of cyber crime similar to Fraser, Bond-Fraser, Buyting, Korotkov, and Noonan (2013) identification of cyber harassment and cyber stalking as methods of cyber bullying. One important point by Notar, Padgett and Roden (2013) in respect of cyber bullying is the fact that the perpetrator need not be strong or swift as all that is needed is access to cellphone or computer with the desire to terrorize target victims.

Cyber Impersonation of the Cyberspace

There is an increase in the rate of cyber impersonation and identity theft of the cyberspace in recent times to which many innocent victims continue to fall victims. Cyber impersonation and identity theft according to T & M Protection Resources (2004) involves using of the internet to post unauthorized, incorrect and/or malicious content that relates to a given individual or fraudulent establishment of an entire personal profile carefully designed and maintained to give the semblance of a real or an existing account. This act can be perpetrated without the knowledge of the affected/target victims as effort is usually made to make such an activity difficult to discover. Ensour (2013) identify two main types of online impersonation as individual impersonation and website impersonation hence these can be in form of impersonation in online commerce, impersonation targeting children, online friendship impersonation, personal identity information theft etc.

Impersonation and deception according to Banerjee, Barman, Faloutsus and Bhuyan (2014) are now very rampant on the internet and they constitute fundamental mechanics usually employed in the perpetration of serious scams especially by pharmers, phishers and DNS

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

squatters. Reznik (2013) corroborates this point and adds that internet or online impersonators usually access the target victims' accounts simply by stealing their passwords using all possible tricks at their disposal and they can equally create a fake profile with which they continue to impersonate their target victim. This is also buttressed with the case of a New Jersey woman who created a fake Facebook profile to discredit her detective ex-boyfriend by portraying him as a drug addict cum sex deviant before she was eventually discovered and accordingly prosecuted. The cyber bullying case of Megan Meier also has element of impersonation as the woman who cyber bullied her first impersonated a 16 year old male friend before eventually resorting to cyber bullying.

Cyber Prostitution on the Cyberspace

Prostitution is an age long illicit act often described as the oldest business or profession which has been revolutionized by computer/internet technology evident in the new concept of cyber prostitution as there is now cyber or online sex. According to Nunez, Medalle, Penaflor and Ranario (2012) cyber prostitution is an online or internet based/aided sexual activity involving the performance of lewd shows before the computer which are paid for accordingly and as agreed. Now, there are online advertisements of brothels sometimes with photographs those offering the services made available, known or unknown to them, so that those interested in their services can contact them online, by email or via text message to book appointment. There are cases of those who pay to watch the private or nude activities of housed prostitutes while dressing, undressing or bathing via cameras strategically installed usually without their knowledge.

Beckham and Prohaska (2012) equally observe that many sex workers now operate on the internet which reduces the number of those now on the streets and makes their activities less obvious. To them, the internet therefore now offers myriads of opportunities for the sexually deviant people to constantly whet their appetite but add that some unfortunate prostitutes usually fall victims of their acts of sexual violence. In a similar vein, Farley (2011) cited in Beckham and Prohaska (2012: 637) also points out that "men who purchase sex often dehumanize women, view them with anger and contempt, and lack empathy for their suffering, hence they separate sex from emotions and they therefore objectify women". However, the cruelty of cyber prostitution is not taken lightly when discovered. Green (2014) reports the arrest of one Aaron Prater charged with felony count of promoting prostitution as one of the ninety people arrested in a six-month five-state investigation into online or cyber

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

prostitution by the Fort Wayne Police Department. This was done in collaboration with members of a federal project leading to several arrests in Ohio, Illinois, Kentucky, Michigan and Texas.

Cyber Defamation (Libel and Slander) on the Cyberspace

Defamation according to Desai and Patel (2013) is otherwise regarded as cyber smearing as it involves the use of a computer/ICT aided message to smudge somebody's image, damage someone's reputation or dent the victim's personality hence its description as character assassination. Such defamation according to Potter (2013) is of two main types namely libel or libelous defamation and slander or slanderous defamation. The former involves defamation in written/printed form or any other form that is permanent while the latter involves defamation in spoken/speech form requiring some additional proofs. Angelotti (2013) looks at the libelous defamation of a form of social media networking, Twitter, with an audience of over 140 million people, described as Twibel and points out the fact that the United States courts are yet to rule on a few Twibel suits that have come up. She further points out the historical position of defamation law to maintain a balance between freedom of speech and protection of people's reputation. She is therefore of the opinion that Twibel should be a legal means of preventing defamation on Twitter without inhibiting civil discourse thereby making the defamation law a legal instrument and not a legal hindrance.

Cyber Malware (Virus, Worm & Trojan) Attack of the Cyberspace

Cyber malware simply refers to malicious code/software which Nosrati, Hariri and Shakarbeygi (2013) identify as one of the three main cybercrimes/attacks that basically target computer devices or networks. To Maitanmi, Ogunlere, Ayinde and Adekunle (2013) malware comprises viruses, worms, Trojans as well as other software that access/attack people's computer systems without their knowledge or pretentiously and which could destroy vital or valuable information if not quickly detected and halted or remedied.

Viruses according to them are computer programs which spread to other computers usually just as biological viruses do but which must be attached to some documents or programs before they can spread and do the havoc or corrupting or deleting data or disrupting an entire system. File virus, boot sector virus, macro virus and hoax(er) virus are forms of computer virus identified by Obi and Okpor (2013). Worms, on the other hand according to them, can automatically replicate themselves and capitalize on some loopholes or weaknesses to attack

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

target systems or essential computer resources like memory space or processing time. Trojans or Trojan horses are unauthorized malicious programs that usually pretend to be authorized and on the basis of which target systems that erroneously accept are attacked (Ibikunle & Eweniyi, 2013). Some of the forms of Trojans identified by experts are hand on theft Trojan, remote access Trojan, data sending Trojan, destructive Trojan, denial of service Trojan and security disabler Trojan.

Cyber Jacking on the Cyberspace

Cyber jacking is somehow closely related to traditional hijacking because just as hijacking involves forcefully or violently seizing and taking control of an aircraft or other related means of transportation, cyber jacking involves forcefully breaking into other people's or organisations' secure or protected systems with the intension of accessing vital information. Nagpal (2008) discusses the concept of web jacking which according to him involves forcefully taking over people's or organisations' websites by web jackers who crack their passwords and may eventually change them. This will ultimately block the access of the original or rightful owners of the hijacked websites thereby depriving them of the sole control of the websites vis-a-vis what is placed on or done via the sites. Recently, the websites of some online/electronic journals have been reportedly hijacked by some cyber criminals who are now operating them with some bogus impact factors to attract authors and make them pay the publication fees, the ultimate goal of hijacking and controlling the journals websites. La Barge and McGuire (2012:47) also discuss the concept of session hijacking which according to them is all about "the exploitation of a valid session key to gain unauthorized access to a computer system or a computer network" They identify four main forms of session hijacking namely session fixation, session side jacking, session key theft and cross site scripting.

Cyber Illicit Business Transactions (Drugs and Fire Arms) of the Cyberspace

The cyberspace is now being used as a cyber haven/rendezvous or safe avenue to initiate, execute or finalize some illegal or illicit business transactions especially the sales of hard drugs and fire arms transactions thereby making the perpetrators activities somehow more hidden. Maitanmi, Ogunlere, Ayinde and Adekunle (2013) therefore identify cyber drug trafficking as a prominent form of cyber crime which is aided by internet technology making the sale and purchase of illegal substances possible online especially through encrypted

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

emails. Nosrati, Hariri and Shakarbeygi (2013) also corroborate the prevalence of cyber drug business and stress the fact that the illicit online business is thriving because it does not involve physical contact or face to face communication hence, many who ordinarily would not have been bold enough to engage in such a transaction conveniently engage in the illicit online business transaction. Another form of cyber illicit business that is thriving online is the sales of guns or fire arms especially those who would have passed background check test like children and those who are non-compos mentis i.e. who are not of sound minds. It is therefore not surprising that the United States alone records about 31,000 gun deaths every year which includes about 19,000 suicides (Bloomberg, 2013).

Cyber Service Denial of the Cyberspace

This is another way of perpetrating cybercrime aimed at depriving given individuals or organizations the opportunity of enjoying desired/required cyber facilities. Denial of Service (DoS) attack is executed basically by flooding a given computer or server with overwhelming requests far more than what can be handled which prevents incoming of expected legitimate requests and which may result in the crash of the system or server and eventual deprivation of authorized users' access. One main type of cyber service denial is Distributed Denial of Service (DDoS) which usually involves a number of perpetrators from different locations or when malware infected computer systems are remotely controlled (as botnet/zombie network) simply to overwhelm the target system or computer.

Gupta, Joshi and Misra (2010) identify Trinoo, TFN, TFN2K, Stachel Draft, Shaft, MStream, Knight and Trinity as some attack tools. According to them a Distributed Denial of Service (DDoS) attack is a situation where a legitimate user or an organization is deprived of some basic cyber services like web, email or network connectivity, that they would normally expect to have". Singleton (2014) however, points out that DDoS attack may not be to attract financial or monetary benefit but to attract some high level attention or recognition. Another form of DoS is email bombing which in a similar vein entails spamming or flooding of an email address or a server with emails so as to block legitimate or authorized emails.

Cyber Piracy/Copy Right Infringement on the Cyberspace

Piracy simply refers to the act of making or producing illegal or unauthorized copies of products or materials considered as the intellectual property of others like books, computer programs or software, films/videos musical CDs or DVDs etc. This is usually prohibited

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

because such items or materials are protected by the copy right law. The copy right law therefore usually prohibits infringement on people's copy righted materials or intellectual property by any person or organization without the copy right owner's permission or appropriate authority's approval. Hommige (2013) observes that with the unique use of the internet as means of information sourcing, gathering and transmission comes the rampant problem of intellectual property infringement due to the unlawful online uploading, downloading or reproduction of other people's copy righted products or materials. Singleton (2013) points out that in February 2013, 178 million Americans watched 33 million online videos which show the value of the intellectual property on the internet just for movies only. Rampant piracy of software according to Hommige (2013) also results in a global loss of about $47 billion annually. Many countries have therefore taken the bold steps of making cyber piracy laws but there are some reservations and challenges in relation to effective implementation of the laws especially due to the ubiquitous nature of the of the cyberspace and the perpetrators of cyber piracy.

Cyber Blackmail and Extortion on the Cyberspace

Cyber blackmail is the online version of the traditional blackmail as it involves using information or secret got about the victim to demand or be demanding for some incredible amount of money backed with the threat to release the said information or secret in case the victim fails to meet the blackmailer's demand. One common secret used in cyber blackmailing or online blackmailing is the nude or seminude pictures of people copied or intercepted by the blackmailer in the course cyber sexual relationship or sexually explicit text messages sent in the course of sexting secret lovers. A lot of money is usually extorted from victims of cyber blackmail especially the wealthy public figures who have names to protect and who do not want to be exposed and there are some ransom ware developed for easy remission of cyber blackmailer's requested ransom. Unfortunately, many blackmailers will usually resurface after collecting and squandering an earlier requested ransom once the victim and the secret are still alive.

Closely related to cyber blackmail is 'sextortion' or sexual blackmail. Sextortion, coined by experts from a combination of 'sex' and 'extortion', involves requesting sexual favour with threat to reveal a secret or release information about somebody's sexual affairs, images or messages. It is therefore a form of sexual blackmail which involves using sexual secret or information to exploit sexually. Frost (2013) gives an account of how some men called

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

'cappers' chat online with teens they call 'camwhores' flatter and manipulate the teens to flash or bare sensitive parts of their body which they secretly capture/snap and use to further blackmail them to do worse things like striping, masturbating or performing other sexual acts that are equally recorded. Many victims of cyber blackmail and sexual blackmail end up killing themselves when they can no longer cope with the incessant demands of the anonymous cyber blackmailers just as in the reported case of Amanda Todd who committed suicide in 2011. Gharibi and Shaabi (2012) therefore caution on sending or posting sensitive personal information on the social networking sites as this may expose people the more to the risk of physical and sexual extortion.

Cyber Spying/Espionage of the Cyberspace

Spying is generally an activity aimed at getting secret information about the target individual, organization or nation while cyber spying involves the use of computers, computer networks or software to get private information which can also be at the individual, organizational, national or international level. Cyber spying is therefore similar to traditional spying except for the fact that it is online or internet based and computer networks or systems aided making it possible for cyber spies to intercept or download valuable documents or information of others by hacking their systems and compromising the security put in place or simply by installing spyware or tracking programs on target systems.

Cyber spying is however described as cyber espionage when there is a large scale case of spying especially which involves nations. China is believed to be one of the perpetrators of cyber espionage done to enhance China's economic competitiveness especially in science and technology hence China is usually alleged of economic espionage (Bryan-Krekel, 2002). However, Pandey and Kusum (2013) believe that on China's economic espionage mechanism, those affected need to put their houses in order, maintain their edge and capitalize on this since reengineering cannot take the place of innovation or originality. The United States National Security Agency (NSA) is also recently accused of large scale spying on Germany, Brazil and others following the spying revelation of Edward Swoden the cyber fugitive now in Russia. The United States however, has been emphasizing the need to employ cyber security surveillance and related measures to protect the interest of America and Americans especially by keeping eyes on the perceived and potential terrorists the world over so as to nip any plans against the US in the bud.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Spoofing on the Cyberspace

Spoofing is all about deception in cyber communication and impersonation aimed at making the targets believe what they would not have believed or do what they would not have done normally. It therefore involves deceptive attempts of some intruders to access the systems/information of some target users by pretending to be who they are not. Different types of cyber spoofing have been identified by Khan (2013) and also by Dalla and Geeta (2013) hence we have SMS spoofing, call spoofing, email spoofing and website spoofing. SMS spoofing involves mobile phone information theft/access and the use of the mobile phone number to send and receive text messages usually through the internet pretending to be the rightful owner of the mobile phone number. Email spoofing similarly involves sending email messages that appear to emanate from the rightful owner of the email address with a similar header but which actually originated from another source. This is done with the aim of sending misinformation or getting vital information like passwords in response. Call spoofing otherwise regarded as caller ID spoofing involves making deceptive telecommunication where telephone network is made or manipulated to show a given number on the receiver's caller ID display quite different that of the real or actual caller. Website spoofing is a situation where a cyber criminal deceives victims with web information and tries to obtain vital information with which they can further scam or defraud e.g. account numbers or passwords. Cyber spoofing however requires or involves some other cyber crimes for its actualization like phishing, key logging, spyware and hacking.

Cyber Murder on the Cyberspace

Cyber murder simply refers to computer or internet technology aided killing which becomes possible because the computer/internet technology is now part and parcel of virtually every human activity which also accounts for why it is embraced by nearly all and sundry. It is in the light of this that Fortinash and Holoday-Worret (2012) describe cyber murder as internet homicide which, according to them, refers to a kind of killing aided by the internet which facilitates the online meeting of the victim and the perpetrator. Ibikunle and Eweniyi (2013) identify as the first example of cyber murder the case in the United States of an hospitalized patient about to be operated but against who some cyber criminal was engaged to murder by remotely altering his prescribed drugs by hacking the hospital computer system. The patient was eventually given a wrong combination of drugs by the nurse and the patient died. In a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

similar vein, there are cases of serial killers who operate via the cyberspace to link, hook and kill their victims or targets hence their activities are equally facilitated by the internet.

Cyber Terrorism of the Cyberspace

Cyber terrorism simply put refers to online or internet based act of terrorism. Embar-Seddon (2002) defines cyber terrorism as "premeditated use of disruptive activities or the threat thereof, in cyberspace, with the intention to further social, ideological religious, political or similar objectives, or to intimidate any person in the furtherance of such objective". In a similar vein, Nosrati, Hariri and Shakarbeygi (2013) describes cyber terrorism as deliberate or intentional use of computers, networks, the internet or other computer tools/devices to perpetrate terrorist activities or to achieve terrorist objectives which could be political or ideological. Cassim (2012) also adds that cyber terrorists now see the cyber space as a digital-age battleground and use computer based high technology to execute their violent or destructive plans making these difficult to detect. Cyber terrorists therefore could target the computer networks controlling power or water supply; road, rail, sea or air transport system; telecommunications, financial/economic or defense system with the ultimate goal of crippling the systems and causing unprecedented havoc. Ahmad, Yunos, Sahib and Yussof (2012) however, present a cyber terrorism conceptual framework that captures the motivation (social, political or ideological), tools (network warfare), method (unlawful means), domain (cyberspace), target (computer/information systems) and impact (economic loss, systemic disruption, and injury/death) of cyber terrorism.

Cyber War/Warfare of the Cyberspace

Cyber warfare is otherwise described as digital war or computer warfare. Cyber warfare according to Dipert (2010) simply refers to an attack of a nation's governmental or civilian information systems via cyber attack instruments like malware and denial of service which unlike in conventional warfare does not cause a physical damage, injure or kill people but which can be inimical to the affected nation's key interests. To Adnan (2010) cyber warfare involves the use of computers and the internet to conduct a cyberspace warfare which may include electronically blinding, jamming, deceiving, overloading or intruding into the target's information and communication circuits/systems. The Star, a Malaysian newspaper, of 9th November, 2013 edition has a story about the recent cyber attack of an Anonymous network of hackers who had threatened war on the government of Singapore and its infrastructure

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

because of the decision to license online news. They actually attacked and made all official websites inaccessible for days which affected the websites of the Police, Internal Security, Ministries of Finance, Home Affairs, National Development, Office of the Prime Minister, the Parliament and the Cabinet. The Estonia's botnet attack of 2007 and 1998 hacking of Serbia's defense system are previous cases that are fresh in the memories of many people. It is important to point out the difference between cyber warfare and cyber terrorism as stressed by Applegate (2014). The former is used to advance the cause or agenda of a given nation while the latter is used to advance the ideology, cause or agenda of a terrorist group or organization.

Conclusion

This paper therefore presents in a nutshell the pros and cons of the virtual world of the cyberspace via the exploration of the fundamental beneficial cyberspace activities and the explication of the prevalent cyber crimes posing great threats or dangers to the cyberspace in the light of relevant contemporary literature. It is therefore paradoxical that just as there are myriads of cyberspace activities positively impacting on individual, organizational, societal, national and international activities or efforts, there are also emergent and challenging cyberspace criminal acts or activities being perpetrated that could negatively impact on individual, organizational, societal, national or international activities or efforts. There is therefore the dire need for all cyberspace stakeholders to sustain or maximize the benefits of the cyberspace, ensure the safety of the cyberspace, protect the cyberspace assets and the interests of the cyberspace users the world over using all logical means and possible strategies.

Good knowledge and application of the basic information and computer security measures are imperative for cyberspace users to be on the safe side while utilizing computer, computer network or cyberspace resources. Contemporary cyber security guidelines and research findings of experts should be widely circulated to enlighten cyberspace users so as to keep them abreast of developments and equip them with the knowledge of contemporary cyber security/safety measures. Such security awareness or consciousness becomes pertinent as a way of exposing reigning or emerging cyberspace crimes/threats, to continually protect innocent cyberspace users and to safeguard their interests. Since cyber criminals now form networks and work in collaboration to rain some cyber havocs, the war against cyber crime should be reinforced with collaborative strategies at the individual, organizational, societal,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

national and international levels. With all cyberspace stakeholders' hands on deck, cyber crimes/threats can be reduced to the barest minimum and the cyberspace made a better and healthier haven for all and sundry.

References

Adnan, M.H. (2010). A dictionary for communication and public relations practice. Shah Alam, Selangor: University Publication Centre (UPENA).

Pfaffenberger, B. (2000). Dictionary of computer terms. (8th ed). Chicago, Il: Webster's New World Book.

Korchmaros, J.D., Ybarra, M.L., Langhinrichsen-Rolling, J., Boyd, D. & Lenhart, A. (2013). Perpetration of teen dating violence in a networked society. *Cyberpsychology, Behavior and Social Networking*, 16(8), 561-567.

McGraw-Hill Dictionary of Computing and Communications (2003). New York: McGraw-Hill Co. Inc.

Vakharia, A.B., Mishra, V. & Kumar, S. (2013). Security glitches related to e-commerce and their solutions. *International Journal of Computer Application,* 2(3), 85-94.

Usman, A.K. & Shah, M.H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2), 1-15.

Rahman, S.M. & Lackey, R. (2013). E-commerce system security for small businesses. *International Journal of Network Security and Its Applications*, 5(2), 193-210.

Permvattana, R., Armstrong, H. & Murray, I. (2013). E-learning for the vision impaired : A holistic perspective. *International Journal of Cyber Society and Education*. 6(1), 15-30.

Yee, R.C.S. (2013). Perception of online learning in an Australian university: An international students' perspective – support for learning. International *Journal of Cyber Society and Education,* 6(1), 45-50.

Adeoluwa, O.V., Aboderin, O.S & Omodara, O.D. (2013). An appraisal of educational technology usage in secondary schools in Ondo State, Nigeria. *International Journal of Innovational and Applied Studies,* 2(3), 265-271.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Zhuhadar, L., Yang, R. & Lytras, M.D. (2013). The impact of social multimedia system on cyber learners. *Computer in Human Behaviour*, 29(1), 378-385.

Sahid, M. (2013). Role of media in political socialization of young generation. *American Based Research Journal*, 2(1), 56-61.

Misra, S. & Stokols, D. (2012). A typology of people-environment relationshipin the digital age. *Technology in Society*, 34(1), 311-325.

Finkel, E.J., Eastwick, P.W., Karney, B.R., Rels, H.T. & Sprecher, S. (2012). Online dating: A critical analysis from the perspective of psychological science. *Psychological Science in the Public Interest*, 13(1), 3-66.

Yee, N. (2007). Motivation of play in online gamers. *Cyber Psychology and Behaviour*, 9(6), 772-775.

Kapahi, A., Ling, C.S., Ramadass, S. & Abdullah, N. (2013). Internet addiction in Malaysia: Causes and Effects, *iBusiness*, 5(2), 72-76.

Cole, H. & Griffiths, M.D. (2007). Social interactions in massively multiplayer online role-playing gamers. *Cyber Psychology and Behaviour*, 10(4), 575-583.

Kaul, V. (2013). Journalism in the age of digital technology. *Online Journal of Communication and Media Technology*, 3(1), 125-143.

Meier, K. (2007). Journalistik. Konstanz: UVK

Sherwood, M. & Nicholson, M. (2012). Web 2.0. platforms and work of newspaper sport journalists. *Journalism*, 14(7), 942-959.

Pottker, H. (2012). Fort mit kommuni kations barrieren. Erwagungen zur rolle des journalismus in der digital mendienwelt. Neue Zuricher Zeitung. Retrieved December 10, 2013 from http://www.nzz.ch/aktwell/startseite/fort-mit-kommunikations-barrieren.

Somu, M. & Rengarajan, (2012), A review on the performance of caching algorithms for video streaming services in IPTV. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(5), 350-355.

Lopez-Fernadez, O., Freixa-Blanxast,& Honrubia-Serrano, M.L. (2013). The problematic internet entertainment use scale for adolescents : Prevalence of problematic internet use

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

among Spanish high school students. *Cyber Psychology, Behaviour and Social Networking*, 16(2), 108-118.

O' Keeffe, G.N. & Clark-Person, K. (2011). Clinical report-The impact of social media on children, adolescents and families. *Pediatrics – Official Journal of the American Academy of Pediatrics.* Retrieved on 5th December, 2013 from pediatrics @ publications.org/content.

Hartung, F., Horn, U., Huschke, J., Lomar, T., Kampmann, M. & Lundevall, M. (2007). Delivery of broadcast services in 3G networks. *IEEE Transactions on Broadcasting*, 5(3), 188-199.

Ha, L. (2008). Online advertising research in advertising journals: A review. *Journal of Current Issues and Researches in Advertising*, 30(1), 31-48.

Haghirian, P. & Madlberger, M. (2005). Consumer attitude toward advertising via mobile devices - An empirical investigation among Austrian users. ECIS, 447-458.

Aronson, E.D. (2012). Cyber-politics: How new media has revolutionized 3rd electoral politics in the United States. *Colgate Academic Review*, 9(1), 148-196.

Cowan, B. Sabri, H. Kapralos, B., Porte, M., Backstein, D., Christancho, S. & Dubrowski, A. (2010). A serious game for total kneel arthroplasty procedure, education and training. *Journal of Cyber therapy and Rehabilitation*, 3(3), 285-298.

Eysenbach, G., Ryoung, S.E. & Diepgen, T.L. (1999). The impact of informatics. Shopping around the internet today and tomorrow: Towards the millennium of cybermedicine. BMJ, 319:1294.

Segal, J.Z. (2009). Internet health and the 21st century patient: A rhetorical view. *Written Communication*, 26 (1), 351-369.

Cyberjournal (July, 2013). Network security: Protecting our information assets. Communication Security Establishment Canada, 3, 1-8. www.csec.st.gc.ca.

Banday, M.T. & Mattoo, M.M. (2013). Social media in e-governance: A study with special reference to China. *Social Networking*, 2, 47-56.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Haque, M., Memon, R.A. & Shaikh, A. (2013). E-government using grid technology: Developing a grid framework for G2G e-communication and collaboration system. *International Journal of Independent Research and Studies*, 2(1), 8-15.

Dixit, M., Belwal, R. & Singh, G. (2006). Online tourism and travel – Analysing trends from marketing perspective. *Skyline Business School Journal*, 3(1), 89-99.

Buhalis, D. & Deimezi, O. (2003). E-tourism development in Greece.: Information communication technologies adoption for the strategic management of the Greek tourism industry. *Tourism and Hospitality Research*, 5(2), 103-130.

Edmiston, J. (2007). Internet evangelism and cyber missions and their impact upon how we do mission in the 21st century. Accessed 13th December, 2013 from www.cybermissions.org/article / 21stc-missions.pdf.

Chiluwa, I. (2012c). Online religion in Nigeria: The internet church and cyber miracles. *Journal of Asian and African Studies*, 47(6), 734-749.

Chiluwa, I. (2013). Communiuty and social interaction in digital religious discourse in Nigeria, Ghana, and Cameroon. Journal of Religion, Media and Digital Culture, 2(1), 1-37.

Kuebler, J. (2011). Overcoming the digital divide: The internet and political mobilization in Egypt and Tunisia. *Cyber Orient*, 5(1). Retrieved from www.cyberorient.net/article. Do?articleid=6212.

Kamis, S. & Vaughan, K. (2012). "We are all Khalid Said": The potentials and limitations of cyberactivism in triggering public mobilization and political change. *Journal of Arab and Muslim Research*, 4(2) DOI: 10.1386/jammr.4.2-3.145-1.

Stork, M. (2011). The roles of social media in political mobilization: A case study of the 2011 Egyptian uprising. Unpublished M.A. Dissertation of University of Andrew, Scotland.

Corson-Finnerty, A. & Blanchard, L. (1998). *Fundraising and friendship raising on the web*. Chicago: American Library Association.

Jalahan, M. & Mahboobi, H. (2013). New corruption detected: Bogus impact factors compiled by fake organisations. *Electronic Physician*, 5(3), 685-686.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Wood, R.J. & Williams, R.J. (2011). A comparative profile of the internet gambler: Demographic characteristics, game play patterns, and problem gambling status. *New Media Society*, 13(7), 1123-1141.

Griffiths, M.D. & Parke, J. (2002). The social impact of internet gambling. *Social Science Computer Review*, 20(3), 312-320.

Kuss, D.J. & Griffiths, M.D. (2011). Online gaming addiction in children and adolescents: A Review of Empirical Research. *Journal of Behavioural Addiction*, 1(1), 1-20.

Desai, P.N. & Patel, A.N. (2013). Cyber crime against person. *International Journal of Innovations in Engineering and Technology*, 2(3), 198-201.

Owens, E.W., Behun, R.J., Manning, J.C., & Reid, R.C. (2012). The impact of internet pornography on Adolescents: A review of the research. *Sexual Addiction and Compulsivity*, 19(2), 99-122.

Seigfried-Spellar, K.C & Rogers, M.K. (2013). Does deviant pornographic use follow a guttman-like progression? *Computer in Human Behaviour*, 29(5), 1997-2003.

Willard, N. (2006). *Cyber bullying and cyber threats*. Eugene, OR: Centre for Safe and Responsible Internet Use.

Willard, N. (2007). *Cyber bullying and cyber threats: Responding to the challenge of online social aggression, threats and distress*. Champaign, Il: Research Press.

Fraser, I., Bond-Fraser, L., Buyting, M., Korotkov, D. & Noonan, S. (2013). Cyber bullying and the law: Are we doing enough? *The American Association of Behavioral and Social Science Journal*, 17(1), 26-39.

Notar, C.E., Padgett, S. & Roden, J. (2013). Cyber bullying: A review of literature. *Universal Journal of Education Research*, 1(1), 1-9.

Belsey, B. (2004). Cyber bullying: An emerging threat to the 'always on' generation. Retrieved January 10, 2014 from www.cyberbullying.ca/pdf/cyberbullying_article_by_Bill - Belsey.pdf.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Hazelwood, S.D. & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminlogy*, 7(2), 155-168.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S. Russel, S. & Tippett, N. (2008). Cyber bullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376-385.

T&M Protection Resources (2014). Cyber identity theft and impersonation. Retrieved 6th January, 2014 from www.tmprotection.com

Reznik, M. (2013). Identity theft on social networking sites: Developing issues of internet impersonation. *Touro Law Review* 29(2).Retrieved from http://digital/commas.tourolaw.edu /lawreview/vol29/1552/12.

Chiong, P. (2009). Cyber bullying and cyber stalking: The verdict. Retrieved January 10, 2014 from www.watoday.com.au/theverdict/2009/cyberbullying.html.

Ensour, H.S. (2013). Online impersonation: A case study in Hashemite Kingdom of Jordan. *International Journal of Engineering and Computer Science*, 5(3), 20-25.

Banerjee, A., Barman, D., Faloutsos, M. & Bhuyan, L.N. (2014). Cyber fraud is one type away. Retrieved January 6, 2014 from http://www.cs.ucr.edu/anirban/anir-infocom.

Numez, V.C., Medalle, M.E., Penaflor, M.V. & Renario, R.J. (2012). Cyber dating determinant factor to cyber prostitution: Basis for the creation of local ordinance. A Research Proposal Presented to the Faculty of Graduate School, Cebu Normal University, Cebu City.

Farley, M. (2011). Comparing sex buyers with men who don't buy sex. A study released exclusively to Newsweek Magazine, 158(4), 637.

Beckham, K. & Prohaska, A. (2012). Deviant man, prostitution and the internet: A qualitative analysis of men who killed prostitute who they met online. **International Journal of Criminal Justice Science**, 7(2), 635-648.

Nosrati, M., Hariri, M. & Shakarbeygi, A. (2013). Computers and internet: From a criminological view. *International Journal of Economy, Management and Social Sciences*, 2(4), 104-107.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Angelotti, E.M. (2003). Twibel law: What defamation and its remedies look like in the age of twitter . *Journal of High Technology Law*, 13(2), 430-507.

Maitanmi, O., Ogunlere, S., Ayinde, S. & Adekunle, Y. (2013). *The International Journal of Engineering and Sciences,* 2(4), 19-25.

Obi, J.C. & Okpor, D.M. (2013). Soft computing virus identification system. *International Journal of Fuzzy Logic System*, 3(2), 63-72.

Ibikunle, F. & Eweniyi, O. (2013). Approaches to cyber security issues in Nigeria: Challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education,* 1(1), 1-11.

Singleton, T. (2014). Understanding the cybercrime waves. *ISACA Journal*, 1(1), 1-5.

Gupta, B.B., Joshi, R.C. & Misra, M. (2010). Distributed denial of service prevention techniques. *International Journal of Computer and Electrical Engineering*, 2(2), 268-276.

Hemmige, N. (2013). Piracy in the internet age. *Journal of Intellectual Property Rights*, 18(1), 457-464.

Bloomberg, M.R. (2013). Forward in Daniel W. Webster and Jon S. Vernick (eds).*Reducing gun violence in America*. Baltimore: John Hopkins University Press.

LaBarge, R. & McGuire, T. (2012), Cloud penetration testing. *International Journal on Cloud Computing Services and Architecture*, 2(6), 43-62.

Bryan-Krekel, P.A. (2012). Occupying the information high ground: Chinese capabilities for computer network operators and cyber espionage. Retrieved from US-China Economic and Security Review Commission at http://www.uscc.gov/rfp/2012/uscc/020report.

Pandey, S.N. & Kusum, H. (2013). China's economic miracle and the statecraft. *Global Research Journal of Business Management*, 1(1), 1-4.

Khan, A.A. (2005). Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Application*, 68?(3), 7-11.

Dalla, H.S. & Geeta, M.S. (2013). Cyber crime-A threat to persons, property, government and societies. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 997-1002.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Frost , R. (2013). Kids online: What are the risks? Centre Arizona Centre against Sexual Assault. http://www. Pewinternet.org/media/files/reports/2013/pip_teenandtechnology.pdf.

Dipert, R.R. (2010). The Ethics of Cyber Warfare. *Journal of Military Ethics,* 9(4), 384-410.

Applegate, S.D. (2014). Cyber Warfare- Addressing new threats in the information age. Retrieved January 26, 2014 from www.academia.edu/cyber_warfare.

Fortinash, K. & Holoday-Worret (2012). *Psychiatric mental health nursing* (5th ed.). Louis: Elsevier.

Green, R.S. (2014).Cyber pimp admits running escort service. *The Journal Gazette*. Retrieved January 4, 2014 from www.journalgazette.net/apps/pbcs.dll/article?

Cassim, F. (2012). Addressing the spectre of cyberterrorism: A comparative perspective. *Potchefstroom Electronic Law Journal,* 15(2), 381-415.

Ahmad, R., Yunos, Z., Sahib, S. & Yusoff, M. (2012). Perception on cyber terrorism: A focus group discussion approach. *Journal of Information Security*, 3(1), 231-237.

Salman, A., Ibrahim, F., Abdullah, M.Y., Mustaffa,N. & Mahhob, M.H. (2011). The impact of new media on traditional mainstream mass media. *The Innovation Journal: The Public Sector Innovation Journal*, 16(3), 1-11.

Nagpal, R. (2008). Evolution of cyber crimes. *Asian School of Cyber Laws Publications*. www.cyberlawdb.co/gcld/wp.

Kumar, V.D. (2013). Cyber crime prevention and role of libraries. *International Journal of Information Dissemination and Technology,* 3(3), 222-224.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500