Texila International Journal of Academic Research
Volume 4, Issue 2, Dec 2017

Cyber Crime in a World without Borders

Article by Henry Osborn Quarshie
Information technology, Texila American University, Ghana
E-mail: henry.quarshie@regent.edu.gh

Abstract

Technology has created a world governed by computers and computer networks. Today's world is a world of a machines. This world of machines evolves and work 24/7 without pausing. This is a man-made world without geographical boundaries. Technology has created a dynamic world out of nowhere. This dynamic world is called the cyberspace, a world without borders. A new world connected by means of computer networks. A virtual space created by networks of computers and the internet. With cybercrime in a world without borders, a criminal no longer needs to be at the actual scene of the crime. This advanced form of crime is perpetuated by means of computer networks and the internet.

Keywords*: Cyberspace, borders, cyber-crime.*

Introduction

Cyberspace is a world created by the Internet. The word became popular in the 1990s when the use of the Internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. *Strate, Lance (1999).* The parent term of cyberspace is ' cybernetics', derived from the Ancient Greek *κυβερνήτης* (*kybernētēs*, steersman, governor, pilot, or rudder), a word introduced by Norbet Wiener for his pioneering work in electronic communication and control science. This word first appeared in the novel Neuromancer by William Gibson. *Vakul Sharma (2010).* With time the term cyberspace has become a conventional means to describe anything associated with the Internet and the every activity associated with the Internet. Although you can find several definitions of cyberspace both in scientific literature and in official governmental sources, there is no fully agreed official definition yet. *Strate, Lance (1999).*

According to Chip Morningstar and F. Randall Farmer, cyberspace is defined more by the social interactions involved rather than its technical implementation. In their view, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other. They derive this concept from the observation that people seek richness, complexity, and depth within a virtual world. *Morningstar, Chip and F. Randall Farmer (2003).*

The most recent draft definition is the following: Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources. *Marco Mayer, Luigi Martino (2014).* Cyberspace includes: a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense ; b) computer systems and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity; c) networks between computer systems; d) networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational); e) the access nodes of users and intermediaries routing nodes; f) constituent data (or resident data). Often, in common parlance (and sometimes in commercial language), networks of networks are called Internet (with a lowercase i), while networks between computers are called intranet. Internet (with a capital I, in journalistic language sometimes called the Net) can be considered a part of the system a). A distinctive and constitutive feature of cyberspace is that no

DOI: 10.21522/TIJAR.2014.04.02.Art007
ISSN: 2520-3088

central entity exercises control over all the networks that make up this new domain. *Marco Mayer, Luigi Martino (2014)*.

Methodology

The paper is a comprehensive review of literature on the concept of crime in the cyber space, a world without borders.

Literature review

Cyberspace and the Physical World

The contours of physical world are fixed. Figure 1, shows the physical world. This shows the earth surface and its climate, countries, people and natural resources. But cyberspace is as vast as human imagination and thus cannot be given a fixed shape. As millions of neurons exist in human brain creating a spectre of life, similarly cyberspace represents network of millions of computers creating a spectre of 'digital life'. Thus, cyberspace can be treated as a natural extension of physical world into an infinite world. *Vakul Sharma (2010)*.

Figure 1. This is the physical world with its fixed contours (Google image).

Cyberspace is a digital medium and not a physical world. It is limitless, constantly changing its shape, attributes and characteristics. It is an interactive world and cannot be referred to as an Xerox version of the geographical space. Such a version exists only in the films like Matrix. The physical world is static, well defined and incremental, but cyberspace is dynamic, undefined and exponential. *Vakul Sharma(2010)*. This is shown on figure 2.

A world without borders

Figure 2. Cyberspace showing networks of communication links, such as blue tooth, WIFI etc., A digital world of communication networks (Google image).

Citizens of cyberspace

Cyberspace has introduced a new kind of world and citizens called Netzens. A Netizen is an inhabitant of the worldwide world (Internet). He is the one, who inhabits the Net and uses it as an extension of his day-to-day physical world. He replicates his physical world actions, like socializing, buying, selling etc. in an online medium. He transcends geographical space and time by a click of a mouse. He recognizes no man-made or geographical boundaries. There is no end to what a netizen can do. The most interesting facet of being netizen is that he could be anonymous, nameless and faceless person, if he wants to and yet can indulge in all kind of activities. *Vakul Sharma (2010).*

A netizen differs from a citizen in the sense that a netizen unlike a citizen, has no constitutional guarantees. No Constitution recognizes netizens as citizens and grant them constitutional rights and duties. Constitution of a country is meant for a specific geographical area. It is meant for the people that reside within that geographical area. Netizens being the traveller of digital highways are basically nameless, faceless nomads crisscrossing the worldwide for convenience. But one should not forget that in cyberspace, netizens exist, citizens don't! It is for these netizens, cyber laws have come into existence. *Vakul Sharma (2010).*

Connecting to the world

With computers and computer networks, one can easily connect to the world in a split second. The internet has made the world smaller, bringing countries, people and businesses close together. Computer devices have become smaller and portable and are able to carry large amount of data/information across the globe. The ever-increasing connectivity of computer technology has brought the world closer. With access to a computer and a modem, you are connected to the world. Today a simple mobile phone is enough to connect you to people in other parts of the world.

DOI: 10.21522/TIJAR.2014.04.02.Art007
ISSN: 2520-3088

Figure 3. This is how one connects to the world today. With a modem and a computer one is connected to the rest of the world (Google image).

Figure 4. These people are connected to the world without borders. With access to an android and any smart phone a person can easily be connected to the world (Google image).

The people behind the cyber crime

Crime is now associated with the use of computers, these types of crime are referred to as computer crime or cybercrime. It is committed by using the computer as a tool, or the computer itself being the subject of the crime. Computer crime is committed by a broad range of people; students, amateurs and professionals. Technology has introduced a host of gangsters with ideological beliefs with the potential to commit all kinds of crime.

Cyber criminals are categorized based on their objectives to commit crime. Children and teenagers between the ages of eight and eighteen are in one category. This group by nature, are anxious to know and explore the world of technology. By this act of exploration, they intend engage in cybercrime. Professionals' criminals have taken their schemes of committing crime online. They have digitised most of the conventional crimes. Today a lot of software tools are developed to perpetuate crime. The crime ranges from stealing simple information to cyber terrorism. These crimes are committed 24/7, making it difficult to crack down on activities. Technology has made it easier for criminals to launch an attack from any part of the world with the means of a simple computer device. These attacks are launched at governments, business organisations, security services and individuals. The difficulty in arresting and persecuting cyber criminals is as a result of different criminal laws in different Countries. These differences in laws have also complicated the fight against cybercrime and increased the activities of the gangsters. In some jurisdictions, cyber criminals are having field day. The pace of crime is a step ahead of arrest and persecution. Typical examples of cybercrimes are; computer hacking, piracy, Internet fraud, identity theft, cyber stalking, credit card information thefts, , spamming, phishing scam, and infecting computers or mobile devices with viruses, spyware, ransomware, Trojan horse and malware. The nature of crime keeps increasing as technology advances.

Figure 5. Pictures depicting how the criminals work. They work from remote places (Google image).

Crime scene

Crime scene, the place where an offence has been committed and forensic evidence may be gathered has gone beyond the conventional methods. The continuous evolving of the techniques by cyber criminals is making it difficult for governments and security agencies to track their activities. With traditional crime, the location of a crime scene can be the place where the crime took place, or can be any area that contains evidence from the crime itself. Scenes are not only limited to a location, but can be any person, place, or object associated with the criminal behaviours that occurred. Today the scene for crime is the computers, laptops, mobile phones and other emerging technological devices. Figure 6. shows a picture of a crime scene. The widespread use of mobile devices has created

DOI: 10.21522/TIJAR.2014.04.02.Art007
ISSN: 2520-3088

unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures.

Figure 6. Today a crime scene is the computer or mobile devices and other emerging technology (Google image).

Reasons for cyber crime

Cybercrime is promoted by many factors, such as Computers and computer networks. These technologies with its speed has added another dimension to crime. Today almost all the conventional crimes have been digitized. Skills in computer programming has also added a new dimension; where tools to perpetuate crimes online have all been developed. These tools are either free and does not cost much. Some of these tools can be downloaded free on the internet. The cybercrime is 24/7 and this is as a result of the following factors.

The coding nature of computer operating systems makes it complex. Criminals are taking advantage of these complexity to carrying out all kinds of fraud. The millions of coding makes it difficult to identify vulnerabilities in a programming. Sometimes before a vulnerability is noted, criminals might have taken advantage to steal millions of cash or crash a system.

New designs in computer technology has made access to computer very easy. With access to a computer and a modem, one is connected to the internet/ world. Criminals are taking advantage of this easy access, to commit all kinds of fraud and develop schemes to rob computer users.

The capacity to store data and information has changed with the advent of computing technology. Devices like the pen drive can store a large amount of data. The carrying of data by simple and small devices makes it vulnerable for criminals to steal. It doesn't take a lot of energy to carry data today.

Criminals always take advantage of vulnerability and the negligence of users of computer systems. A lot of users are not security conscious and will not keep and protect their passwords. Computer technology exposes a lot of users to all kinds of attack.

Another challenge in the criminal justice systems is the finding of evidence to support criminal case. Sometimes the evidence will be hiding in a computer devices in a remote site. Access to it can be difficult and expensive. Some other evidences can be on small and simple devices like the pen drive and mobile phone, which can easily be disposed of by the criminal, making access to it to support a criminal case very difficult and in some case impossible.

Practical international challenges

The growing trend of computing technology has not kept pace with the criminal justice systems of the world. Very few countries have adequate laws to address the problem of cyber-crime. Cybercrime is a new form of transnational crime and addressing it requires a concerted international cooperation. The United Nations has identified some challenges in addressing these international cooperation in fighting cyber-crime. The following are the challenges in addressing the legal and criminal justice system according to the United Nations.

- The lack of global consensus on what types of conduct should constitute a computer-related crime;
- The lack of global consensus on the legal definition of criminal conduct;
- The lack of expertise on the part of police, prosecutors and the courts in this field;
- The inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerized data;
- The lack of harmonization between the different national procedural laws concerning the investigation of computer-related crimes;
- The transnational character of many computer crimes;

The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special requirements of computer-crime investigation. (United Nations Manual on the prevention and control of computer-related crime).

Conclusion

The forgoing analysis indicates that the internet has made the world smaller than we thought. Computer devices have become smaller and portable and are able to carry large amount of data/information across the globe. The ever-increasing connectivity of computer technology has brought the world closer. With access to a computer and a modem, you are connected to the world. Today a simple mobile phone is enough to connect you to people in other parts of the world. Fighting cyber-crime in a world without borders needs a concerted efforts by all stakeholders in the Law enforcement, civil society and governments. Cyber-crime is a new form of transnational crime and effectively addressing it requires concerted international cooperation.

References

[1]. Henry O. Quarshie & Alex Martin Odoom, (2012), Fighting Cyber-crime in Africa. Scientific and Academic publishing. Computer Science and Engineering (Vol.2, No.6,).

[2]. Henry O. Quarshie (2013), Fighting Cyber Crime- Issues of Jurisdiction, Journal of Emerging Trends in Computing Information Sciences (vol 4. No. 1).

[3]. Marco Mayer, Luigi Martino, Pablo Mazurier and Gergana Tzvetkova, Draft Pisa, 19.05.2014 www.academia.edu.

[4]. Michael Hauben, New York and Beppu November 1995 netizens@computer.org.

[5]. Morningstar, Chip and F. Randall Farmer. The Lessons of Lucasfilm's Habitat. *The New Media Reader*. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, 2003. 664-667.

[6]. Parthasarathi Pati, (2010) Cyber-crime, The Indian Law Institute.

[7]. Strate, Lance (1999). "The varieties of cyberspace: Problems in definition and delimitation". Western Journal of Communication. **63** (3).

[8]. United Nations, International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime.

[9]. Vakul Sharma (2010) Introduction to Cyber World and Cyber Law, the Indian Law Institute.

[10]. Versha Vahini, Regulatory framework, The Indian Law Institute. New Delhi.

[11]. Vishnu Konoorayar, (2003) Regulating Cyberspace: The Emerging Problems and Challenges, Cochin University Law Review. www.carnegiecyberacademy.com.