Webology (ISSN: 1735-188X)
Volume 17, Number 4, 2020

# An Analysis of issues and challenges in Cybercrime related to Jurisdiction in the Transnational Cyberspace

Surender Kumar*
* Assistant Professor, Institute of Law, Kurukshetra University, Kurukshetra-136119
e-mail: surenjaglan@gmail.com

**Abstract**

In the Information Technology revolution, cyberspace and cyber world are unavoidable advancements. This paper aims at providing a brief overview of cybercrime, issues and challenges involved in it. The new place for committing offences and crimes. The virtual world connects the people of one place or territory with people of another place without their physical meetings through the internet to access a number of services. Information is made available electronically through the use of technological advancements. It is important to keep in mind that technological advancements come with both advantages and disadvantages. The close association of technology and crime is not a new thing. As a result of the revolution in information technology, cybercrime has become an increasingly widespread criminal activity.

**Keywords:** Information Technology, Cyber world, Cyber crime

## Introduction

It is a common saying that "crimes will be committed in every age, every place and by every means". Theorists have predicted that in the future, as technology advances, criminals will be able to commit more sophisticated and difficult to detect crimes by using computers. The internet is the epitome of the information society (Fitzgerald, 2003).Our society has undergone some significant changes as a result of information being easily accessible to many. The world is experiencing a unique era in human history. The internet provides the users with a sense of freedom, anonymity, and global access. The internet has become an indispensable tool for business, education, social interaction and entertainment. Due to the increased use of the internet, the number of cybercrime cases has also increased. The internet provides the users with a sense of freedom, anonymity, and global access. The internet has become an indispensable tool for business, education, social interaction and entertainment. Due to the increased use of the internet, the number of cybercrime cases has also increased.

It is quite interesting to learn some of the reasons behind the internet's popularity. Globalization has become a reality thanks to the internet. You can save time and It is easier and cheaper to access and publish information this way than using traditional methods.

Everyone, who have an active internet connection, correct web address can assess all informations available on the internet. The certain amount of material can be accessed indiscriminately through this method. By using the internet, a person can sell goods to a number of different customers all over the world today, unlike in the old days. Furthermore, anyone can publish information about certain person or corporation on a webpage.

**Cyber space**

It encompasses a wide range of e-devices that use optical fibers, digital signals, data, bytes, and similar elements. At an instant of time on web space so many activities are performed but that all cannot be seen, and out of that some are visible but that are intangible. That's a world away from one's believe. There has been a dramatic change in the real world due to this virtual work. Due to immense potential and infinite possibilities it's become compulsion for a man to live in the digital world. In other words, he is looking for something that he could never even dream of finding in reality. Hence his fascination and obsession for this subject is growing stronger and more consuming with each moment that he experiences.

It has been defined in many ways that includes data to be stored, modified and exchanged through a network and associated physical infrastructures by the use of electronics and the electromagnetic spectrum. The electronic medium have an online communication through computer networks. The electronic information is communicated over computer networks. The computer network transmit and exchange data by using TCP/IP Network protocols; or the realm of e-communication, or a virtual reality; or, a non-physical terrain created by computer systems.

William Gibson in his novel 'Neuromancer' first time used the word 'cyberspace', which waspublished in 1984. Gibson has explain the cyber space in these words:

"A In every nation, there are billions of legitimate operators experiencing a consensual hallucination, as do children who are learning mathematics. A graphical representation of abstract data that has been extracted from the databases of every computer in the human system. An unimaginable complexity, light lines stretching in the non-space of the mind, clusters and constellations of data."

**Objectives of the Study**

The present article has the primary aim to gain knowledge and discuss about the major issues and challenges relating to cyber-crimes. The goals of this paper are:

- To examine the traditional philosophy of law towards cybercrime and impacts of the internet upon this
- To define the different types cyber crimes
- To discuss about the new challenges relating to jurisdiction and applicability oftraditional legislations

**Methodology**

This study is based upon the Secondary data and investigates literature on the cyber-crimes in India and worldwide, which is available. Journals, newspapers, books, and websites were used to gather the information in this paper.

## Meaning and Description

### Cyber crimes

That's always a matter of debate whether new legislation should be passed to deal with cybercrimes or whether already existing legal systems can effectively deal with this new type of criminality. In some schools of thought, cybercrimes are not different from ordinary crimes like trespass, larceny, and conspiracy, except such crimes are commit by using a computer as a tool or medium. As jurists of other schools have recognized the distinctive nature of this emerging technologies and the distinctive set of challenges they entail, regarding nature and scope of cybercrime, and the difficulties in tracking down the offender, as well as the difficulties in enforcing the law. It contents that there should be a new legislative framework for dealing with cybercrimes because cybercrimes have been viewed as crimes committed by computers and requiring new laws.

With the exponential growth of the internet, computer crimes have taken on a whole new dimension. According to a survey conducted in the U.S. on 643 computer security practitioners, 70% of those reported serious computer security breaches unlike Malware-viruses, Identity theft, or employee internet abuse. These computer security breaches includes theft of proprietary information, financial fraud, system penetration and sabotage of networks or data.

Internet has led to a new generation of crimes. A number of offences have already made their mark, including hacking and cracking, website defacement, cyber pornography, Phishing, Key Loggers, tele-communication fraud, cyber terrorism, spamming, pornography, and pirated products and services. One of the most pressing issues with the current electronic payment system is the vulnerability to credit card fraud. In addition, the rise of cyber terrorism has also created new risks, such as cyber laundering and a secure internet communication. The lack of adequate safeguards is a major concern for both banks and law enforcement agencies. The pirated software is also a major problem. The video and phonographic industries are strugglingas a result.

### Cybercrime and Its kinds

Cybercrime is commonly defined as any crime that takes place online or through the use of computers. This can include, but is not only limited to, computer trespass and defacing, possession and transmission of harmful programs without any authority. The another category of cybercrime, which is more commonly referred to as cyber terrorism, is one in which governments are often targeted.

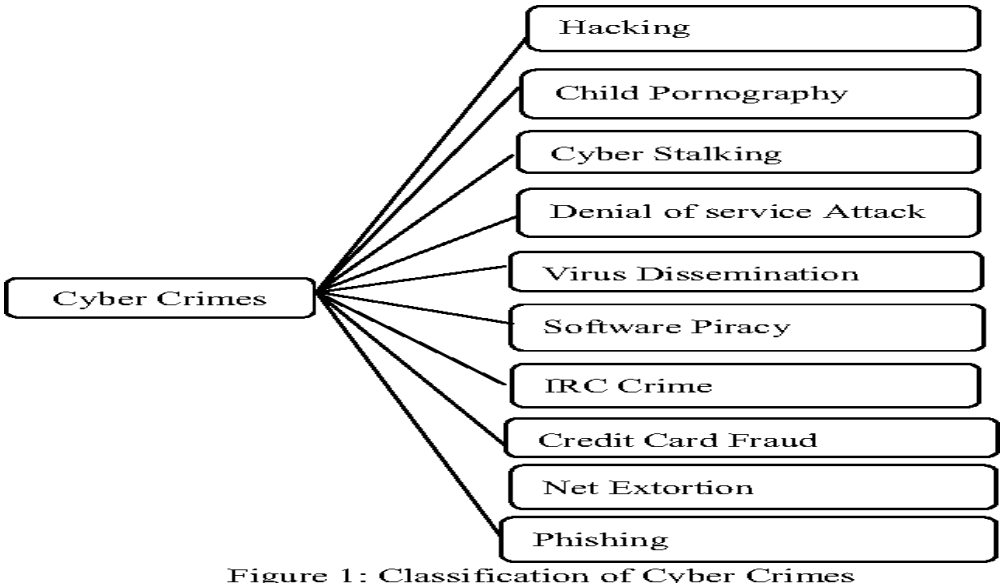


Figure 1: Classification of Cyber Crimes

David L. Carter has given the most comprehensive classification of computer crimes, dividing them into three categories:

A. the crime in which computer is targeted;
B. the commission of those crime where computer facilitates;
C. Crime in which, computer is incidental.

**Jurisdictional Challenge of Cyber Crimes**

Cyberspace knows no geographical borderline, which is an advantage for cyber criminals. They perform illegal activities without any fear to be tracked on the internet. The law enforcement agencies be lacking of knowledge of how the internet actually works further complicates the matter. In terms of cybercrime challenges, we can categorize them as follows:

**A.** The legal challenges of cybercrime related to investigation and control dependents on the use of statutory provisions;
**B.** Well-trained and equipped investigators repiure at a national and international level to overcome operational challenges;
**C.** Online offenders must be caught and prosecuted by the law enforcement agencies that's a great technical challenges for all the world agencies.

Cybercrimes are often committed without any specific borderline. The behavior of criminals also vary due to national standards. Furthermore, due to internet facilities and anonymity it becomes back-breaking to point out the perpetrator of wrong. That gives cybercrimes a unique character unlike traditional crime. It is not sufficient to pass national legislation to deal with these crimes effectively. The Information Technology Act, 2000 has jurisdiction beyond territory of India and also applies to any illegal act or contravention committed outside India by any person. Internet laws features like this are not uncommon. Almost identical provision is found in the Information Technology legislations of other nations also. A provision like this can, however, only be effective if governments and enforcement authorities work together at the international level.

## Challenges to the Law

The internet provides the ability to conduct trans-border activities, which poses a challenge for traditional philosophy. With the increase of e-commerce it becomes more difficult to protect consumers from cross-border fraudulent and deceptive commercial practices because the current laws, consumer protection policy and enforcement systems to stop fraudulent and deceptive commercial practices against consumers were created when such practices were mostly happening domestically. Another challenge that global law enforcement faces is the diverse legal systems present throughout the world.

## Conclusion

Combating cybercrime still has a long way to go. More laws need to be enacted while amending the current ones so that they can easily deal with the sophistication of cybercrime. New technologies must be developed to protect people from mobile devices, as this is the next front for cyber criminals to attack. The lag between technological advancements and the ability of law-makers to regulate them, give rise to a serious challenge that the existing theories cannot adequately explain how to regulate the internet by traditional legal notions. Legislators and Jurists must accept this challenge and develop a new viewpoint relating to jurisdiction issue. As internet activities are ubiquitous, non-territorial, and potentially anonymous in nature, hence conventional approaches are road-blockers to innovation because they are unable to adapt it.

Education of the public must be upped so that people can be able to take precautionary measures to avoid being victims of cybercrime activities. Educating people will also help them identify suspicious activities that may lead to cybercrime

## References


- Raut, Bimal.(2004). Judicial Jurisdiction in The Transnational Cyberspace. New Era LawPublication. Print.
- Viswanathan, Aparna.(2012). Cyber Law: Indian and International Perspectives. LexisNexis Butterworths Wadhwa,Nagpur.Print
- Allen, Paller. (2007). The Chattered Institute for IT. Web.
- Jain, Atul. (2005). Cyber Crime: Cyber Crime: issues and threats. Delhi: Asha Books, Print.Kitchen, Cute. (2010). Cyber Crime History and Cyber Crime Types. Web.
- Newton, Michael. (2004).The encyclopedia of high-tech crime and crime-fighting. New York:Check Mark Books. Print.
- Regoli, Robert, & Hewitt, John.( 2007). Exploring Criminal Justice. New York: Jones &Bartlette Learning, Print.
- Schell, Bernadette Hlubik, Martin, & Clemens. (2004).Cybercrime: A reference handbook. Santa Barbara: ABC-CLIO Inc, Print.
- Wall, David.(2007). Cybercrime: The transformation of crime in the information age.Cambridge: Polity press, Print.
- Fitzgerald B ' *Dow Jones & Co Inc.v. Gutnick:* Negotiating " American Legal Hegemony" in the Transnational World of Cyberspace'(2003)27 *Melbourne University Law Review* 590.