CYBER CRIMES AND GLOBLIZATION

Dr. Bijendr Pradhan - Associate Professor, Department of Social Work
Jain Vishva Bharti University, Ladnun, Rajasthan

Prince Jain - MSW (Final Year Student), Department of Social Work
Jain Vishva Bharti University, Ladnun, Rajasthan

Abstract:
The invention of fire and wheel were the two greatest inventions by earlier men. Later on it led to inventions like telegram, telephone, Computer etc. The advent of computer brought revolution in information technology sector, and now the world is in your hand within a click with help of INTERNET, the internet grown at a staggering rate. It's become part and parcel of our social life. Due to the development of computer and internet system, people can access the information throughout the world. Today, no part of the world can remain unaccessed of human being. Computer civilization has made great significant changes in information sector. Due to development of private sector in communication systems one person who resides in interior area can access an institution, knowledge and job prospective within a second. The purpose of information technology law is free flow of information with reasonable restrictions.[1] Due to development information and technology, crimes have also increased. To check the cyber-crime, IT laws have become essential.[2] Why we need this is matter because Globalization brings opportunities with challenges and it's our collective responsibility to tackle it, because changes to society and technology have increased the dangers associated with inadequate controls on processing activities. The use of computer technology and the ability to transfer and publish our life became easier but on another side it's also create problems. Present paper focuses on cyber-crime and globalization.
Key words: Globalization, cyber, cyber-crime & laws, information technology, etc.

1. Introduction:

" Necessity is mother of invention " the Invention of fire and wheel, two greatest invention by early men which later leads to modern men an invention of telegram, telephone, telescope, pen radio many more things without which use can't product or survive now a day , it is either medical or communication.

Communication: - which change whole world scenario an invention of abacus to birth of computer. In earlier time, human beings used birds, drums etc. to communicate message but now, with in a click we can reach to many people at many place at any time, without any time los. What is that things--- internet? It's brings revolution in fields of communication. The computer, revolution has become part and parcel of social economic and political life. It makes life more fast and easy and more suitable for development of human civilization. The internet user is increasing day by day. Medical, education, politics, government, science, law, agriculture even music, art not escaping from this magic. And here, the problems arise as it is said that, "any things in excess becomes dangerous".

Computer & internet also brings challenges paperless contract, digital signature, online transition, and result into cybercrimes. Cracking computer becomes rite of passage for some teenager and students and day by day cyber phobia among computer user is increasing. As our life becomes easy and smart on the other hand it gives us as "cybercrimes".

2. What is cyber crime ?

21st century , in which people makes contacts virtually , spending more time on internet and less time to talk face to face, through mobile technology with 3G & 4G speed , no doubt its save time and money and making our life luxurious but it also causes serious problems, which affect globally. The internet is fast becoming a way of life for millions of people. However , it is also being transformed into a havens of criminals.[4] Cyber space create lots of opportunities for knowledge, information but also give birth to disorder like cyber phobia. And we got confused about the term 'cybercrime'.

Generally we have picture about crime is that it is murder, killing, robbery, kidnapping etc. but in cyberspace, it is all about hacking, forgery, cyber terrorism etc. as there is no uniform accepted definition. Cyber-crime is that crime which violate cyber law and cyber jurisprudence. Cyber-crime is the most dangerous of all crimes because of the magnitude of the loss, it is causing today and its potential. The term cyber is derived from term 'cybernetics ' which means science of communication and control over machine and man. In wider sense cyber-crime is crime on the internet which includes hacking, terrorism, fraud, illegal gambling, and cyber stalking and cyber theft forgery, cyber pornography.

3. Types of cyber crime:

Cyber pornography

Broadly explaining, cyber pornography refers to stimulating sexual or other erotic activity over internet. This would include pornography web sites, magazines, pictures photos, writing etc. in recent times these have been incurable instances of promotion of pornography through use of computer. Information technology has made it much easier to create and distribute pornographic materials through the internet such material can be transmitted all over the world in a matter of seconds. Child pornography is different from other pornography and consequently receives more strength legal treatment.

Section 67B of information technology Act 2000; discuss punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.

Child abuse sexual violence against woman and other sexual crimes are the direct effect of pornographic images which also causing breaking of marriage tie, juvenile delinquency and sexual disease. In contemporary phenomenon World Wide Web has become the playground and game room.

Steganography

This technique is the secret data inside other files as usages files, sound or video files. The secret data can also be hidden in the files unallocated sector of a disk. This data become invisible for anyone who does not know the life name and password. Stenography mean hide the files which are out of reach of any person information hide in different files is known as steganography.

(a) Trojan horse

It is a commonly used methods for committing computer based frond and very hard to detect. A Trojan horse is a malicious programmed that pretend to be beginning appreciation it's contains codes intended to descript computer system or E-commerce site. It is a program that contains hidden code allowing an outsider to assuming use privileges and steal passwords and files.

(b) Computer forgery

It is the altercation of computerization document. Since the advent of high resolution computerization color laser copier, a new generation of fraud dent counter testing was emerged. These copiers can modify existing documents the quality of which is indistinguishable from the original without referring to an expert for analysis.

(c) Computer sabotage

The use of internet to hinder the normal functioning of computer system through the internet introducing of worms, virus or logic banks referred to as computer sabotage. Computer sabotage can be used to gain economic advantages over a competition to promote the illegal activities, or steals data or program me for extortion purpose.

(d) Computer defamation

The law of defamation is danger to protect the reputation of an injured party by giving him the right to sue for damages. Cyber defamation in this context would imply defamation by anything which can be read, seen, or heard with help of computer. Computer is tool for transferring information one place to other place when information which defame in nature is cyber defamation.

(e) Corporate Cybermear

It is false and disparaging rumors about a company, its management or its stock that is posted on the internet. This kind of criminal activity has been concern especially in stock market and financial sector where knowledge and information are the key factor for business .

(f) Cryptography

Privacy and data security have been important issue since the dawn of computer age, but they did not originate with the computer age. Paper records and files can also threaten privacy or reveal other confidential or sensitive information. Long before computers were invented, most organizational kept their critical files under lock and key restricted access to them maintains security. Cryptography is the science and art of secret writing. Keeping information secret when applied in computer environment cryptography can protect data against unauthorized disclosure.

(g) Encryption

Encryption is the process of encoding information so that it is secure from the internet user. It refers to any process that is intended to obscure the contents of the message. It is often describing in general media as scrambling of data to make it unintelligible. It is translation of data in secret code.[18]

Cyber Terrorism

The term cyber terrorism is coined by a senior research fellow in California Institute for security and intelligence Mr. Barry Collin in 1980 composed two term Cyberspace and terrorism. According to him cyberspace is the place where computers data move and computers function. In year, 1997 Mathews Devort Brian Honghton and Neal Pollard said, “Information Terrorism is the international abuse of digital information system, network or components towards an end that support or facilitates a terrorist campaign or action.

The two prime concepts of cyber terrorism is, that Terrorist use the information ,technology to attract their audience by creating violence through deferment of web sites, denial of service attack, hacking cracking , tampering with source code flowing virus etc. Where computer is used as target or weapon and which go against government and national security. Another ids terrorized used of information technology i.e. cyber pornography, fraud, cyber theft spamming, etc.

Cyber Warfare

Cyber war is that war which fought by internet between countries. When one country accesses the secret of other country by internet and uses that secret against that country is known as cyber warfare. In the era of information and communication technology one nation causes terrorist violence by using new technology against other nation. For example between India and Pakistan Net war, China and USA net war.

Spamming Fake Information

Spamming which is fake information, junk mail to harass other and to damage or unauthorized access computer data or network.

Cyber Squatting

In popular term, cyber-squatting is the term most frequently used to describe the deliberate, bad faith, abusive registration of a domain name in violation of rights in trade mark and service mark.

Obscenity

The word obscenity as the dictionaries tell us denotes the quality of being obscure which means offensive, to modesty or decency loud filthy repulsive. Loathsome, indecent and Lewd.

In Radian law Dictionary obscure has been defined as "a term applied to acts or words or representations that shock public ideas of sexual purity or modesty. The test for obscenity has been said to be whether words tend to be define the morals of persons who would see the publication of suggesting law thoughts and exciting sexual desires.

4 Nature of Cyber Crime:

(a) Cyber Stalking

In very general terms stalking refers to harassing or threatening behavior that an individual engages in repeatedly towards another person. Cyber stalking, is simply a extension of the physical form of stalking, is where the electronic mediums such as internet are used to pursue, or contact another in an unsolicited fashion.

(b) Hacking

It is unauthorized access to computer and refer to access to the whole or any part of a computer system without permission. Hackers worldwide attempt to hack into remote computer for multiple purpose like eavesdropping data theft, fraud, destruction of data, causing damages to computer system, or for mere pleasure or personal satisfaction.

5. Cyber Fraud:

The United Kingdom defined Cyber fraud as "any fraudulent behavior connected with computerization by which someone intends to gain financial advantage".

According to D. Bainbridge, the phrase 'computer fraud' is used to describe stealing money or property by means of a computer that is using a computer to obtain dishonesty, property, including money and cheques , credit cards services, or to evade dishonestly some debts or liability , it involve dishonestly giving an instruction to a computer to transfer funds into a bank account or using a forged bank cards to obtain money from a ATM.

6. International Initiative to Prevent and Control Cyber Terrorism:

Cyber terrorism brought back the cold war situation again. The United Nations and European Union's always played and are playing significant roles to prevent and control menace.

1) International Ministerial Conference

In July, 1997 the international ministerial conference on global information network was held in Bonn. International Organization and information Technology industries came together for the protection of Net users and to evolve standard of functioning system and self-regulation.

2) Justice and Home Affair council

The Justice and Home Affair Council also came forward to establish practical cooperation between the countries worldwide at the investigative and procedural stage. For this end G-8 senior level group on the transnational organized crime was investigating mechanism to determine identity and prosecute cyber terrorism.

3) The News Conference of G-8 Countries

In the year 1998, in march to prevent and control the high tech crime G-7 had taken initiatives and United Kingdom came toward to combat cyber-crime.

4) European Committee on Crime Problems.

5) United States initiatives to prevent and control cyber terrorism.

6) United Kingdom initiatives to fight Cyber Terrorism (2000).

Conclusion:

Better education, health, food etc. are our basic needs, with these internet and computer also become today's needs, either students or businessmen, politician even a common man could not escape from internet, at the one side we are marching ahead with Sustainable Development Goals, & focusing on digital education and digitalization, at other end cyber space becoming place for crime like fraud, hacking, cyber terrorism. No doubt Globalization brings the world close to each other and creates opportunities, it brought many challenges. Cyber-crime is one of the challenges which need attention from the world community. Without paying attention and action we can't reach to the development goals. This paper makes a small effort to bring attention towards cyber world & cyber-crime.

References:

1. Amita Verma, Cyber Crime and Law, CLA, 65, Ed., 2010.
2. D. Bainbridge, Introduction to Computer Law, 4th Ed., 2000.
3. D.P. Mittal, Laws of Information Technology, 230, Ed., 2000.
4. Dr. M. Dasgupta, Cyber Crime in India, Eastern Book Company, 135, Ed. 2009.
5. Dr. M. Dasgupta, Cyber Crime in India - A Comparative Study, 2009, Eastern law House, p. 101.
6. H.S. Gaur, Penal Law of India, Law Publisher, 2305, Ed., 2008.
7. Jaswal , Vikram Singh and shweta thakur ,Cyber crime and Information technology act , 2000, Regal Publications , New Delhi , 2014 p. 3.
8. Jaswal , Vikram Singh and shweta thakur ,Cyber crime and Information technology act , 2000, Regal Publications , New Delhi , 2014 p. 27,28.
9. Justice Yatindra Singh , Cyber Law, Universal Law Publishing , 183, Ed., 2010.According to statistics provided in 1997there were 12 million total users, in 1998 the number went up to 85 million and it is projected that by the turn of millennium the number of net users would have crossed 900 millions.
10. M. Das Gupta, Cyber Crime in India, Eastern law House, 188, Ed., 2009.
11. Rahul Mthan, the Law Relating to Computers and Internet, 238, Ed., 2000.
12. Rodney, D., Ryder Guide to Cyber Law, Wadhwa Maypur, 524, Ed., 2001.
13. R.A. Nelson's, Indian Penal Code, Lexis Nexis Butter Worths, 2504, Ed., 2003.
14. S.K. Verma, Raman Mittal, Legal Dimensions of Cyberspace, 233, Ed., 2004.