EMERGENCE OF CYBER LAW

Chitrarekha Bharadwaj[1] and Tanvi Pandey[2]

Abstract

Cyber Law is a term that refers to all the legal and with its regulatory portion of Internet and World Wide Web. All the features of legal issues concerning to any activity of Nitizens and others in Cyberspace come within the ambit of Cyber Law. Nitizens are the people who uses internet and utilize the networks from their home or workplace. Cybercrimes are recent and new specialized domain in which the communication medium is via online which is utilized with higher specification in identifying cyber criminals using cyber laws. Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. This research paper aims to discuss the following aspects of Cybercrimes: its definition, why they occur, laws governing them; in India, methods of committing those crimes, who they affect and cybercrime prevention and procedures. The report will show the usage and progression of technology has amplified different types of crimes such as theft crimes.

[1] Student, Banasthali Vidyapith
[2] Student, Banasthali Vidyapith

Introduction

Residing in this modern era and in order to keep ourselves updated, we are very much prone to the technology around us. From dusk till dawn, people around us are aware when we commence our day and when do we end it. Dealing with our day-to-day lives, we also ought to deal with the threats complying by the technology. As a part of 21st century, we have to deal with the new upgraded challenge i.e. to keep our personal information more private.

Over the past twenty years, unscrupulous computer users have continued to use the computer to commit crime; this has greatly fascinated people and evoked the mixed feeling of admiration and fear. This phenomenon has been sophisticated and unprecedented increase recently and has called for quick response in providing laws that would protect the cyberspace[3] and its users. The level of sophistication has gone high to the point of using the system to commit the murder and other havoc. The first recorded cyber murder committed in the US seven years ago according to the Indian Express, January 2002 "has to do with the underworld don in hospital to undergo a minor surgery. His rival goon hired a computer expert who alerted his prescriptions through hacking the hospital's computer system. He was administered the alerted prescription by an innocent nurse, this resulted in the death of the patient". According to Norton, "over the last 18 months, an ominous change has swept across the internet. The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers is now ruled by a new breed of cybercriminals. Cybercrime is motivated by fraud, typified by the bogus emails sent by "phishers"[4] that aim to steal personal information".

[3]The national environment in which communication over computer networks occurs.
[4]A person who attempts to trick someone by phishing (is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication).

CC BY-NC 4.0

Cyber-crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave opens and refrigerator to nuclear power plants in being run on computers, cybercrime has assumed rather sinister implications. When seclusion and confidential information is lost or intervened by unlawfully individuals, it gives way to eminent and distinguished crimes such as hacking[5], cyber terrorism, espionage[6], financial theft, copyright infringement, spamming[7], cyber warfare[8] and many more crimes which occur across borders.Cybercrimes are responsible for the downfall of the many companies and success in the assets of criminals. Cybercrimes can happen to anyone once their information is breach by an unlawful user.

This work seeks to define the concept of cyber-crime, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

Defining the problem

The offences which take place on or using the medium of Internet are known as Cyber-crimes. These include a plethora of legal activities. The term 'cyber-crime' is an umbrella term under which many illegal activities may be grouped together. Because of the anonymous nature of the Internet, there are many disturbing activities occurring in the cyberspace which may enable the perpetrators to indulge in various types of criminal activities which are called cyber-crimes. The weapon with which cyber-crimes are committed is technology and therefore, the perpetrators of these crimes are mostly technically skilled person who have a thorough understanding of the Internet and computer applications.

As regards exact definition of cyber-crime, it has not been statutorily defined in any statute or law ass yet. Even the Information Technology Act, 2000 does not contain the definition of cyber-crime. However, cybercrimes may precisely be said to be those species of crime in which

[5]A person who uses computer to gain unauthorized access to data.
[6]The practice of spying or using spies to obtain information about the plans and activities.
[7]Spamming is the use of messaging systems to send an unsolicited message (spam), especially advertising. As well as sending messages repeatedly on the same site.
[8]The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information system for strategic or military purposes.

CC BY-NC 4.0

computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime.

Some of the other definitions are defined below:

- ***Bukisa*** defines it as "It is this access to the technical specifications of how the Internet and Internet technologies are implemented that allows an attacker to subvert systems, networks and the Internet for their own ends."
- ***Director of computer crime research center*** "cybercrime is an illegal behavior directed by the means of electronic operations that targets the security of computer system and the data processed by them".

Laws of Cyber Crime

In this part of the paper we will discuss about the pronouncement and proclamation that administers cybercrime within the India and outside the India. This section will throw the light on some rules and regulations and let people know some of the laws that are out there to secure them and some of the amendments to these laws to keep checkthe different improvement in technology.

In India

Prior to the enactment of the Information Technology Act[9], 2000, there was no separate and independent cyber law in India and all the crimes were tried under the Indian Penal Code, 1860. Subsequent to this, government has passed many other legislation to shield the people from such crimes. The Parliament of India has passed its first Cyber law, the Information Technology Act, 2000 which provides the legal infrastructure for E-commerce[10] in India.

The object of The Information Technology Act, 2000 as defined therein is as under:-

[9]The Information Technology Act, 2000 received the accent of the President of India on June 9, 2000 and came into force w.e.f. October 17, 2000 it consists of 94 sections in 13 chapters and four schedules.
[10]Commercial transactions conducted electronically on the internet.

CC BY-NC 4.0

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

When we will read the statement of objects of the Act, it would disclose us that the Information Technology Act was primarily instituted to accelerate and assist E-commerce, which had attained momentum due to the changeover from traditional paper-based methods of information communication system to that of computer networks. The Preamble of the Act sought to-

- Provide legal recognition for E-commerce;
- Facilitate E-filing of documents with government agencies;
- Amend the India Penal Code,1860, Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891 and The Reserve Bank of India Act, 1934; and
- Ensure efficient delivery of government services by means reliable electronic records.

The Act thus provides for a legal framework so that the legal sanctity is accorded to all the electronic records and other activities carried out by electronic means.

The working of the Act in subsequent years brought to light certain lacunae and shortcomings inherent therein which obstructed its smooth operation and therefore, it was amended in 2002 and again proposed to be amended by the Information Technology (Amendment) Bill, 2006 which was cleared by the Parliament on December 24, 2008 and received the assent of the President of India on February 5, 2009 to be enforced as the Information Technology (Amendment) Act, 2008 (Act no. 10 of 2009). The amendment act seeks to plug the loopholes in the existing information technology law so as to make it more effective.

Looking from an overall perspective, the Information Technology Act, 2000 is commendable effort by the Government to create the necessary legal infrastructure for furtherance and growth of electronic commerce. As on date, the judiciary in India is disinclined to accept electronic records and communications as evidence. Even email has not been defined in the existing

CC BY-NC 4.0

statutes of India and is not an accepted legal form of communication as evidence in a court of law as of today.

Causes of Cybercrimes and method of committing

Professor H.L.A. Hart in his classic work entitled 'The Concept of Law' has stated that human beings are vulnerable to unlawful acts which are crimes and therefore, rules of law are required to protect them against such acts. Despite the high-tech devices this technology can easily be used to exploit a person or his computer by illegal or unauthorized access. In the absence of any foolproof mechanism to protect and safeguard innocent computer users against cyber criminality, the cyber criminals indulge in criminal activities through networks unabated without any fear of being apprehended and tried for the offence committed by them. The reasons for these crimes are stated below:

1. **Huge data storage capacity –**the computer carries the unique feature of capacity to store huge data in small space. A small chip can store lakhs of pages in a CD ROM. Any data stored in ROM[11] will remain intact even when the power is off. The data stored therein is non-volatile and will remain in it unless it is intentionally erased or overwritten.
2. **Wider access to information –**being an electronic device the computer carries out its function with the help of complex technologies rather than manual actions. The greatest advantage of networking in the computer age is wider access to information resources over a large and extensive medium.

   A new environment of e-mails, chats, downloads etc. has been created and everyone is just a mouse clicking from another. Wider access to information creates some problems like protecting any computer system against unauthorized access where there is a possibility of breach, not due to human error, but because of the complex technological manipulations.
3. **Complexity of computer system –** the computers work on operating systems which are composed of millions of codes. Human mind is fallible and it is possible that there might be a lapse at many stages. The cyber criminals take undue advantage of these lapses and

[11]ROM is the permanent part of a computer's memory. The information stored there can be read but not changed. ROM is an abbreviation for 'read-only memory'.

CC BY-NC 4.0

lacunae and penetrate into the computer system. Such criminals are called hackers who exploit the weaknesses in existing operating system and security devices.

4. **Negligence of network users –** human conduct is synonym of negligence. It is therefore; quite predictable that while safeguarding the computer system there might be any negligence on the part of the user which may provide an opportunity for the criminal to gain unauthorized access over the network. People regularly indulge in operations of computer software and allow the access, control and security measures to take a back seat, thus giving a chance to cyber criminals to intrude and steal, alter or erase substantial data.
5. **Non-availability or loss of evidence–**all the traditional method for handling computer software has now been replaced by the digital computer processing and network technology. The main issue before the law enforcement agencies is how to preserve evidence. Unlike the traditional offences, it is very difficult to collect evidence of cybercrime which could establish the guilt of cyber accused beyond doubt. Not having sufficient evidence marks encourages the criminal to indulge more in criminal activities, and even if some evidence is left it is hardly sufficient to held the criminal guilty of the crime.

Modes used for committing cybercrimes:-

- Super zapping[12]
- Data diddling[13]
- Packet sniffing[14]
- Tempest attack[15]
- Password cracking[16]
- Buffer overflow[17]

[12]Using software that bypasses normal security constraints to allow unauthorized access to data.
[13]It is unauthorized altering data before or during entry onto a computer system, and then changing it back after processing is done.
[14]Packet sniffing allows the individual to capture data as it is transmitted over a network.
[15]Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct data. This attack can be thwarted by properly shielding computer equipment & network cabling so that they do not emit these signals.
[16]In computer system, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system.

CC BY-NC 4.0

- Salami attacks[18]
- Spyware installations[19]
- Encryptions[20]

Preventive Strategies

Despite penal provisions and preventive measures provided in the Indian Penal Code and IT Act, a perusal of cybercrime statistics of proceeding years clearly indicates that there has been no decline in crime rate and on the contrary, they are recording a steady rising trend . There are many new cybercrimes emerging which need improvised investigative and legal techniques and skills to handle them efficiently.

Presently, in most cases the investigation ends up with the conclusion that victim's computer system was attacked and there was sufficient evidence to show that substantial damage has been caused to his computer system due to such intrusion attack, but the exact source of attack could not be located or traced. Therefore, recourse to intrusion management process which seeks to plug the security loopholes may be found to be very useful as a measure of e-security[21].

The main intrusion protection devices that may be used for e-security can be placed into four major categories, namely, (i) Antivirus software, (ii) Fire walls, (iii) Authentication and (iv) Encryption.

I. Antivirus Software – virus scanning software is installed at all points of attack. All diskettes must be scanned before being loaded on to network and attack servers.
II. Firewalls – Firewall is a software which provides a layer of isolation between the inside network and the outside network. Firewall technology has now been certified by the National Computer Security Association (NCSA).

[17]In Information security and programming, a butter overflow, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.
[18]An attack is made on the computer system or network where a cybercriminal successfully transfers a small amount of money from the victims file or bank account to his account.
[19]The definition of spyware is a software program that secretly gathers personal information and sends it without the user's knowledge from a computer when it is online.
[20]The process of converting information or data into a code.
[21]Another term for cyber security. Cyber security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed exploitation.

CC BY-NC 4.0

III. Authentication – Implies password protection so that only properly authenticated users are able to access the particular network resource. Bio-metric authentication device is also used for the purpose wherein attributes arising from a person's retinal patterns, voice recognition etc. are derives from electronic analysis which helps the user to make sure whether the transmitted data is genuine or unauthorized.

IV. Encryption – Involves changing of data into an indecipherable form prior to transmission. Thus even if transmitted, it cannot be interpreted. The changed unmeaningful data is called cipher text. Encryption must be accompanied by decryption or changing the unreadable text back into its original form.

Suggestions

In view of the expanding dimensions of computer related crimes, there is need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. The process of crime prevention essentially requires co-operation and active support of citizens, institutions, industries and the government alike. Therefore, a sound strategy for prevention of cybercrimes necessitates mobilization of community participation in combating this menace. Regulatory control through effective laws is a quality measure of cybercrime prevention. Some other suggestions to prevent and reduce the incidence of cybercrimes at domestic levels are as follows:-

- Net security be tightened up
- Use of encryption technology
- False e-mail identify registration be treated as an offence
- Self-regulation by computer and net users
- Liberalization of law relating to search and seizure
- Need for universalisation of cyber law
- Need for cybercrime reporter or cyber law journal
- Special cybercrime investigation cell for high-tech crimes
- Need for a universal legal regulatory mechanism
- Need to establish a computer crime R&D center

CC BY-NC 4.0

Conclusion

Commenting on the information technology revolution which has transformed the world into a global community. Walter B Wriston observed, "Technology has made us a 'global community' in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long".

The foregoing analysis clearly indicates that cybercrimes are such harmful activities in the cyberspace which may cause damage to a person, property or even the state or society as a whole. There are many cybercrimes which are been committed by offenders all over the world using computer technology. Being radically different from conventional crimes, the law enforcement agencies find it difficult to tackle cybercrimes with the existing infrastructural mechanism because of lack of adequate knowledge about the computer operating system. This is main reason why this relatively new variety of crime is posing a challenge to the legal regime. The problem has been further aggravated by the introduction of internet.

It hardly needs to be stated that science and technology has extended its tentacles cutting across the national frontiers whereas the law still struggling to define and redefine the boundaries for the control of cybercrimes. Following a similar course, cyber law particularly, the Information Technology Act is engaged in prevention and control of cybercrimes within the country's territorial jurisdiction overlooking the fact that cyber criminality is a global phenomenon which has no territorial limits.

The countries which have updated their cyber law to suit the needs on developing computer technology are notably, United States, Canada, Australia, Japan, India, Germany and other European countries. Though United States was the first country to adopt a comprehensive law on cyber crime but it was found to be insufficient to cope with all incidents of cyber space crime and therefore, new legislation has to be introduced to cater the requirements of the rapidly developing information technology and the resulting new criminal activities.

CC BY-NC 4.0

An overall global view of cyber law indicated that many countries do have their national legislation for combating cyber criminality , but they radically differ from each other as a result of which, a particular cyber space activity which is considered as a criminal offence in one country may not be necessarily so in another country.

It is almost impossible to reduce cybercrime from the cyber-space. Looking back on the many different acts passed, history can be witness that no legislation has thrived in total elimination of cybercrime from the world. The only possible step is to make people aware of their rights and duties and further making more punishable laws which is more stringent to check them.

CC BY-NC 4.0

References

- Paranjape, Vishwanath; Cyber Crimes and Law; Central Law Academy; 2010
- KamathNandan; Law relating to Computers Internet and E-Commerce; Universal Law Publishing; 2017
- Sharma,Vakul; Information Technology; Universal Law Publishing; 2017
- Chatterjee, Ishita; Law on Information Technology; Central Law Publications; 2014
- www.bukisa.com/articles/206_internet-security-concepts
- www.techopedia.com
- www.computerhope.com
- www.cyberlawsindia.net
- www.legalservicesindia.com
- https://economictimes.indiatimes.com
- www.cyberlawclinic.net

CC BY-NC 4.0