Cyber Crimes

Madan kumar

LLB/LLM Kurukshetra university kurukshetra

Abstract: **The 21st century, communication, organizational functioning and scientific and industrial progress and technological innovations have paved the way for us to experience new and wonderful convenieness. Recent and anticipated changes in technology arising from the convergence of communications and computing are truly breathtaking, and have already had a significant impact on many aspects of life's Banking, stock exchanges, air traffic control, telephones, electric Power, and a wide range of institutions of health, welfare, and education are Largely dependent on information technology and telecommunications for their operation. While computer technology has opened doors to enhanced conveniences for may, this same technology has also opened new doors for criminals.**

Keywords: **Cyber Crimes, Impacts, Society**

I. INTRODUCTION

Businesses that have grown to rely upon computerization to collect and assemble sensitive information on the critical resources now face the daunting, and costly, task of protecting this information from those who would seek illegal access to it or infringe Intellectual Property Rights. Due to the extraordinary impact of the internet, a computer crime scene can now span from the geographical point of the victimization *e.g.* the victim's personal computer) to any other point on the planet, further complicating criminal investigative efforts. In effect, computer technology has dramatically altered the criminal justice terrain such that enterprising and opportunistic criminals nave Consciously turned to the computer to commit their illegal acts in situations in which the computer serves as the instrument of the crime, the means by which the crime IS Committed, as well as in cases in which the victim's computer, or computer system, is the target, or objective, of the Act. (The presence of new Computer technology aids cyber criminal in situations in which the computer's role is incidental to the crime; situations in which the computer is used to house and protect information that is evidence tying the offender to criminal acts, Crimes such as organized crimes, software, video, audio piracy are also being used in co-cordinating and winding their activities even beyond national borders. Information and communications technologies (ICTs) have drastically, increased the porosity between national boeders.3 .he increased porosity and anonymity of the internet super impose in a complex interaction that enables criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage of expand their operations globally .

II. DEFINING CYBER SECURITY, CYBER SPACE AND CYBER CRIME

Section 2 (nb) of the Information Technology Act 2000, defines "Cyber Security" as protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. The word cyber space was first coined by William Gibson, in his science fiction novel "Necromancer" published in 1984. Today the term cyber space became a platform to perform different human activities which congregate on the internet. However the term cyber crime has not been defined by any of the Act but it can be understood as Crimes which are committed on cyber space via techno expert mainly through the mode of Internet.

III. TYPES OF CYBER CRIMES

In today's era of digitalization and internet, a variety of Internet based Crime would happen in one way or other on daily basis and it is very difficult to ascertain such crime as everybody is not a techno expert nor having adequate knowledge of cyber space. As a result of which we are in one way or the other are victim of Cyber Crimes such as:-

(1) ***Cyber Stalking*** - Stalking is defined *as* a course of conduct directed at a specific person that involves repeated visual or physical proximity non consensual communication or verbal, written or implied threats or a combination thereof that would cause a reasonable person fear. Computer systems and information and Communication technology can also be used for harassing, threatening or intrusive communications by "cyber stalking" in which persistent messages are sent to an unwilling recipient. Cyber stalking is just an extension of the physical form of stalking, the only difference being that in cyber stalking electronic mediums Like Internet are used to pursue, harass or contact another in an unsolicited fashion.

(2) ***Cyber defamation*** - implies defamation of an individual by anything, which can be read, seen or heard with the help of computers the number of people reading or visualizing the comment defaming a person might reach sigantic proportions and hence would affect be reputation of the defamed person in a much graver manner the defaming message can also be posted to

se1ective'specific groups to become a crime of defamation.

(3) ***Denial of service*** - *it* is to prevent legitimate users of a service from using that service for example attempts to flood (Jam) a network preventing legitimate network traffic, attempts to disrupt connection between two machines (computer systems) or attempts to disrupt service to Specific system a person. Section 43(f) of Information Technology Act, 2000 (IT. Act) specifically provides for penalty in case anyone is found guilty of causing denial of access.

(4) ***E-mail Spamming / bombing and Spoofing*** – *Spamming means* to crash a program to over running a fixed size buffer with excessively large input data. For example: Bombing and e-mail account with large number of messages *may* be the same or different messages. Spoofed e-mail is one which appears *to* originate from one Source but actually has been sent from another source. Section 43 of Information Technology Act.2000 specifically provides for penalty in this case.

(5) ***Privacy Infringement*** - Right to privacy is considered as fundamental right in almost all civilized world. The availability of information in the cyberspace, for anyone with capability to access, has brought up the issue of criminal infringements of privacy. Increasing use of computers and Internet, people, knowingly or unknowingly store and transmit their personal data, which may be illegally accessed by capable offenders. Under Section 72 of the Information Technology Act, 2000, where any person illegally and without consent of the person concerned discloses any electronic, book, register, correspondence, information, document or other material to which he got access under any of the provision of the Act is any rule or regulations made under is liable for breach of confidentiality and privacy.

IV. TOOLS AND TECHNIQUES OF CYBER CRIME

.today there is a plethora of electronic gadgets and tool which are available in the market specially with the techno experts as they uses shorts cuts for becoming billionaires in day by misusing their talent for criminal activities. However it is difficult to broadly provide a list of such tool and technique they use for committing cyber crimes. Few Tools and Techniques are as under:-

1. Unauthorized access : Access is defined in section 2(1)(a) of the Information Technology Act, 2000 as gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access therefore means any kind of cyber tress pass in to the privacy and data of other user without seeking his or her permission and without his knowledge. Such a tress pass would include or mainly done by cracking the password of the current user or by hacking his Computer server with the help of Internet.
2. Trojan attacks: Torjan may be understood as a sort of patching program or PC software or a application for smart phone users. Torjan may easily interlude in ones Computer when the user of such a PC access internet or he downloads any program thinking that such program will be use full for his Computer such as add on in web browser. Torjan basically crack the original authentication of a secured program and then the owner of such Trojan may easily access your entire data.
3. Virus and worm attacks: - both of these attach themselves to the user computer system files and then tress passes the whole system. These are also get installed in User Computer without his knowledge through internet. Virus and worms are so much harmful that they have potential to corrupt your entire system including your server too.
4. Web Jacking: web jacking can be understood as website hacking.

V. INDIAN LEGISLATION FOR DEALING WITH CYBER CRIMES

With the advancement in e – technology and proliferation of internet an Act 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 commerce", which involve the use of alternatives to paper-based 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. Has been enacted by the parliament of India; The Act came to be known the Information Technology Act, 2000. The object behind the enactment of the Information Technology Act was 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 commerce”. The preamble of the Act provides that the Act has to do nothing with Cyber Crimes specifically. However the Act defines various electronic terms such as asymmetric crypto system, computer network, data, digital signature etc. further it also provides punishments for unauthorise acces of data Section 43 of the Act provides that If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,

a) accesses or secures access to such computer, computer system or computer network;

b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
e) disrupts or causes disruption of any computer, computer system or computer network;
f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected

VI. CONCLUSION

According to the report of "*National Crimes Record Bureau*", Published by Ministry of Home Affairs, India in 2016, 12,317 cyber-crimes were registered under the IT Act. [1] The manual of "*Digital Evidence Investigation of Central Board of Direct Taxes*" [2] of Department of Revenue Ministry of Finance, Government of India, 2014; deals with challenges posed by investigating teams to retrieve, authenticate and store digital evidence. And provides steps for seizure of digital evidence in the following manner:-

1. Collect all the digital evidence: either the original or the cloned copies.
2. Separate out the main copy and working copies.
3. Pack all the working copies in a separate box, which would later be used in the office for analysis. For the main copies, wrap a white tape on the connecting ports of each Hard Disk Drive along with department‘s seal. The seal and the tape will ensure that no one has accessed the Hard Disk Drives.
4. Seal the main copies by putting them in a bubble bag and then in a storage box. And then again wrap the white tape around the storage box so that no-one can open the box without removing the tape, and then place a seal of the department.
5. Take signature of assesses and officer in charge, on the seal.
6. If, seizing a system or a server or any other digital evidence, then it should be wrapped with tape and sealed in such a manner that no-one can start or open the digital evidence without breaking the seal.

The manual also discloses that there are no uniform instructions at present before the department on how to access computer systems, other digital devices and retrieve digital data during a search operation and shortcomings of different practices which are being followed like -

- Taking hard copies of data and seizing the same
- Using a CD writer or USB pen drive or USP Portable Hard Drive to
- take copy of data on the original hard disk
- Seizing Hard disks or computers and taking them to office.
- Very often, copying is done with Windows utilities and without any forensic software.

One think is to be noted and to be kept in mind that legislation alone cannot do anything it's not a magic stick which will solve your all problems in a fraction of seconds. Law will play its role when it gets in to motion on the footing of provided road map. Framing legislation one by one for one thing and other is not a solution. Individual self awareness about the ongoing era and problems is much more necessary. Thought it is not possible for everyone to be a techno expert but one can take a little step of precautionary measures to prevent the misuse of Technology. Altleas one can protect him or herself from cyber threats and from unauthorized access in to their privacy by their little self awareness about how things took place. Taking little steps to protect your own privacy over the web will result in true execution of the legislative intent.

[1] NCRB "Crime in India", 417, (MHA, 2016).

[2] CBDT," Digital evidence investigation manual", DOR, 86 (MOF, GOI 2014).