Cyber Crimes under Indian IT Laws

Shashirekha Malgi*

Introduction

Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel.

The term 'cyber crime' is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counter balanced by the sanction of the state.

Cyber crime

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime". "*Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime"*[1]

Cyber crimes include hacking into a computer network, creation of viruses and forcibly taking over a computer network. Standard crimes like fraud, sabotage, pornography, copyrights piracy, etc., have been redefined to include the aspects of the Internet.[2]

A generalized definition of cyber crime may be "*unlawful acts wherein the computer is either a tool or target or both"***.** The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery,

* Assistant Professor in KLSU's Law School, Hubli.

[1] Tarun Aroara, 'The Concept of Cyber Crimes: An Introduction', Legal News & Views, Vol.22, No.6, June 2008.p.28

[2] JagrutiDekavadiyahttp://www.legalserviceindia.com/article/l323-Cyber-Crimes-& Cyber-Law.html

cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.[3]

Reasons for cyber crime

Work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

Capacity to store data in comparatively small space-

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much more easier.

Easy to access-

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

Complex-

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence-

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any

[3] Monika Bhardwaj, 'Cyber Crime', retrieved from http://EzineArticles.com/3479824

negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

Loss of evidence-

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.[4]

Cyber Criminals

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals-

Children and adolescents between the age group of 6 – 18 years –

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the *Bal Bharati* (Delhi) case was the outcome of harassment of the delinquent by his friends.

Organised hackers-

These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the *NASA* as well as the *Microsoft* sites is always under attack by the hackers.

Professional hackers / crackers –

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

Discontented employees-

This group include those people who have been either sacked by their employer or aredissatisfied

[4] Dr. Sub hash Chandra Gupta, 'Information technology Act, 2000 and its Drawbacks', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad

with their employer. To avenge they normally hack the system of their employee.[5]

Different kinds of Cyber Crimes

- Financial Crimes : Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc[6].

- Cyber Pornography**:** Cyber pornography covers pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc)[7].

- Attacks By Hackers : Hacker is computer expert who uses his knowledge to gain unauthorized access to the computer network. He's not any person who intends to break through the system but also includes one who has no intent to damage the system but intends to learn more by using one's computer. Information Technology Act 2000 doesn't make hacking per se an offence but looks into factor of mens rea. Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider or an employee is quite prominent in present date. Section 66 (b) of the Information Technology Act 2000, provides punishment of imprisonment for the term of 3 years and fine which may extent to two lakhs rupees, or with both[8].

- Online Gambling : There are thousands of websites that offer online gambling. The special issue with online gambling is that it is legalized in several countries. So legally the owners of these websites are safe in their home countries[9].

- Intellectual Property Crimes**:** These include software piracy, copyright infringement, trademarks

[5] B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.

[6] Justice S.B. Sinha, 'Cyber Crime in the Information Age', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.p20

[7] Jonathan clough, "Principles of Cybercrime",2010,University Press,Cambdidge.p.247

[8]http://legalservicesindia.com/article/article/offences-&-penalties-under-the-it-act-2000-439-1.html

[9] Ibid

violations, theft of computer source code etc[10].

- Cyber Defamation: This occurs when defamation takes place with the help of computers and / or the Internet. e.g. Sameer publishes defamatory matter about xyz on a website or sends e-mails containing defamatory information to xyz's friends[11].

- Cyber Stalking **:** Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects[12].

- Web Jacking : Just as conventional hijacking of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom. The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom[13].

- Email Bombing: Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing[14].

- Data Diddling :Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining,

[10] Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.p.18

[11] Barkha &u.Rama Mohan, "Cyber Law & Crimes"2009,Asia law House,Hydrabad.p.14

[12] Ibid

[13] C. Suman and Duvva Pavan Kumar, 'Data Protection - An overview', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.p.14

[14]http://www.slideshare.net/RanjanaAdhikari/cyber-crime-9203478, visited on 26/4/2012.

checking, converting, or transmitting data[15].

- Salami Attacks : These attacks are used for committing financial crimes. For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month[16].

- Denial of Service Attack : Denial of Service attacks (DOS attacks) involve flooding a computer or a server with more requests than it can handle. This causes the computer (e.g. a web server) to crash and results in authorized users being unable to access the service offered by the computer[17].

- Virus / Worm Attacks : Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk.[18]

- Cyber Terrorism:Cyber terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large- scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses." Section 66F of the Information Technology Act- 2000 provides punishment for cyber terrorism and it also defines terrorism.Section 66F mainly highlights 'denial of service', 'unauthorized access to a computer resource' with intent to threat the unity, integrity, security or sovereignty of India.It also provides for punishment which may extend to "*Life Imprisonment*"[19]

[15] http://www.articlesbase.com/cyber-law-articles/cyber-crimes-539363.html ,visited on 51/4/2012.

[16] Ibid

[17] http://astrealegal.com/cyber-laws, visited on 2/5/2012.

[18], http://www.legalindia.in/cyber-crimes-and-the-law , visited on 2/5/2012.

[19] http://cyberlawsinindia.blogspot.in/2009/05/cyber-terrorism-in-india.html

Indian IT laws

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This had led to tremendous development and progress which has been a launching pad for further development. Of all the significant advances made by mankind from the beginning till date, probably the most important is the development of Internet. When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all-pervading revolution which could be misused for criminal activities and which required regulation .Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage in a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for cyber laws. Also our existing laws have deficiencies in dealing with crimes in cyberspace.[20]

In view of the above background and with the fast advancement in Information Technology, there are new ways of crime in cyber space, for which there are no national boundaries. Also, there are no proper provisions in our existing legal system to help the judiciary for arresting such crimes. In India, the first major and significant steps toward control of cyber crimes has been initiated through the enactment of Information Technology Act,2000.

Importance of Cyber Laws

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and cyberspace. Initially, it may seem that cyber law is a very technical field and that it does not have any bearing to most activities in cyberspace. But nothing could be further than the truth .Whether we

[20] Kamlesh N.Agarwal ,murli D.Tiwari, “IT and Indian Legal System”[New Delhi:Published by Rajiv Beri for Macmillan India Ltd.] p.172

realize it or not, every reaction in cyberspace has some legal and cyber legal perspectives.[21]

Statutory Provisions for cyber crimes under Indian IT Law

The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th May 2000.the preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934**.** *The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000.* So that they may regulate and control the affairs of the cyber world in an effective manner. **[22]**

The Information Technology Act deals with the various cyber crimes in chapters IX & XI. The important sections are Ss. 43,65,66,67.

- Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Crore by way of remedy.
- Section 65 deals with '*tampering with computer source documents*' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.
- Section 66 deals with '*hacking with computer system'* and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.
- Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.
- Section .68 not complying with directions of controller.
- Section 70attempting or securing access to computer.

[21].Ibid.p.173

[22] http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf, visited on 1/4/2012.

- Section 72, For breaking confidentiality of the information of computer .section 72 of Information
- Technology Act, 2000 provides punishment for an unauthorised access or, disclosure of that information to third person punishable with an imprisonment up to 2 years or fine which may extend to 1 lakh rupees or with both. English courts have also dealt with an issue as to what activities would constitute crime under existing legislation, in the case of *R. v. Fellows and Arnold* it was held that the legislation before the 1994 amendment would also enable computer data to be considered a 'copy of an indecent photograph' and making images available for downloading from the website would constitute material being 'distributed or shown'. Statute is wide enough to deal with the use of computer technology.
- Sec.73 Publishing false digital signatures, false in certain particulars. Fine of 1 lakh, or imprisonment of 2 years or both.[23]

Criticism

"The IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime". The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T.Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T.Act 2000 read with the Penal Code is capable of dealing with these felonies.

Conclusion

No one can deny the positive role of the cyber space in today's world either it be political, economic, or social sphere of life. But everything has its pro's and corns, cyber terrorists have taken over the technology to their advantage. To curb their activities, the Information Technology Act 2000 came into existence which is based on UNICITRAL model of Law on e-commerce. It has many advantages as it gave legal recognition to

[23] "Anusuya Sadhu", "The Menace of Cyber Crime", can be viewed at http://www.legalserviceindia.com/articles/article+2302682a.htm

electronic records, transactions, authentication and certification of digital signatures, prevention of computer crimes etc. but at the same time is inflicted with various drawbacks also like it doesn't refer to the protection of Intellectual Property rights, domain name, cyber squatting etc. This inhibits the corporate bodies to invest in the Information technology infrastructure. Cases like Dawood and Quattrochi clearly reveals the problem of enforceability machinery in India. Cryptography is new phenomenon to secure sensitive information. There are very few companies in present date which have this technology. Other millions of them are still posed to the risk of cyber crimes.

It's like 'eye for an eye' kind of situation where the technology can be curbed only by an understanding of the technology taken over by cyber terrorists. Even if the technology is made better enough to curb the computer related crime there is no guarantee if that would stay out of reach of cyber terrorists. Therefore Nations need to update the Law whether by amendments or by adopting sui generic system. Though Judiciary continues to comprehend the nature of computer related crimes there is a strong need to have better law enforcement mechanism to make the system workable.

Suggestions:

Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyber crime.
- There is an urgent need for unification of internet laws to reduce the confusion in their application. For e.g. for publication of harmful contents or such sites, we have Indian Penal Code (IPC), Obscenity Law, Communication Decency law, self regulation, Information Technology Act 2000 ,Data Protection Act, Indian Penal Code, Criminal Procedure Code etc but as they deal with the subject vaguely therefore lacks efficient enforceability mechanism. Due to numerous Laws dealing with the subject there is confusion as to their applicability, and none of the Laws deal with the subject specifically in toto. To end this

confusion in applicability of Legislation, picking from variousLlaws to tackle the problem, unification of laws by taking all the internet laws to arrive at Code which is efficient enough to deal with all the problems related to internet crimes.

- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Harsher laws are required at the alarming situation to deal with criminals posing threat to security of funds, information, destruction of computer systems etc. Data protection, by promotion of general principles of good information practice with an independent supervisory regime, would enable the law to maintain sufficient flexibility. To achieve an appropriate balance between the need to protect the rights of the individuals and to have a control over the way their personal information have been used would be helpful in this increasingly networked economy. Just having two provisions in the Information Technology Act, 2000 for protection of data without any proper mechanism to tackle the crime makes their mention in the Act redundant.
- Information Technology Act is applicable to all the persons irrespective of their nationalities (i.e. to non-citizens also) who commit offence under the Information Technology Act outside India, provided the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Section 1 and Section 75 of the Information Technology Act. But this provision lacks practical value until and unless the person can be extradited to India. Therefore, it is advised that we should have Extradition treaties among countries, to make such provisions workable.