International Journal of Multidisciplinary Allied Research Review and Practices
www.ijmarrp.com (Volume 3, Issue 2, February 2016) ISSN: 2455 -1570
IJMARRP

STUDY OF CRIMES AND THE INTERNET

Asst.Prof. Vikram Vitthal Irale*

Dr. Vijay Pal Singh**

Yashwantrao Chavan Law College, Karad

Sun Shine College Mandrella, Rajasthan

Abstract: ***Society as on today is happening more and more dependent upon technology and crime those are based on electronic offences are bound to increase. Endeavour of law making machinery of the country should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Cyber crimes are a new class of crimes which are increasing due to extensive use of internet. The different types of Internet crime vary in their design and how easily they are able to be committed. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The Information Technology Act specifies the acts which have been made punishable as cyber crime . The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes. Still cyber crimes are increasing day by day.***

CRIMES AND THE INTERNET

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly “cyberspace”, i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including

intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

In Simple way we can say that digital wrongdoing is unlawful acts wherein the PC is either an instrument or an objective or both. Digital law violations can include criminal exercises that are conventional in nature, for example, burglary, misrepresentation, phony, criticism and devilishness, all of which are liable to the Indian Penal Code. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The quantity of clients and their assorted qualities in their cosmetics has presented the Internet to everybody. A few culprits in the Internet have grown up comprehension this superhighway of data, not at all like the more seasoned era of clients

. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

But under Indian law "Cybercrime" as such has not been defined under any legislation. One legislation that deals with the offences related to such crimes in India is **Information Technology Act, 2000,** which was also further amended in the form of **IT Amendment Act, 2008.** But these two important legislations also do not include any **definition** for **cyber crime**

Maharashtra has developed as the focal point of digital wrongdoing with most extreme number of rate of enlisted cases under digital unlawful acts. Hacking with PC frameworks and revolting distribution are the primary cases under IT Act for digital law violations. Most extreme guilty parties captured for digital unlawful acts were in the age aggregate 18-30 years. 563 individuals in the age amass 18-30 years were captured in the year 2010 which had expanded to 883 in the year 2011.

Cyber Crime is not defined in Information Technology Act 2000 or in the Information Technology (Amendment) Act, 2008 or in any other legislation in India. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime.[i]

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The misuse of PCs has likewise brought forth an array of new age wrongdoings that are tended to by the Information Technology Act, 2000.[ii]

We can categorize Cyber crimes in two ways

The Computer as a Target:-using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon:-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

What is the importance of Cyber law?

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 laws are a very technical field and that it does not have any bearing to most activities The misuse of PCs has additionally brought forth an extent of new age criminal acts that are tended to by the Information Technology Act, 20in Cyberspace. In any case, the genuine truth is that nothing could be more remote than reality. Whether we understand it or not, every activity and each response in Cyberspace has some legitimate and Cyber lawful points of view.

Types of Cyber crime:

Crime denotes an unlawful act which is harmful to society at large and which is punishable by a state.The different types of Internet crime vary in their design and how easily they are able to be committed.

1. **Unauthorized access & Hacking:-**

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They have the longing to destruct and they get the kick out of such pulverization. A few programmers hack for individual fiscal increases, for example, to taking the Visa data, exchanging cash from different financial balances to their own record took after by withdrawal of cash. By hacking web server taking control on someone else's site called as web hijacking[iii]

2. **Virus, Worm and Trojan attack:**

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Viruses can do any amount of damage; the creator intends them to do. They can send your data to a third party or they can delete your data from your computer.

Programs that duplicate like infections yet spread from PC to PC are called as worms. The system that demonstrations like something valuable, yet do the things that are peaceful risky; the projects of this kind are called as Trojans.[iv]

3. **E-Mail Spoofing , E-Mail spamming, Email phishing and Email bombing:**

Email Spoofing- sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else (May through SMS)

Email spamming- refers to sending email to thousands and thousands of users - similar to a chain letter

Email Phishing- is a system in which the culprit conveys authentic looking email trying to accumulate individual and money related data from beneficiaries

Email bombing- sending tremendous volumes of email to a location trying to flood the post box.[v]

4. **Identity Theft:**

Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.

5. **Publishing or transmitting obscene material in electronic form:**

   The strict importance of the expression "Erotic entertainment" is depicting or demonstrating sexual acts keeping in mind the end goal to bring about sexual energy. Obscene sites; explicit material delivered utilizing PCs and utilization of web to download and transmit explicit features, pictures, photographs, works and so forth is considered as digital wrongdoing. 420 million individual explicit WebPages arrive in the internet today.

6. **Preservation and Retention of Obscene material:**

   Preservation of videos, pictures, photos, writings in to Personal Computers, Mobile phones, Lap-tops, Albums etc. is a cyber crime.

   Side Effects:

   -Adultery, prostitution and unreal expectations

   -Marriage and children becomes main obstacles

   -Pornography Addiction etc.

7. **Cyber Terrorism:**

   Targeted attacks- on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. e.g. Mumbai, 20 September 2007- Official website of Maharashtra government hacked.[vi]

8. **Sending threatening messages :**

   Sending Messages through Emails, SMS and through any other medium for Extortion or Black mailing is considered as cyber crime.

9. **Word, gesture or act intended to insult the modesty of a woman:**

   IPC Section 354: 354. Assault or criminal force to woman with intent to outrage her modesty.. Sexual harassment and Voyeurism- (Any man who watches, or captures the image of a woman engaging in a private act), or Stalking is considered as cyber crime.

10. **Cyber Stalking:**

Following a woman or men and contacts, or attempts to contact such woman or men to get personal interaction repeatedly despite a clear indication of disinterest by such woman or men and also constantly bombarding the victim with emails, Messages, Phone calls etc is called as cyber stalking.

11. **Sale of illegal articles:**

This includes trade of narcotics, weapons, wildlife and porn films etc through the medium of internet.

12. **Cyber Forgery:**

This includes- Counterfeit of currency notes, Postage and revenue stamps, Passport, Mark sheets, Certificates, Check -books etc

13. **Flooding a computer resource:**

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users and Authorized users became the Victim.

14. **Data Theft, Piracy & IPR Violations:**

Theft or piracy of Movies & songs, Software's, Central Data Base of Organization, Personal information, intellectual work etc also comes under the purview of cyber crime.

15. **Defamation:**

Defamation can be understood as the intentional infringement of another person's right to his good name. E.g.- someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends; Information posted to a bulletin board can be accessed by anyone is considered as defamation.

16. **Virus Dissemination:**

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious.[vii]

17. **Network Packet Sniffers:**

Network computers communicate serially where large information pieces are broken into smaller ones. The information stream would be broken into smaller pieces even if networks

communicated in parallel. These littler pieces are called system bundles. Since these system parcels are not scrambled they can be handled and comprehended by any application that can pick them off the system and procedure them. A system convention indicates how parcels are recognized and marked which empowers a PC to figure out if a bundle is planned for it. The specifications for network protocols such as TCP/IP are widely published. A third party can easily interpret the network packets and develop a packet sniffer. A bundle sniffer is a product application that uses a system connector card in an indiscriminate mode (a mode in which the system connector card sends all parcels got by the physical system wire to an application for handling) to catch all system bundles that are sent over a nearby system. A packet sniffer can provide its users with meaningful and often sensitive information such as user account names and passwords.[viii]

Offences Under major Act[ix]:

1. Tampering with computer source Documents -Sec.65
2. Hacking with computer systems , Data Alteration -Sec.66
3. Sending offensive messages through communication service, etc -Sec.66A
4. Dishonestly receiving stolen computer resource or communication device -Sec.66B
5. Identity theft -Sec.66C
6. Cheating by personating by using computer resource -Sec.66D
7. Violation of privacy -Sec.66E
8. Cyber terrorism -Sec.66F
9. Publishing or transmitting obscene material in electronic form -Sec .67
10. Publishing or transmitting of material containing sexually explicit act, etc. in electronic Form -Sec.67A
11. Punishment for publishing or transmitting of material depicting children in sexually Explicit act, etc. in electronic form -Sec.67B
11. Preservation and Retention of information by intermediaries -Sec.67C
12. Powers to issue directions for interception or monitoring or decryption of any information Through any computer resource -Sec.69
13. Power to issue directions for blocking for public access of any information through any

Computer resource -Sec.69A

14. Power to authorize to monitor and collect traffic data or information through any Computer resource for Cyber Security -Sec.69B
15. Un-authorized access to protected system -Sec.70
16. Penalty for misrepresentation -Sec.71
17. Breach of confidentiality and privacy -Sec.72
18. Publishing False digital signature certificates -Sec.73
19. Publication for fraudulent purpose -Sec.74
29. Act to apply for offence or contraventions committed outside India -Sec.75
21. Compensation, penalties or confiscation not to interfere with other punishment -Sec.77
22. Compounding of Offences -Sec.77A
23. Offences with three years imprisonment to be cognizable -Sec.77B
24. Exemption from liability of intermediary in certain cases -Sec.79
25. Punishment for abetment of offences -Sec.84B
26. Punishment for attempt to commit offences -Sec.84C
27. Offences by Companies -Sec.85
28. Sending threatening messages by e-mail -Sec .503 IPC
29. Word, gesture or act intended to insult the modesty of a woman -Sec.509 IPC
30. Sending defamatory messages by e-mail -Sec .499 IPC
31. Bogus websites, Cyber Frauds -Sec .420 IPC
32. E-mail Spoofing -Sec .463 IPC
33. Making a false document -Sec.464 IPC
34. Forgery for purpose of cheating -Sec.468 IPC
35. Forgery for purpose of harming reputation -Sec.469 IPC
36. Web-Jacking -Sec .383 IPC
37. E-mail Abuse -Sec .500 IPC
38. Punishment for criminal intimidation -Sec.506 IPC
39. Criminal intimidation by an anonymous communication -Sec.507 IPC
40. When copyright infringed:- Copyright in a work shall be deemed to be Infringed -Sec.51
41. Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of -Sec.63

42. Enhanced penalty on second and subsequent convictions -Sec.63A
43. Knowing use of infringing copy of computer programme to be an offence -Sec.63B
44. Obscenity -Sec. 292 IPC
45. Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail- Sec.292A IPC
46. Sale, etc., of obscene objects to young person[x] -Sec .293 IPC
47. Obscene acts and songs -Sec.294 IPC
48. Theft of Computer Hardware -Sec. 378 IPC
49. Punishment for theft -Sec.379 IPC
50. Online Sale of Drugs[xi] -NDPS Act
51. Online Sale of Arms- Arms Act

How to file a complaint:

The complaint regarding commission of cyber crime can be made to the in-charge of the cyber crime cells which are present almost in every city[xii]. To file a complaint alleging commission of a cyber crime the following documents must be provided:

In case of hacking the following information should be provided:

- Server Logs
- Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced
- If data is compromised on your server or computer or any other network equipment, soft copy of original data and soft copy of compromised data.
- Access control mechanism details i.e.- who had what kind of the access to the compromised system
- List of suspects if the victim is having any suspicion on anyone.

In case of e-mail abuse, vulgar e-mail etc. the following information should be provided:

- Extract the extended headers of offending e-mail and bring soft copy as well hard copy of offending e-mail.
- Please do not delete the offending e-mail from your e-mail box.

- Please save the copy of offending e-mail on your computer's hard drive.

Precautions:

-Be careful while giving out personal information

-Read privacy policy information

-Monitor your bank accounts statement regularly

-Activate SMS alert

-Be careful about account Password

-Avoid strangers

CONCLUSION:

The complaint regarding commission of cyber crime can be made to the in-charge of the cyber crime cells which are present almost in every city. 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 laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. A bundle sniffer is a product application that uses a system connector card in an indiscriminate mode (a mode in which the system connector card sends all parcels got by the physical system wire to an application for preparing) to catch all system bundles that are sent over a nearby system.

Society as on today is happening more and more dependent upon technology and crime based on electronic offences are bound to increase. Endeavour of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes most reduced. Subsequently, it ought to be the steady endeavors of rulers and legislators to guarantee that representing laws of innovation contains each viewpoint and issues of digital wrongdoing and further develop in nonstop and solid way to keep consistent vigil and check over the related unlawful acts.

[i] Book on "IT" Security of IIBF Published by M/s Tax Mann Publishers

[ii] http://infosecawareness.in/cyber-laws/cyber-law-in-india/

[iii] http://www.cyberlawsindia.net/

[iv] http://www.cyberlawsindia.net/

[v] http://cybercellmumbai.gov.in/

[vi] http://www.slideshare.net/RanjanaAdhikari/cyber-crime-9203478

[vii] http://cybercellmumbai.gov.in/

[viii] http://www.legalserviceindia.com/articles/article+2302682a.htm

[ix] Information Technology Act, 2000; Indian Penal Code, 1860

[x] Indian Penal Code,1860 Section-293

[xi] The Narcotic Drugs and Psychotropic Substances Act, 1985

[xii] http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html