CYBER CRIME AND CYBER TERRORISM IN INDIA

A DISSERTATION TO BE SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS

SUBMITTED BY

MOHD. ASIM KHAN

[UNIVERSITY ROLL NO.: 1200997033]

SCHOOL OF LEGAL STUDIES

UNDER THE GUIDANCE

OF

MRS. SARITA SINGH

ASSISTANT PROFESSOR

SCHOOL OF LEGAL STUDIES

SESSION 2020-21

CERTIFICATE

This is to certify that the dissertation titled, "CYBER CRIME AND CYBER TERRORISM IN INDIA" is the work done by MOhd. Asim Khan under my guidance and supervision for the partial fulfilment of the requirement for the Degree of **Master of Laws** in School of Legal Studies Babu Banarasi Das University, Lucknow, Uttar Pradesh.

I wish his success in life.

Date ----------

Place - Lucknow

Mrs. Sarita Singh

(Assistant Professor)

DECLARATION

Title of Dissertation **CYBER CRIME AND CYBER TERRORISM IN INDIA**

I understand what plagiarism is and am aware of the University's policy in this regard.

Mohd. Asim Khan

I declare that

(a) This dissertation is submitted for assessment in partial fulfilment of the requirement for the award of degree of **Master of Laws.**

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other source has been used i.e., words, data, arguments and ideas have been appropriately acknowledged.

(c) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.

(d) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date : ……

Place- Lucknow **Mohd. Asim Khan**

UNIVERSITY ROLL No.: 1200997033

LL.M. (2020-21)

(CSL)

ACKNOWLEDGEMENT

I acknowledge the heartfelt thanks to the School of legal Studies. B.B.D. University. to give me the opportunities to complete my dissertation for the Partial Fulfillment of the Degree in Master in Laws.

I am thankful to my Supervisor Mrs. Sarita Singh Assistant Professor mam for not only helping me to choose the dissertation topic but also for his valuable suggestions. and co-operations till the completion of my dissertation. She provided me every possible opportunity. and guidance. and being a support in completing my work.

I also thank to all the respondents without whom this study would have never been completed.

I am thankful to everyone from core of my heart.

(**Mohd. Asim Khan**)
LL.M. II Semester
School of legal Studies
B.B.D. University

ABBREVIATION

AC	:~	Appeal Cases
AES	:~	Advanced Encryption Standard
AIR	:~	All India Reporter
All. ER	:~	All England Reporter
All.	:~	Allahabad
App Cases	:~	Appeal Cases
ATM	:~	Automated Tailor Machine
AVS	:~	Address verification system
B& Ad	:~	Barnwell. and Adolphus. 1830-1834 K.B
BBM	:~	Black Berry Messenger
BES	:~	Black Berry Enterprise Server
Beav.	:~	Beavens's Reports. 1838-1866
Bing.	:~	Bingham Reports. 1822-34
Bom.	:~	Bombay
BPC	:~	Best Practice Code
BPO	:~	Business process outsourcing
BRA	:~	Banking Regulation Act. 1949
B2B	:~	Business to Business
B2C	:~	Business to Customer
Cal	:~	Calcutta
CAT	:~	Cyber Appellate Tribunal
CBI	:~	Central Bureau of Investigation
CDMA	:~	Code Division Mulitple Access
Ch	:~	Chancery. Law Reports
Ch.D	:~	Chancery Division. Law Reports. 1875-1890
CIC	:~	Central data Commissioner
CJI	:~	Chief Justice of India
CMD	:~	Chief Managing Director
Co.	:~	Company

Comp.Cas.	:~	Company Cases
CP	:~	Common Pleas
CPC	:~	Civil Procedure Code. 1908
Cr. P C	:~	Criminal Procedure Code. 1973
Cr.LJ	:~	Criminal Law Journal
CVC	:~	Central Vigilance Commission
D Ds	:~	Demand Drafts
DBS	:~	Department of Banking Supervision
DCS	:~	Digital Collection System
DES	:~	Digital Encryption Standard
DIT	:~	Department of Information Technology
DNS	:~	Domain Name System
DRM	:~	Digital Rights Management
EOD	:~	Economic Offence Division
Ex.	:~	Exchequer Reports. 1847-56
Exch.	:~	Exchequer Reports. 1847-56
F Is	:~	Financial Institutions
Guj	:~	Gujrat
H&C	:~	Hurlstone & Coltman. 1862-66
HL	:~	House of Lords
I T	:~	Information Technology
Ibid.	:~	Ibedum
ICA	:~	Indian Contract Act. 1872
IPC	:~	Indian Penal Code. 1860
IRDA	:~	Insurance Regulatory. and Development Authority
J.	:~	Judge
JJ.	:~	Judges
K B	:~	Kings Bench
LR	:~	Law Reports. Exchequer.1865-75
LT	:~	Law Times Reports 1843-
Ltd.	:~	Limited

Macq.	:~	McQueen's Practice in H.L. & P.C.
Macq.	:~	McQueen's Scotch Appeals. 1852. H L
Mad.	:~	Madras
MD	:~	Managing Director
NI Act	:~	Negotiable Instruments Act. 1881
Pa	:~	Pennsylvania
PC	:~	Privy Council
PCA	:~	Prevention of Corruption Act. 1988
PIN	:~	Personal Identification Number
PSU	:~	Public Sector Undertaking
Pvt.	:~	Private
QBD	:~	Queen Bench Division
RBI	:~	Reserve Bank of India
RECLAB	:~	Report of the Expert Committee on Legal Aspects of Bank Frauds
SBI	:~	State Bank of India
SC	:~	Supreme Court
SCC	:~	Supreme Court Cases
SEBI	:~	Stock Exchange Board of India
SFF	:~	Serious Financial Frauds
SPE	:~	Special Police Establishment
TR	:~	Durnford . and East's Term Reports. 1775- 1800.
UCC	:~	Uniform Commercial Code
UK	:~	United Kingdom
UOI	:~	Union of India
URL	:~	Uniform Resource Location
USA	:~	United States of America
VOIP	:~	Voices Over Internet Protocol
VSNL	:~	Videsh Sanchar Nigam Ltd.
WAP	:~	Wireless Access Protocol
WLL	:~	Wireless in Local Loope

WPSIP	:~	Working Parties on data Securities & Privacy
WWW	:~	World Wide Web

.....

LIST OF CASES

1. *Avinash bajaj v. State of Delhi .. (2005) 116 DLT 427:~ (2005) 79 DRJ 576*
2. *Fatima riswana v. State..... SLP (Crl) No. 1606 of 2004*
3. *Karan girotra v. State..... (2011) 1 RCR (Cri) 513*
4. *Manish kathuria case..... ITAA 2008*
5. *Sanjay Kumar Vs State Of Haryana ..... (2015) 3 SCC 220*
6. *State of Chattisgarh v Prakash yadav. and others .....* 1427 of 2007
7. *State of Delhi v Aneesh chopra..... 1950 AIR 129 1950 SCR 605.*
8. *State of Maharastra v Anand Ashok khare..... (crl.) 180 of 2000*
9. *State of Tamil Nadu v Dr. L. Prakash..... (crl.) 66 of 2002..*
10. *State of UP v saket sanghania..... 1954 AIR 728 1955 SCR 707*
11. *State v amit Prasad..... (2014) 6 SCC 404*

LIST OF STATUE

1. The Information Technology Act. 2000
2. The Information Technology (Amendment)Act. 2008
3. Computer Misuse Act 1990 (Title 18. Crimes. and Criminal Procedure)
4. Cyber Regulation Appellate Tribunal (Procedure) Rules. 2000
5. IT (Certifying Authority) Regulations. 2001
6. IT (Other Standards) Rules. 2003
7. IT (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules. 2003
8. IT (Securities Procedure) Rules. 2004
9. IT (Use of Electronic Records. and Digital Signatures) Rules. 2004
6. IT (Procedure. and Safeguarads for Interception Etc.) Rules 2009
11. IT (Procedure. and Safeguarads for Blocking Etc.) Rules 2009
12. IT (Procedure. and Safeguarads for Monitoring Etc.) Rules 2009
13. IT (Reasonable Securities Practices. and Procedure etc.) Rules. 2011
14. IT (Intermediaries Guidelines) Rules. 2011
15. IT (Guidelines for Cyber Cafe) Rules. 2011
16. IT (Electronic Service Delivery) Rules. 2011
17. IT (National Critical data Infrasturucture Etc.) Rules. 2013
18. IT (The Indian Computer Emergency Response Team. and Manner of Performing Functions. and Duties) Rules. 2013
19. IT (Recognition of Foreign Certifying Authorities operating under a Regulatory Authority) Regulations. 2013
20. IT (Recognition of Foreign Certifying Authorities not operating under a Regulatory Authority) Regulations. 2013
21. Electronic Signature or Electronic Authentication Technique. and Procedure Rules. 2015.
22. Digital Signature (End Entity) Rules. 2015.

CONTENTS

COMBATING CRIME IN CYBER SPACE:~ INDIAN PERSPECTIVE

CHAPTER -01
INTRODUCTION

CHAPTER-01

INTRODUCTION

The modern thief can steal more by way of a computer than by way of a gun. Tomorrow's terrorist may be able to do more damages by way of a keyboard than by way of a bomb.[1]

The invention of the computer has opened new avenue for the fraudsters. It is an evil having its origin in the growing dependence on computer in modern life. Though there is great talk about the Cyber Crimes there is nothing called CyberCrime. The crime such as frauds. forgery are traditional. and are covered by the separate statute such as Indian Penal Code or alike. However the abuse of computer. and the related electronic media has given birth to a gamut of new type of crimes which has some peculiar features. A simple yet sturdy definition of these crimes would be "unlawful acts wherein the equipment transforming the data be it a computer or mobile is either a tool or a target or both". In India the Information Technology Act deals by way of the acts wherein the computer is tool for an unlawful act. The kind of activities usually involves a modification of a conventional crime by using computer. Some examples are financial crimes. child pornography. sale of illegals articles. online gambling. intellectual properties crimes. email spoofing. forgery. cyber defamation. cyber stalking. unauthorized access to computer

[1] National Research Council. "computer at Risk". 1991

systems or networks. email bombing. theft of data contained in electronic form. data diddling. salami attacks. worms/virus attacks etc.

The use of Computers is increasingly spreading.. and more. and more users are connecting to the internet. The internet is a source for almost anybody to access. manipulate. and destroy others information. The rapid development of the Internet. and computer technology globally has also led to the growth of new forms of transnational crimes especially those which are internet related. These criminal activities directly relate to the use of computers. specifically illegal trespass into the computer system or database of another. manipulation or theft of stored data. or sabotage of systems. and data. Characteristic feature of these crimes are that these crimes are considered as illegal. unethical or unauthorized behavior of people relating to the automatic processing. and transmission of data by the use of Computer Systems. and Networks. These crimes have virtually no boundaries. and may affect any country across the globe within a fraction of second. Ways of tackling Cyber Crimes through legislation may vary from one country to another. especially when Cyber Crimes occur within a specific national jurisdiction by way of different definition. and socio-political environment.[2]

Cybercrime spans not only state but national boundaries as well. At the Tenth United Nations Congress on the Prevention of Crime. and Treatment of Offenders. in a workshop devoted to the issues of crimes related to computer networks. cybercrime was broken into two categories. and defined thus:~

[2] Anirudh Rastogi. Cyber Laws. lexi Nexi

Firstly. cybercrime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the securities of computer systems. and the data processed by them. And. secondly cybercrime in a broader sense is any illegal behavior committed by means of. or in relation to. a computer system or network. including such crimes as illegal possession offering or distributing data by means of a computer system or network.

Cyber Crime is the latest type of crime which affects many people. It refers to the criminal activities taking place in computer or computer networks. intentionally access without permission. alters. damages. deletes. and destroys the database available on the computer or network.. and also includes access without permission on a database or programme of a computer in order to devise or execute any unlawful scheme or wrongfully control or obtain money. properties or data. It poses the biggest challenge for the Police. Prosecutors. and legislators. Crimes of this nature are usually indulged in by young teens. recreational computer programmers. and persons having vested interest. Cyber crime in its most practiced form includes offences such as tampering by way of the source code of a programme. hacking into computer systems. publication of obscene information. and misuse of licenses. and digital signatures. The problem is multifold as it covers the crime related to economy as well as other crimes such as pornography which has its basis in certain moral standards. and uses parameters like indecency. and obscenity.[3]

[3] K.K. Singh. "Information Security. and Cyber Laws"

In a day. and age where everything from a microwave oven to nuclear plants run on computer. and computer programmes. Cyber crimes has assumed a rather sinister implication. Life is about a mix of good. and evil. So is the internet. For all the good it does to us. Cyber crimes have its dark side too. Unlike conventional crimes though. there is no policeman patrolling the data superhighway. leaving it open to everything from Trojan horses. and Viruses to Cyber stalking. trademark counterfeiting. and Cyber terrorism.

Enormous amount of money is earned by the Cybercriminals. either by causing huge damage to the computer systems or by stealing data which is marketable or by way of some foul play through the network. The question here is what constitutes a computer crime[4]. and how can it be distinguished from routine crime. The query has no legal answer because in India neither the IT Act. 2000 nor the Indian Penal Code gives any precise or concise definition for the same. However some recent changes in the IPC provides punishments to certain acts without making any specific reference to computers. This create a lot of imbroglio in the minds of cyber users because of the confusion arising out of how any rule or doctrine should be made applicable in case of infringements or violations made by parties within the country. and outside. One of the critical issues in the cyber era is the matter of jurisdiction. which is the authorities of a court to hear a case. and resolve a dispute within a sovereign territory. Because the legal establishment of e-commerce has no geographical boundaries. it establishes immediate long- distance

[4] S.P. Tripathi vs. Inroduction data security. and Cyber Crime

communications by way of anyone who can access the internet. For example. an online e-merchant has no way of knowing where the data on its site is being accessed. Hence. the issue of jurisdiction is of primary importance in cyberspace. Engaging in e-commerce on the internet may expose the company to the risk of being sued in any State or foreign country. where an internet user can establish a legal claim. In consideration of all these issues under the scope of cyber-crimes subject to each country‟s jurisdiction. and their impacts on global socio-economy beyond the jurisdiction. we may need to be more aware of them. and take appropriate legislative measures to govern the cyber world before it is too late. In order to achieve this end many countries of the world including India have enacted Laws related to Information Technology. these laws have been usually termed as Cyber Laws.

Cyber law is a term used to describe the legal issues related to the use of communications technology. particularly „cyber-space‟ It is a less distinct field of law in the way that properties or contract are. as it is an inter-section of many fields. including intellectual property. privacy. freedom of expression. and jurisdiction. In essence. Cyber law is an attempt to integrate the challenges presented by human activities on the internet by way of legacy system of laws app licable to the physical world. 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 activities in Cyberspace. but the actual truth is remotely different.[5]

When the Internet was developed. its founding fathers hardly had any inclination that the internet could transform itself into an all pervading revolution which could be misused for criminal activities. and which would require regulation. Today however the situation is quite different. and due to the anonymous nature of the internet. it is possible to engage into a varieties of criminal activities by way of impunity. and people by way of intelligence have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence. there has been felt the need for cyber laws in India.

Keeping this is mind. in May 2000. both houses of the Indian Parliament passed the Information Technology Bill. The bill received the assent of the President in August 2000.. and came to be known as the Information Technology Act. 2000. Cyber laws are contained in this IT Act. and it aims to give the legal infrastructure for e-commerce in India.. and the cyber laws have a major impact for e-businesses. and the new economy in India.

Cyber crimes. and attacks cost Indian companies Rs 58 lakh in revenue in 2009. and affected over 66% of Indian enterprises. according to a study by internet securities providers. Symantec Corp.

[5] Aparna Vishwanarthan "Cyber Law"

According to the findings on India in the research titled 2010 State of Enterprise Security. over. and above these revenue losses. Indian enterprises also lost an average of Rs 94.56 lakh in organisation. customer. and employee data.. and an average of Rs 84.57 lakhs in productivities costs last year. Protecting data today is more challenging than ever. By putting in place a securities blueprint that protects their infrastructure. and information. enforces IT policies.. and manages systems more efficiently. businesses can increase their competitive edge in today‟s information-driven world.

The study further found that close to half of the of Indian Enterprises saw cyber securities as their top issue. rating it above threats from natural disasters. terrorism. and traditional crime combined. by way of the rate of attacks increasing in several organizations. a sizeable chunk of the companies said that the nature of cyber attacks consisted of external threats as well as internal threats. and negligence.

1.1 DEFINITION OF CYBERCRIME:~

The term 'cyber crime' has not been defined in any Statute or Act. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet. The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology. So what exactly is Cyber Crime. Cyber Crime could reasonably include a wide varieties of criminal offences. and activities. A generalized

definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both".

CBI Manual defines cyber crime as:~

(i) Crimes committed by using computers as a means. including conventional crimes.

(ii) Crimes in which computers are targets.

The Information Technology Act. 2000. does not define the term 'cyber crime'. Cyber crime can generally defined as a criminal activities in which Information Technology systems are the means used for the commission of the crime.

The IT Act provides legal recognition for transactions carried out by mea ns of electronic datainterchange.. and other means of electronic communication. commonly referred to as "electron iccommerce". involving the use of alternatives to paper-based methods of communication andstorage of information. The IT Act f acilitates electronic filing of documents by way of the Governmentagencies.

1.2 LITERATURE REVIEW:~

Cyber- crime or computer crime is considered to be any crime that uses a computer. and acomputer network (Matthews. 2010). A basic definition describes cybercrime as a crime wherecomputers have the possibilities of

playing an important part (Thomas. and Loader. 2000). Themain factor in cyber-crime increase is the Internet. By use of Internet. cybercriminals oftenappeal to images. codes or electronic communication in order to run malicious activities. Amongthe most important types of Internet crimes we can mention:~ identities theft. financial theft.espionage. pornography. or copyright infringement. The cyber- crimes can be divided into twocategories:~ the crimes where a computer network attacks other computers networks – e.g. acode or a virus used to disable a system. and. the second category. crimes where a computernetwork attacks a target population – e.g. identities theft. fraud. intrusions (Svensson. 2011).Issues revolving around cyber-crime have become more. and more complex. Computer criminalactivities have grown in importance. and institutions are more interested than ever in putting anend to these attacks. Progressions have been made in the development of new malwaresoftware. which can easily detect criminal behavior (Balkin et al.. 2007). Moreover. high qualityanti-virus systems are offered for free now in many countries at every purchase of a computeror an operating system.

1.3 RESEARCH OBJECTIVES. AND AIM:~

The growing danger from crimes commited against computer . or against data on computer. is beginning to claim attention in national capital. The study investigates whether or not people would use the internet to report crime. The pin pointed objective of the study is to find out awareness among different respondents on the issue of Cyber Crime. It is assumed that there is no association between Respndents Occupation. and the level of awareness.

1.4 RESEARCH METHODOLOGY:~

The doctrinal research covers the broader contours of the cyber frauds in relation by way of cybercrimes. The researcher has consulted by way of Bare Act. books. websites cases. articles. journals. The research paper will not only be help full for students. academicians. policy maker in enhancing their knowledge about world constitutions discussing socio- economic right of their citizen but also provoke people to think about protecting. and preserving beautiful creation.

1.5 RESEARCH QUESTION:~

To look into the meaning. concept. and definition of cybercrimes

1. What will be the future consequence of not preventing of threats to cybercrimes?
2. To find out the legal strength in protecting from cyber crime?
3. What are the legal guarantees in protection of confidential sources of information?
4. Will the recent proposed amendment to the Information Technology Act. 2000 answer the contemporary complications in the cybercrimes arena in India?
5. To find out the solution. and make proper suggestion for how to fight by way of increasing threat of cybercrimes?

CHAPTER- 02

CYBERCRIME AND ITS CATEGORIZATION

CHAPTER- 02

CYBER CRIME. and ITS CATEGORISATION

Computers did not commit crimes. Howother computer by way of internet has given to a new generation of Crime. Automated machine are used. Internet is a wonder gift of science to mankind. but now has become a heaven for criminals.

According to the researcher. Cybercrime can be basically divided into 3 major categories:~

- Cybercrimes against persons.
- Cybercrime against property.
- Cybercrime against government.

2.1 CYBERCRIME AGAINST PERSONS:~

Cybercrimes committed against persons include crimes like transmission of child-pornography . harassment of any one by way of the use of a computer such as e-mail. The trafficking. distribution. posting. and dissemination of obscene material include pornography. and indecent exposure.constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanities can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scar. and injury on the younger generation. if not controlled. [6]

Cyber-harassment is the distinct cybercrime. Various kinds of harasament can do occur in cyberspace. or through the use of cyberspace. Harassment can be sexual. racial. religious or others. Person perpetuating such harassment is also gulities of

[6] Talat Fatima. "Cyber Crime ". Eastern Book Company

cybercrime. Cyber-harassment as a crime also bring us to another related area of voilation of privacy of cirizen. Voilation of privacy of online citizen is a Cybercrime of a grave nature. No one likes any other person invading the invaluable. and extremely touchy area of his/her privacy which the medium of internet grants to the citizen.

2.2 CYBERCRIME AGAINST PROPERTY:~

The second category of Cybercrime is that Cybercrime against all forms of property. These crimes include computer vandalism(destruction of other's property). transmission of harmful programmmes. These are numerous example of such computer viruses few of them being "Melissa". and "Love bug". which appeared on the internet in March of 1999. It spread rapidly throughout computer system in the United States an Europe. It is estimated that the virus caused 80 million dollars in damages to the worldwide. Companies lose much money in the business when the rival companies. steal the technical database from their computer by way of the help of a corporate cyberspy.

2.3 CYBERCRIMES AGAINST THE GOVERNMENT:~

The third category of Cybercrime relate to Cybercrime against Government. Cyber-terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individual. and group to threaten the international government as also to terriorise the citizen of a country. This crime manifiests itself into terrorism when an individual "cracks" into a government or military maintained websites. It was said that internet was becoming a boon for the terriorist organization.

Cracking is amongst the gravest Cybercrimes known. It is dreadful feeling to know that a stranger has broken into your computer system without knowledge. and consent. and has tampered by way of precious confidential data. and information. Coupled by way of this

the actually is that no computer system in the world is cracking proof. It is unamimously agreed that any. and every system in the world can be cracked. The recent denial of service written as DoS attack seen over the popular commercial sites like Ebay. flipkart. amazon. myntra. and others are a new category of Cybercrime which are slowly emerging as being extremely dangerous.

The ten commandments of Cyber Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere by way of other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid .
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in away that ensures consideration. and respect for your fellow humans.

CHAPTER-03:~ THE CAUSES AND CRIMINALS

CHAPTER-03

THE CAUSES AND CRIMINALS

3.1 PASSION OF YOUNGSTER:~

Cybercrime can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed. and feel among the group of the big. and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be spotlight.

3.2 DESIRE OF MAKING QUICK MONEY:~

Another cause of Cybercrime is to make quick money. This group is greed motivated. and is career criminal. who tamper by way of data on the net or system especially. e-commerce. e-banking data data by way of the sole aim of committing fraud. and swindling money off unsuspecting customers.

3.3 MISCONCEPTION OF FIGHTING A JUST CAUSE:~

Thirdly Cybercrime can be committed to fight a cause one thinks he believes in; to cause threat. and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of Cybercrime. Those who get involved believe that they are fighting a just cause. and so do not mind who or what they destroy in their quest to get their goals achieved. These are the Cyber- terrorists.

3.4 CAPACITIES TO STORE DATA IN COMPARATIVELY IN A SMALL SPACE:~

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

3.5 AVAILABILITIES OF CONFIDENTIAL DATA IS ONLINE:~

Confidential data from securities firms. scientific databases. financial institutes. and even governmental organization is stored online. and on networks. This allows Cybercrime to initiate unauthorized access. and use it for their own needs. Complex technology can be bypassed. allowing criminals to gain access to securities codes. bank accounts. and other information.

3.6 NEGLIGENCE& CARELESSNESS :~

Sometimes simple negligence can rise to criminal activities. such as saving a password on office computer. using official data in a public place. and even storing data without protecting it. The Cybercriminal can take advantage of such negligence. and use it to obtain. manipulate. and forge information.

Negligence is very closely connected by way of human conduct. It is therefore very probable that while protecting the computer system there might be some negligence. which in turn provides Cybercriminals to gain access. and control over the computer system.

3.7 COMPLEXITIES IN UNDERSTANDING:~

The computer work on operating systems. and these operating system 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 Cybercriminals take advantages of these lacunae. and penetrate into the computer system.

CHAPTER - 04

THE VARIOUS KINDS. and MANNERISM OF COMMITTING CYBER CRIMES

CHAPTER - 04

THE VARIOUS KINDS AND MANNERISM OF COMMITTING CYBER CRIMES

Cyber crimes involve a modification of a conventional crime by using computers.Following is a comprehensive list of the various types of Crimes which have been committed in the recent times.

4.1 CYBER TERRORISM

Cyber terrorism may be defined to be "the premeditated use of distruptive activities. or the threat thereof. in cyber space. by way of the intention to further social. ideologic al. religious. political or similar objectives. or to intimidate any person in furtherance of such objectives". [7]The role of computer by way of respect to terrorism is that a modern thief can steal more by way of a computer than by way of a gun. and a future terrorist may be able to cause more damage by way of a keyboard than by way of a bomb. No doubt. the great fears are combined in terrorism. the fear of random. violent. victamisation segues well by way of the distrust. and out of fear of computertechnology. Technology is complex. abstract. and indirect in its impact on individual. and it iseasy to distrust that which one is not able to control. People believe that technology has theabilities to become the master. and humanities its servant.

4.2 CYBER PORNOGRAPHY

The growth of technology has flip side to it causing multiple problems in everyday life. The Internet has provided a medium for the facilitation of

[7]http:~//www/fb i.gov/quickfacts.htm

crimes like pornography. Cyber porn as it is popularly known is widespread. Almost 50 % of the websites exhibit pornographic material today. Pornographic materials can also be reproduced more quickly. and cheaply on new media like hard disks. and cd-roms. The new technology is not merely limited to texts. and images but have full motion video clips. and movies too. These have serious consequences. and have result in serious offences which have universal disapproval like child pornography which are far easier for offenders to hide. and propagate through the medium of the internet. [8]

4.3 CYBER STALKING

Cyber stalking can be defined as the repeated actsof harassment or threatening behaviour of the cyber criminal on the victim by using the internet services. Stalking may be followed by serious violent acts such as physical harm to the victim. and the same has to be treated. and viewed seriously. It all depends on the course of conduct of the stalker. Cyber Stalking is a problem which many people especially young teenage girls complain about.[9]

4.5 CYBER CRIME RELATED TO FINANCE

There are various types of Cyber Crimes which are directly related to financial or monetory gains by illegal means. To achieve this end. the persons on the cyber world who could be suitably called as fraudsters use of different techniques. and schemes to befool other people on the

[8] Buskin J. „THE W EB"S DIRTIES SECRET". Wall St reet Journal. Available:~ Proquest:~ABI/ Inform Global. 2000.

[9]Dudeja V D. CRIM ES IN CYBER SPACE- SCAMS. and FRAUDS (ISSUES. and REM EDIES) Co mmonwealth Publishers. New Delhi. 2003.

internet. Online fraud. and cheating is one of the most lucrative business that is growing today in the cyberspace. It may assume different forms. Some of the cases of online fraud. and cheating have come to light are pertaining to credit-card crimes. contractual crimes. online auction frauds. online investment schemes. job offerings. etc. [10]

4.6 CYBER CRIMES INVOLVING MOBILE. and WIRELESS TECHNOLOGY

At present the mobile technology has developed so much that is becomes somewhat equivalent to a personal computer. There is also increase in the services which were never available on mobile phones before. such as mobile banking. which is also prone to cyber crimes.

Due to the development in the wireless technology the cyber crimes on the mobile device is coming at par by way of the cyber crimes on the inernet day by day.[11]

4.7 DATA DIDDLING

Data diddling involves changing data prior or during input into a computer. In other words. data is changed from the way it should be entered by a person typing in the data. or a virus that changes data. or the programmer of the database or application. or anyone else involved in the process of having data stored in a computer file. The culprit can be anyone involved the process of creating. recording. encoding. examining. checking. converting or transmitting data.[12] This kind of an attack

---

[10] Love. David. CYBER TERRORISM :~ IS IT A SERIOUS THREAT TO COMM ERCIAL ORGANISATION?
www.crime-research.org/news/2003/04/Mess0204.ht ml.

[11]US Depart ment of Justice. Criminal Division. Fraud Section. http:~//www.usdoj.gov/criminal/fraud/internet.

[12]http:~//www.n rps.com/community/comprev.asp.

involves altering raw data just before it is processed by a computer. and. then changing it back after the processing is completed.[13] Electricities Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

This is one of the simplest methods of committing a computer-related crime. because it requires almost no computer skills whatsoever. Despite the ease of committing. the cost can be considerable. To deal by way of this crime. a company must implement policies. and internal controls.This may include performing regular audits. using softwares by way of built in features to combat such problems.. and supervising employees. [14]

4.8 DENIAL OF SERVICE ATTACKS

This is an act by a criminal who floods the bandwidth of the victam‟s network or fills hisemail box by way of spam mail depriving him of the service he is entitled to access or give Shortfor denial-of-service attack. a type of service attack on a network which is designed to bring thenetwork down to its knees by flooding it by way of useless traffic.[15] Many DoS attack such as Ping ofDeath[16]. and Teardrop attack[17]. exploit limitation in the TCP/IP protocols. For all known DoSattacks. there are softwares fixes that system administrators can install to limit the damagecaused by the attacks. But. like Virus. new DoS attacks are constantly being dreamed up

---

[13]

[14]David Bowen. Viruses. Worms. and Other Nasties. Protecting yourself online; Depart ment of InterdiscplinaryStudies. 2003.

[15]Understanding Denail of Serv ice Attacks (US CERT) http:~//www.us -cert.gov/cas/tips/ST04-015.html.

[16]A Ping of Death is type of attack on a co mputer network that involves sending a malformed o r otherwisemalicious ping. A ping is normally of 64 bytes in size. Sending a p ing which is larger than the maximu m IP packetsize can crash the target computer.

[17]A tear drop attack is a DoS attack where frag mented packets are forged to overlap each other when the receivinghost tries to reassemble them.

by hackers. This involves flooding computer resources by way of more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. [18]Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many. and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victam‟s computer. exceeding the limit that the victam‟s server can support. and making the servers crash. Denial-of-service attacks have had an impressivehistory in the past. and have brought down websites like the Amazon. CNN. Yahoo. and eBay.

4.9 EMAIL BOMBING

In internet usage. an email-bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox.[19] Mailbombing is the act of sending an email bomb. a term shared by way of the act of sending actual exploding devices. There are two ways of e- mail bombing. mass mailing. and list linking. Mass mailing consists of sending numerous duplicate mails to the same email ID. These types of mail bombers are simple to design. but due to their extreme simplicities they can be easily filtered by sham filters. List linking on the other hand. consists of signing a particular email ID up to several subscriptions. This type of bombing is effective as the person has to unsubscribe from all he services manually. In order to prevent this type

[18]http:~//www.cert.org/advisories/CA-1997-28.ht ml.
[19]http:~//www.cert.org/tech_tips/e-mail_bo mbing_spamming.ht ml.

of bombing most type of services send a confirmation to the mailbox when we register for the subscription on a particular website.

E-mail spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users. E- mail spamming can be made worse of the recipients reply to the email. causing all the original addresses to receive the reply. [20]

4.10 EMAIL SPOOFING

E- mail spoofing is a term used to describe fraudulent email activities in which the senderaddress. and other parts of the email header are altered to appear as though the email originatedfrom a different source. Email spoofing is a technique commonly used for spam email andphishing to hide the origin of an email message. By changing certain properties of the email. such as the From. Return-Path. and Reply- To fields. ill-intentioned users can make the email appear to be from someone other than the actual sender. It is often associated by way of website spoofing which mimic an actual well-known website but are run by other parties either withfraudulent intentions or as a means of criticism of the organizational activities.

It is forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual code. Distributors of spam often use spoofing in an attempt to get recipient to open.. and possibly respond to such solicitations. Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the email include a sender reporting mistreatment by a spouse to

[20]http:~//www.lse.ac.uk/ itservices/help/spamming&spoofing.htm.

a welfare agency or a "whistle blower" who fears retaliation. However. spoofing anyone other than yourself is illegal in many jurisdictions.[21]

Email spoofing is possible because Simple Mail Transfer Protocol (SMTP). the main protocol used in sending email. does not allow an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a securities level by way of a mail server. however this precaution is not always taken.

If the precaution is not taken. anyone by way of the requisite knowledge can connect to the server. and use it to send messages. To send spoofed messages. senders insert commands in headers that modifies the message information. It is possible to send a message that appears from anyone. and anywhere. saying whatever the sender wants to say. [22]

4.11 HACKING

Hacking means unauthorized access to a computer system.[23] It is the most common type of Cyber Crime being committed across the world. The word "hacking" has been defined in section 66 of the Information Technology Act. 2000 as follows. "whoever by way of the intent to cause or knowingly that he is likely to cause wrongful loss or damage to the public or any person. destroys or deletes or alters any data residing in a computer resource or diminishes its value or utilities or affects it injuriously by any means commits hacking"

[21]To m Merritt. What is Email Spoofing? See www.g4tv.co m.
[22]http:~//www.mailsbroadcast.com/e-email.broadcast.faq/46.e-mail.spoofing.htm
[23]Section 66 of data Technology Act. 2000.

Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend up to two lakh rupees or both. [24]

4.12 INTELLECTUAL PROPERTIES CRIME

Criminal IP offences are also known as "IP crime" or "counterfeiting". and "piracy". Counterfeiting can be defined as the manufacture. importation. distribution. and sale of products which falsely carry the trade mark of a genuine brand without permission. and for gain or loss to another. Piracy. which includes copying. distribution. importation etc. of infringing works. does not always require direct profits from sales - wider. and indirect benefits may be enough along by way of inflicting financial loss onto the rights holder. For example possession of an infringing copy of a work protected by copyright in the course of your business may be a criminal offence under section 107 (1)(c) of the Copyright. Designs. and Patents Act 1988.

Not all cases that fall within the criminal law provisions will be dealt by way of as criminal offences. and in many cases business to business type disputes are tackled by the civil law. Further data is available on what is the law. and the guide to offences.

4.13 INTERNET TIME THEFT

Theft of Internet hours refers to using someone else internet hours. Section 43 (h) of the IT Act. 2000 lays down civil liabilities for this offence. It reads as . whosoever without the permission of the owner or any other person who is in charge a computer system or computer

[24]Ibid.

network. charges the service availed of by a person to the account of another person by**tampering by way of or manipulating any computer. computer systems or network is liable to paydamages not exceeding one crore to the person in office.** [25]

In the Colonel Bajwa's case[26]. the economic offences wing. IPR section crime branch of Delhi Police registered its first case involving theft of internet hours. In this case. the accused. Mukesh Gupta. an engineer by way of Nicom System (p) Ltd was sent to the residence of the complainant to activate internet connection. However. the accused used Col. Bajwa's login name. and password from various places causing wrongful loss of 100 hours to him. Initially the Police could not believe that time could be stolen. They were not aware of the concept of time theft at all. and his report was rejected. He decided to approach the Times of India. New Delhi which in turn carried a report on the inadequacy of the Delhi Police in handling Cyber Crimes. The Commissioner of Police.. then took the case in his own hands. and the Policethen registered a case under Section 379. 411. 34 of the IPC. and section 25 of the Indian Telegraph Act.

4.15 LOGIC BOMBS

A logic bomb is a programming code. inserted surreptitiously or intentionally. and which is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. [27]Software that is inherently malicious.

[25]Section 43 of the IT Act. 2000.
[26]http:~//www.asain laws.org/cyberlaw/library/cc/what_cc.htm.
[27]M E Kabay. Logic bombs. Part 1. Network World Securities Newsletter.

such as viruses. and worms. often contains logic bombs that execute a certain payload at the pre-defined time or when some other conditions are met. Many viruses attack their hosts systems on specific days. e.g. Friday the 13th. and April fool's day logic bombs. A logic bomb when exploded may be designed to display or print a spurious message. delete or corrupt data. or have other undesirable effects. [28]

Some logic bombs can be detected. and eliminated before they execute through a periodic scan of all computer files. including compresses files. by way of an up to date anti- virus program. For best results. the auto-protect. and email screening functions should be activated by the user whenever the machine is online. A logic bomb can also be programmed to wait for a certain.

4.16 PHISHING

In computing. phishing is a form of social engineering. characterized by attempts to fraudulently acquire sensitive information. such as passwords. and credit cards. by masquerading as a trustworthy person or business in an apparently official electronic communication. such as an email or an instant message.[29] The term phishing arises from the use of increasingly sophisticated lures to a Phish for usersfinancial information. and passwords.[30] The act of sending an email to a user falsely claiming to be an established. and legitimate enterprise in anattempt to scam the user into surrendering private data that will be used for identities theft.

The email directs the user to visit a website where they are asked to update personal information.such as passwords. and credit card. social

[28]Meaning of logic bomb. http:~//en.wikipedia.org/wiki/logic_bomb.
[29] http:~//www/trai.gov.in
[30] Tan. Koon. Phishing. and Spamming via IM.Internet Storm Center. December 5th. 2006.

securities no.. and bank account no. that the legitimateorganization already has. The website. however is bogus. and is setup only to steal the usersinformation. By spamming large group large group of people. the „phisher counted on the emailbeing read by a percentage of people who actually had listed credit cards numbers withlegitimacy. Phishing also refers to a brand spoofing or carding. is a variation on phishing. the ideabeing that the bait is thrown out by way of the hope that while most will ignore the bait. some will betempted into biting it. by way of the growing no. of reported phishing incidents. additional methods ofprotection are needed. Attempts include legislation. user training. and technical measures. Morerecent phishing attempts have started to target the customers of banks. and online paymentservices. [31] While the first such example are sent indiscriminately in the hope of finding acustomer of a given bank or service. recent research has shown that phishers may in principle beable to establish what bank a potential victim has a relation with.. and. then sends an appropriatespoofed email to the victim. In general such targeted versions of phishing have been termed asspear phishing.[32]

4.17 SALAMI ATTACKS

A salami attack is a series of minor data-securities attack that together result in a larger attack. For example. a fraud activities in a bank. where an employee steals a small amount of funds from several accounts. can be considered a Salami Attack. [33]Crimes involving salami attacks are

[31]Ollmann. Gunter. THE PHISHING GUIDE:~ UNDERSTA NDING A ND PREVENTING PHISHING ATTA CKS:~ Technical Info. 2006.
[32]What is Spear Phishing?. Microsoft Securities At Ho me. July 10th 2006.
[33]Aderucci. Scott. Salami Fraud. www.all.net/CID/attack/papers/Salami .html.

typically difficult to detect. and trace. These attacks are used for commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e g a bank employee inserts a program into the bank servers that deducts a small amount of money (say Rs. 5 a month) from the account of every customer.No account holder will probably notice this unauthorized debit. but the bank employee will make a sizable amount each month.[34] To cite an example. an employee of a bank in USA was dismissed from his job. Disgruntled at having been mistreated by his employers. he introduced a program into the bank systems. This program was programmed to take ten cents from all accounts in the bank. and put them into the account of the person whose name was alphabetically the last name in the bank's rosters.. then he went. and opened an account in the name ofZiegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither the accountholders nor the bank officials noticed the fault. It was brought to their notice when a person bythe name of „Zygler" opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday. [35]From a systems development standpoint. such scams reinforce the critical importance of sound qualities assurance throughout the software development life cycle. [36]

message from the programmer. However in some ways a logic bomb is the most civilized programmed threat. because it targeted against a

[34]Kabay. M E Salami fraud. www.nwfusion.com/newsletters/sec/2002/01467137.ht ml.
[35]Smith RG. Grabosky PN. and Urbas GF 2004. Cyber criminals on trial. CamridgeUniversities Press.
[36]B. Michael Hale. Salami Attacks. http:~//all.net/CID/Attack/papers/Salami2.html.

particular victim. The classic use of a logic bomb is to ensure the payment for software. If payment is not made by a certain date. the logic bomb gets activated. and the software automatically deletes itself.

4.18 SALE OF ILLEGAL ARTICLES:~

This would include sale of narcotics. weapons. and wildlife etc.. by posting data on websites. bulletin boards or simply by using e-mail communications.

4.19 THEFT OF data CONTAINED IN ELECTRONIC FORM

There have been a growing number of cases of data theft over the past few years. While more. and more electronic securities measures have been going up to protect people's possessions. and information. these new technologies have bugs. and design flaws that are opening up whole new worlds for the technologically advanced criminal.

Credit Card Number Theft

People are using credit cards for more. and more of their purchases as time goes on. This is opening up a larger. and larger arena for credit card fraud. Credit cards are especially easy to use fraudulently. because they require no extra identification number to use. All that a thief needs is pure information-they don't need the card. but just the number on the card. Recently. by way of people spending more on purchases transacted over the internet. credit card fraud is becoming easier. Now thieves never have to get within 5.000 miles of the people they are stealing from. All they would need is a quick. and dirties web site (which could be hosted for free.. and anonymously) advertising some fictional product.. and including a form for buying online. Instantly the perpetrators would have

a list of credit card numbers linked by way of names. and mailing addresses. ready to use for anything they want.

ATM Spoofing

These crooks have pulled some impressively intricate heists. One group of criminals set up a complete fake ATM machine inside a mall in Connecticut.. It looked. and worked just like a real one. except that after giving it your card. and typing in your pin. it would refuse you service saying it was out of order. It. then had a record of the card. and PIN numbers of all the people who tried to use the machine. The thieves. then used legitimate ATM machines all over town to withdraw over $3.000 from these accounts.["The Risks Digest Volume 14:~ Issue 60" 1]

PIN Capturing

Another group of criminals scoured the area across the street from a busy ATM. looking for the perfect spot to hide a video camera aimed at the keys on the ATM machine. They found such a spot. and set up their camera. After each successful PIN number identification that they recorded. one of the group members would go check for a discarded receipt at the ATM. If they found one. the group had the card number. and the PIN number.

Database Theft

The previous criminal activities are all aimed at compiling databases of data obtained fraudulently from people one by one. This takes time.. and these people only have limited amounts of time before their operations will be recognized. and shut down. This limits the number of people whose data these criminals can obtain. There are. however. large

databases of this kind of data that have been built up slowly. and legally by mild-mannered. legitimate internet companies. For example. BMG Music Service lets customers give their credit card numbers when they sign up. so they don't need to bother each time they make a purchase. There are thousands of users of this service. many of whom likely use this feature. Combine this by way of the fact that hundreds of computer systems are hacked into every day.. and we have a situation where hackers could steal an industrial-sized database of this kind of information.. and run wild.

Electronic Cash

We are already well on the way to a cash-free society. People now use ATM cards. credit cards.. and check-cards for a large percentage of their purchasing. As we move further from a paper-money society. to a purely electronic economy. new types of crime will emerge. What types exactly will depend on what new forms of securities tomorrow's criminals will need to break. Will people be synthesizing voice authorizations? Or running replay attacks on retinal scanners? Or even learning to imitate a victim's typing style. All we can be sure of. is that criminals of tomorrow. like those of last century. and those of today. will keep on innovating.

4.20 UNAUTHORIZED ACCESS TO COMPUTER SYSTEM OR NETWORK

Unauthorized access to data through the compromising of computer securities is known also as hacking. Ideally any organization should have some kind of incident response plan to deal by way of hacking incidents

but resent research shows that that they do not. More over the threat of hacking by insiders to organizations is far more serious than outsiders.. and the potential for damage to organizations today from this threat is even higher today than it ever was in the past.

4.21 VIRUSES. TROJANS. and WORMS

A computer virus is a program designed to replicate. and spread. generally by way of the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programme like word-processors or spreadsheets or they attach themselves to the boot sector of a disk. Thus when an infected file is activated. the virus itself is also executed. [37]Trojan horse is defined a "malicious. security-breaking program that is disguised as something benign" such as a directory list .archiver. game. or a program to search or destroy viruses.[38]

A computer worm is a self contained program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses. worms do not need to attach themselves to a host program. [39]

4.22 WEB JACKING

This term is derived from the term hi jacking. This occurs when someone forcefully takes control of a website by cracking the password. and. then changing it. The actual owner of the website does not have any control

[37]Baratz Adam.. and McLaughlin. Charles. "MALWARE:~ WHAT IT IS. and HOW TO PREVENT IT" A rsTechnica.2004. http:~//www.ncsl.org/programs/lis/cip/viruslaws.ht m

[38]The word „Trojan Horse" is generally attributed to Daniel Ed wards of the NSA. He is given the credit foridentifying the attack form in the report „Co mputer Securities Technology Planning Study"

[39]http:~//cybercrime.planetindia.net/worms.ht m.

over what appears on that website. 47[40] In a recent incident reported in USA. the owner of a hobby website for children received an email informing her that

a group of hackers had gained control over her website. The owner did not take the threat seriously. Three days later she came know from phone calls from across the globe that the hackers had web jacked her website. Subsequently they had altered a portion of text in the website which said „How to have fun by way of a goldfish" to „how to have fun by way of pirhanas". Many children believed the content of the website. and unfortunately were seriously injured as they tried playing by way of the pirhanas which they bought from pet shops.[41]

[40]http:~//www.asian laws.org/cyberlaw/library/cc/what_cc.htm.
[41]RohasNagpal. Asian School of cyber Law. http:~//www.asianlaws.org/press/esecurity.htm.

THE HIGH-TECH CRIMINALS

Cyber crime has become a profession. and the demographic of typical cyber criminal is changing rapidly. from bedroom-bound geek to the type of organized gangster more traditionally associated by way of drug-trafficking. extortion. and money laundering. It has become possible for people by way of comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact. to make more money than can be made selling heroin. the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that. The rise of cyber crime is inextricably linked to the ubiquities of credit card transactions. and online bank accounts. Get hold of this financial data. and not only can you steal silently. but also through a process of virus-driven automation by way of ruthlessly efficient. and hypothetically infinite frequency.

Out of the pool of these hi-tech cyberpunks. the most prominent. and well-known ones are known as hackers. Until the 1980s. all people by way of a high level of skills at computing were known as "hackers". A group that calls themselves hackers refers to "a group that consists of skilled computer enthusiasts". Over time. the distinction between those perceived to use such skills by way of social responsibility. and those who used them maliciously or criminally became perceived as an important divide. The general public tends to use the term "hackers" for both types. a source of some conflict when the word is perceived to be used incorrectly; for example Linux has been criticised as "written by hackers".

In computer jargon the meaning of "hacker" can be much broader. Now. these are broadly classified under three broad categories.

5.1 Black Hat Hackers

A black hat Hacker is a person who compromises the securities of a computer system without permission from an authorized party. typically by way of malicious intent. Usually. a black hat is a person who uses their knowledge of vulnerabilities. and exploits for private gain.Eric S. Ray mond:~ A BRIEF HISTORY OF HACKERDOM (2000) revealing them either to the general public or the manufacturer for correction. Many black hats hack networks. and web pages solely for financial gain. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system they have already obtained secure control over. A black hat hacker may write their own zero-day exploits. which is private software that exploits securities vulnerabilities.The general public does not have access to 0-day exploits. In the most extreme cases. black hats may work to cause damage maliciously. and/or make threats to do so as extortion. Black hat person is also called as hactivist who uses the same tools as a regular hacker hactivism is a new global phenomenon of the hackers underground to reveal sensitive data like details of U.S. war against Iraq. and Afghanistan.

5.2 White Hat Hackers

A white hat hacker. also rendered as ethical hacker. is. in the realm of Information Technology. a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrities an important pastime for many. A white hat generally focuses on securing IT systems. whereas a black hat would like to break into them. The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of securities flaws. or to perform some other altruistic activity. Many such people are employed by computer securities companies; these professionals are sometimes called sneakers. Groups of these people are often called tiger teams.

5.3 Grey Hat Hackers

A Grey Hat in the computer securities community. refers to a skilled hacker who sometimes acts legally. sometimes in good will.. and sometimes not. They are a hybrid between white. and black hat hackers. They usually do not hack for personal gain or have malicious intentions. but may or may not occasionally commit crimes during the course of their technological exploits. One reason a grey hat might consider himself to be grey is to disambiguate from the other two extremes:~ black. and white. It might be a little misleading to say that grey hat hackers do not hack for personal gain. While they do not necessarily hack for malicious purposes. grey hats do hack for a reason. a reason which more often than not remains undisclosed. A

grey hat will not necessarily notify the system admin of a penetrated system of their penetration. Such a hacker will prefer anonymities at almost all cost. carrying out their penetration undetected. and. then exiting said system still undetected by way of minimal damages.

Consequently. grey hat penetrations of systems tend to be for far more passive activities such as testing. monitoring. or less destructive forms of data transfer. and retrieval[42]

Not all cyber-criminals operate at the coalface.. and certainly don‟t work exclusively of one another; different protagonists in the crime communities perform a range of important. specialized functions. These broadly encompass.

1. Coders – comparative veterans of the hacking community. by way of a few years' experience at the art. and a list of established contacts. „coders‟ produce ready-to-use tools (i.e. Trojans. mailers. custom bots) or services (such as making a binary code undetectable to AV engines) to the cyber crimelabour force – the „kids‟. Coders can make a few hundred dollars for every criminal activities they engage in.

2. Script Kids – so-called because of their tender age:~ most are under 18. They buy. trade. and resell the elementary building blocks of effective cyber-scams such as spam lists. php mailers. proxies. credit card numbers. hacked hosts. scam pages etc. Kidswill make less than $100 a month. largely because of the frequency of being ripped off by one another.

3. Drops – the individuals who convert the virtual money obtained in cyber crime into real cash. Usually located in countries by way of lax e-

[42]http:~//webzone.k3.mah.se/k3jolo/HackerCultures/origins.htm.

crime laws (Bolivia. Indonesia. and Malaysia are currently very popular). they represent safe addresses for goods purchased by way of stolen financial details to be sent. or else safe legitimate bank accounts for money to be transferred into illegally.. and paid out of legitimately.

4. Mobs – professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organized crime makes particularly good use of safe drops. as well as recruiting accomplished coders onto their payrolls. Gaining control of a bank account is increasingly accomplished through phishing.

The alarming efficiency of cybercrime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster. less detectable. more profitable (generating a return around 400 times higher than the outlay). and primarily non-violent. The other takes months or years to set- up or realise an investment. is cracked down upon by all almost all governmentsinternationally. fraught by way of expensive overheads.. and extremely dangerous.

On top of viruses. worms. bots. and Trojan attacks. organizations in particular are contending by way of social engineering deception. and traffic masquerading as legitimate applicationson the network. In a reactive approach to this onslaught. companies have been layering their networks by way of stand alone firewalls. intrusion prevention devices. anti- virus. and anti-spyware solutions in a desperate attempt to plug holes in the armoury. They're beginning to recognize it's a failed strategy. After all. billions of pounds are being spent on securities technology.. and yetsecurities breaches continue to rise.

To fight Cyber Crime there needs to be a tightening of international digital legislation. and of cross-border law enforcement co-ordination but. there also needs to be a more creative. and inventive response from the organisations under threat. Piecemeal. reactive securities solutions are giving way to strategically deployed multi-threat securities systems. Instead of having to install. manage. and maintain disparate devices. organizations can consolidate their securities capabilities into a commonly managed appliance. These measures combined. in addition to greater user education are the best safeguard against the deviousness. and pure innovation of cyber-criminal activities.

Chapter- 05:~ LAWS RELATED TO CYBER CRIME IN INDIA

CHAPTER-05

LAWS RELATED TO CYBER CRIME IN INDIA

5..1. THE Information Technology ACT. 2000

The IT Act. 2000 came at a time when cyber-specific legislation was much needed. It filled up the lacunae for a law in the field of e-commerce. Taking cue from its base-document. i.e. the UNICITRAL Model Law on electronic commerce. adopted in 1996. a law attuned to the Indian needs has been formulated. Apart from e-commerce related provisions. computer crimes. and offences along by way of punishments have been enumerated. and defined. The power the police to investigate. and power of search. and seizure. etc have been provided for. However. certain points need a re-working right from the scratch or require revamping.

At the first instance. though the IT Act. 2000 purports to have followed the pattern UNICITRAL Model Law on Electronic Commerce. yet what took people by surprise is coverage not only of e-commerce. but something more. i.e. computer crime. and amendments to the Indian Penal Code. The UNICITRAL Model Law did not cover any of the other aspects. Therefore in a way. the IT Act. 2000 has been an attempt to include other issues relating to cyber world as well which might have an impact on the ecommerce transactions. and its smooth functioning. Though. that of course is not reflected even from the Statements of Objectives. and reasons

or the preamble of the Statute. Amendments to the Indian evidence Act are evidently made to permit electronic evidence in court. This is a step in the right direction.

Secondly. a single section devoted to liabilities of the Network Service Provider is highly inadequate. The issues are many more. Apart from classification of the Network Service provider itself there can be various other instances in which the Provider can be made liable specially under other enactments like the Copyright Act or the Trade Marks Act. However the provision in the IT Act. 2000 devoted to ISP protection against any liabilities is restricted only to the Act or rules or regulations made there under. The section is not very clear as to whether the protection for the ISP's extends even under the other enactments.

It has been argued that the Act of this nature would divide the societies into digital haves. and digital have-nots. This argument is based on the premise that by way of an extremely low PC penetration. poor Internet connectivity. and other poor communication infrastructure facilities. a country like India would have islands of digital haves surrounded by digital have-nots . Logically speaking. such an argument is untenable as the „digital core has been expanding horizontally. and everyday communication connectivities is rising across India.

There has been a general criticism of the wide powers given to the police under the Act. Fear. specially among cyber café owners. regarding misuse of powers under the IT Act. 2000 is not misplaced. Anyone can be searched. and arrested without warrant at any point of time in a public place. But at the same time. the fact that committing a computer crime

over the net. and the possibilities of escaping thereafter is so much more viable. that providing such policing powers check the menace of computer crimes is also equally important. Yet this is no reason for giving draconian powers to the police. For example. interception of electronic messages. and emails might be necessary under certain situations but the authorities cannot be given a free-hand in interception as. and when they feel. Similarly. we need to enquire. and delve deeper into the police power of investigation. search. and warrant under the IT Act. 2000. and look for a more balanced solution.

In addition to this. various other Advantages. and Disadvantages of the IT Act. 2000 can be attributed which are highlighted in following headings.

5..1 ADVANTAGES

The Act offers the much-needed legal framework so that data is not denied legal effect. validities or enforceability. solely on the ground that it is in the form of electronic records.

From the perspective of e-commerce in India. the IT Act 2000. and its provisions contain many positive aspects.

Firstly. the implications of these provisions for the e-businesses would be that email would now be a valid. and legal form of communication in our country that can be duly produced. and approved in a court of law.

Second. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Third. Digital signatures have been given legal validity. and sanction in the Act.

Fourth. the Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

Fifth. the Act now allows Government to issue notification on the web thus heralding e-governance.

Sixth. the Act enables the companies to file any form. application or any other document by way of any office. authority. body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

Seventh. the IT Act also addresses the important issues of security. which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a securities procedure. as stipulated by the Government at a later date.

Eighth. under the IT Act. 2000. it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network. and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages. not exceeding Rs. 1 crore.

5..2 DISADVANTAGES

The IT Law 2000. though appears to be self sufficient. it takes mixed stand when it comes to many practical situations. It loses its certainties at many places like the one mentioned below:~-

First. the law misses out completely the issue of Intellectual Properties Rights.. and makes no provisions whatsoever for copyrighting. trade

marking or patenting of electronic information. and data. The law even doesn't talk of the rights. and liabilities of domain name holders. the first step of entering into the e-commerce.

Second. the law even stays silent over the regulation of electronic payments gateway. and segregates the negotiable instruments from the applicabilities of the IT Act . which may have major effect on the growth of e-commerce in India . It leads to make the banking. and financial sectors irresolute in their stands.

Third. the act empowers the Deputies Superintendent of Police to look up into the investigations. and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result. companies will not be able to escape potential harassment at the hands of the DSP.

Fourth. internet is a borderless medium. it spreads to every corner of the world where life is possible. and hence is the cyber criminal.. then how come is it possible to feel relaxed. and secured once this law is enforced in the nation?

Fifth. the Act initially was supposed to apply to crimes committed all over the world. but nobody knows how can this be achieved in practice. how to enforce it all over the world at the same time?

Sixth. the IT Act is silent on filming anyone s personal actions in public. and. then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third parties data. and information. unless

contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention. This is a practically impossible approach.

Further according to the researcher. the recently proposed IT Act. 2000 amendments are neither desirable nor conducive for the growth of ICT in India. They are suffering from numerous drawbacks. and grey areas. and they must not be transformed into the law of the land. These amendments must be seen in the light of contemporary standards. and requirements. Some of the more pressing. and genuine requirements in this regard are

1. There are no securities concerns for e-governance in India.
2. The concept of due diligence for companies. and its officers is not clear to the concerned segments.
3. The use of ICT for justice administration must be enhanced. and improved.
4. The offence of cyber extortions must be added to the IT Act. 2000 along by way of Cyber Terrorism. and other contemporary cyber crimes.
5.. The increasing nuisance of e-mail hijacking. and hacking must also be addressed.
5.. The use of ICT for day to day procedural matters must be considered.
7. The legal risks of e-commerce in India must be kept in mind.
8. The concepts of private defence. and aggressive defence are missing from the IT Act. 2000.

9. Internet banking. and its legal challenges in India must be considered

6. Adequate. and reasonable provisions must be made in the IT Act. 2000 regarding "Internet censorship"

11. The use of private defence for cyber terrorism must be introduced in the IT Act. 2000

12. The legalities of sting operations (like Channel 4) must be adjudged.

13. The deficiencies of Indian ICT strategies must be removed as soon as possible.

14. A sound BPO platform must be established in India. etc.

The act. on an overall analysis. demonstrates a lack of discussion. and incorporation of various issues relating to cyber law. Through the Act has been given the name „Information Technology Act yet many legal issues like online rights of consumers. privacy concerns. domain names disputes. payment. and security-bugbears. etc have not been addressed. Finally. how the act will be implemented by a Court of law. and its implementation. and flaws in the long run are yet to be tested in the case-specific factual terrain.

5..3 THE RECENT PROPOSED AMENDMENTS IN THE IT ACT.2000

Note on Proposed Amendments to Information Technology Act 2000:~

Report of the Expert Committee:~ Summary of

1. The Amendments to the data Technology Act. 2000 have been shown in revision mode by way of footnotes explaining the amendments.

2. As the technologies . and applications in IT sector change very rapidly. some of the provisions related to parameters that may change from time to time have been amended to give for the new developments to be incorporated by changes in rules/govt. notifications. This would enable the law to be amended . and approved much faster . and would keep our laws in line by way of the changing technological environment.

3.Sub-section 4 of Section 1 relates to "Exclusion". In view of changing needs. operation of this section has been made more flexible through prescription of such exception by rules rather than being part of the main Act.

4. The Act is being made technology neutral by way of minimum change in the existing IT Act 2000. This has been made by amendment of Section 4 of the Act to give for electronic signature by way of digital signature as one of the types of electronic signature . and by enabling the details of other forms of electronic signature to be provided in the Rules to be issued by the Central Government from time to time. This is an enabling provision for the Central Government to exercise as . and when the technology other than digital signature matures. . then there will be no need to amend the Act. and the issue of rules will be sufficient. Consequently the term digital is changed to electronic in other sections.

5.. In Section 4. the main aspect of electronic signature for legal recognition. namely. its reliabilities have been provided consistent by way of the UNCITRAL Model on Electronic Commerce.

5.. Section 6(2)(b) has been amended to allow public-private partnership in e-governance delivery of services.

7. A new Section 10 has been added for "Formulation . and Validities of Electronic Contracts".

8. Relationship between CCA. CA . and Subscribers (Sections 17 to 42) have been revisited on the basis of the recent operational experiences . and certain amendments proposed.

9.In view recent concerns about the operating provisions in IT Act related to "Data Protection. and Privacy" in addition to contractual agreements between the parties. the existing Sections (viz. 43. 65.. 66 . and 72) have been revisited . and some amendments/more stringent provisions have been provided for. Notably amongst these are:~

(i) Proposal at Sec. 43(2) related to handling of sensitive personal data or data by way of reasonable securities practices. and procedures thereto

(ii) Gradation of severities of computer related offences under Section 66. committed dishonestly or fradulently. and punishment thereof

(iii)Proposed additional Section 72 (2) for breach of confidentialities by way of intent to cause injury to a subscriber.

6. Language of Section 66 related to computer related offences has been revised to be in lines by way of Section 43 related to penalties for damage to computer resource. These have been graded by way of the degree of severities of offence when done by any person. dishonestly or

fraudulently without the permission of the owner. Sometimes because of lack of knowledge or for curiosity. new learners/Netizens unintentionally or without knowing that it is not correct to do so end up doing certain undesirable act on the Net. For a country like India where we are trying to enhance the positive use of Internet . and working on reducing the digital divide. it need to be ensured that new users do not get scared away because of publicities of computer related offences.

Section 43 acts as a reassuring Section to a common Nitizen. IT Act in order to ensure that it promotes the use of e-commerce. e-governance . and other online uses has been cautious not to use the word cyber crime in the text.

11.Section 67 related to Obscenities in electronic form has been revised to bring in line by way of IPC. and other laws but fine has been increased because of ease of such operation in electronic form; link-up by way of Section 79 w.r.t. liabilities of intermediary in certain cases has been provided.

12.A new section on Section 67 (2) has been added to address child pornography by way of higher punishment. a globally accepted offense.

13.A new phenomenon of video voyeurism has emerged in recent times where images of private area of an individual are captured without his knowledge. and. then transmitted widely without his consent thus violating privacy rights. This has been specifically addressed in a new proposed sub-section 72(3).

14.A new Section 68(A) has been proposed for providing modes . and methods for encryption for secure use of the electronic medium. as recommended by earlier Inter Ministerial Working Group on Cyber Laws & Cyber Forensics (IMWG).

15.. Section 69 related to power to issue directions for interception or monitoring or decryption of any data through any computer resource has been amended to take care of the concern of MHA . and also on lines by way of the recommendations of IMWG.

15.. A new section 78 A (Examiners of Electronic Evidence) has been added to notify the examiners of electronic evidence by the Central Government. This will help the Judiciary/Adjudicating officers in handling technical issues.

17. Section 79 has been revised to bring-out explicitly the extent of liabilities of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules by way of respect to the functioning of the "Intermediary" including "Cyber Cafes" has been provided for under Section 87.

18. In order to use IT as a tool for socio-economic development. as explained in para 10 above. particularly to promote e-commerce. e-governance. its uses in health. learning. creating more opportunities for employment. reducing digital divide amongst others. it is necessary to encourage societies to go through the learning experience. In order to enable this to happen. it has been made clear that the normal provisions of

CrPC will apply. except that only DSP's . and above will be authorized to investigate the offences.

19.The amendment to the 1st Schedule (Indian Penal Code) . and 2nd Schedule (Indian Evidence Act) around the recommendations of earlier IMWG has been incorporated.

However. the term digital signature would be replaced by electronic signature at suitable places.

ESSENTIAL PRE-REQUISITES OF AN EFFECTIVE CYBER LAW

The cyber law. in any country of the World. cannot be effective unless the concerned legal system has the following three pre requisites.

Firstly. a Sound Cyber Law regime:~ The Cyber law in India can be found in the form of IT Act. 2000. Now the IT Act. as originally enacted. was suffering from various loopholes. and lacunas. These "grey areas" were excusable since India introduced the law recently. and every law needs some time to mature. and grow. It was understood that over a period of time it will grow. and further amendments will be introduced to make it compatible by way of the International standards. It is important to realise that we need "qualitative law". and not "quantitative laws". In other words. one single Act can fulfil the need of the hour provided we give it a "dedicated. and futuristic treatment". The dedicated law essentially requires a consideration of "public interest" as against interest of few influential segments. Further. the futuristic aspect requires an additional exercise. and pain of deciding the trend that may be faced in future. This exercise is not needed while legislating for traditional laws but the nature of cyber space is such that we have to take additional precautions. Since the Internet is boundary less. any person sitting in an alien territory can do havoc by way of the computer system of India. For instance. the Information Technology is much more advanced in other countries. If India does not shed its traditional core that it will be vulnerable to numerous cyber threats in the future. The need of the hour is not only to consider the "contemporary standards" of the countries having developed

Information Technology standards but to "anticipate" future threats as well in advance. Thus. a "futuristic aspect" of the current law has to be considered. Now the big question is whether India is following this approach? Unfortunately. the answer is in NEGATIVE. Firstly. the IT Act was deficient in certain aspects. though that was bound to happen. However. instead of bringing the suitable amendments. the Proposed IT Act. 2000 amendments have further "diluted" the criminal provisions of the Act. The "national interest" was ignored for the sake of "commercial expediencies". The proposed amendments have made the IT Act a "tiger without teeth". and a "remedy worst than malady".

Secondly. sound enforcement machinery:~ A law might have been properly enacted. and may be theoretically effective too but it is useless unless enforced in its true letter. and spirit. The law enforcement machinery in India is not well equipped to deal by way of cyber law offences. and contraventions. They must be trained appropriately. and should be provided by way of suitable technological support.

And. lastly. a sound judicial system:~ A sound judicial system is the backbone for preserving the law. and order in a society. It is commonly misunderstood that it is the "sole" responsibilities of the "Bench" alone to maintain law. and order. That is a misleading notion. and the "Bar" is equally responsible for maintaining it. This essentially means a rigorous training of the members of both the Bar. and the Bench. The fact is that the cyber law is in its infancy stage in India hence not much Judges. and Lawyers are aware of it. Thus. a sound cyber law training of the Judges. and Lawyers is the need of the hour. Inshort. the dream for an "Ideal Cyber

Law in India" requires a "considerable" amount of time. money. and resources. In the present state of things. it may take five more years to appreciate its application. The good news is that Government has sanctioned a considerable amount as a grant to bring e-governance within the judicial functioning. The need of the hour is to appreciate the difference between mere "computerisation". and "cyber law literacy". The judges. and lawyers must be trained in the contemporary legal issues like cyber law so that their enforcement in India is effective. by way of all the challenges that India is facing in education. and training. e- learning has a lot of answers. and needs to be addressed seriously by the countries planners. and private industry alike. E-learning can give education to a large population not having access to it.[43]

Challenges:~ Law students need to apply the concepts of IPR (Intellectual Properties Rights) protection in the context of actual world cases. by way of the emergence of multiple sub-disciplines in IPR. their scope. and contents are getting extremely complicated. and require far more effort. energy. and time. Staying up-to-date by way of international developments in this field is particularly important.

Prospects:~ Its relevance today is evident because it deals by way of all the legalities pertaining to use of digital. and mobile ecosystem. Anyone using the seven raw materials such as computers. computer systems. computer networks. computer resources. and communication devices besides data. and data in electronic form. are covered within the ambit of cyber law.

[43]Kerr. Orin S. THE PROBLEM OF PERSPECTIVE IN INTERNET LAW. Georgetown Law Journal. 91. 357-405.

Starting salary:~ It varies on the role. The biggest factor is the merit of the law student in question. If you're hired by a company as an in-house cyber law counsel. the starting salary would be between Rs 50.000. and Rs 60.000 per month.

After graduating in economics from St Stephen's College. Delhi. I was undecided about my career path. and got into television journalism. Around the same time. I discovered that had an interest in law. I was 19 when I went to the Universities of Cambridge. UK. to study law. I returned six years later to India to start a career in litigation. There are two reasons why I chose this field. It is a high-impact job. and gives opportunities to make a difference instantly in some cases. Being a Supreme Court lawyer means you have chances to take intriguing cases that revolve around monitoring the implementation of fundamental rights.

Their relatively swift decisions are gratifying. and at times can double as a significant step on a good cause. It's also intellectually stimulating. This is easily the most fulfilling part of my job. Things are harder than when I started out. and I'd say it's important for a young litigator to be extremely articulate. have good memory. and be able to think on their feet. You'd have to speak in court often. eventually.. and should be cool-headed. That's the only way to deal by way of conflict effectively. Law. being a vast field. is intimidating but students should know that qualities of a lawyer can be acquired.

Challenges:~ Anyone who wants to pursue this field must understand that it could be a long time before you make any real money. and that is one of the biggest challenges faced by lawyers today. Young litigators are

severely underpaid. and bar associations should create fellowships for them.

Prospects:~ My advice would be to choose carefully who you work for; find someone who will teach you. pay you decently. and mentor your practice after you leave. Starting salary:~ A fresh graduate gets around Rs 1 lakh per annum. It takes a few years for increments to start coming through. While it's a fulfilling field to work in. you have to be prepared for disappointments.

Intellectual properties (IP) was indeed one of the subjects of interest at the time I was studying law at ILS Law College. Pune. While in college. I had the good fortune of being introduced to Neel Mason. Managing Partner of Mason & Associates. who had specialised in the field. and was. then working by way of one of the biggest IP law firms in India. I got a perspective on the subject. and the challenges that lay ahead. While still a student. I decided to pursue a career in Intellectual Properties Rights.

I felt drawn to the subject as a graduate in 1998. and the subject continues to fascinate me. IPR being a specialised area of law. the essential pre-requisite for any student is interest in the subject. A student desiring to excel in this field must have basic understanding of science. art. technology. industry. and commercial matters. One may also acquire these on the job. and perfect them over the years provided there is an interest in the subject. Besides. as required for any other area of law. one must possess analytical abilities. critical thinking. good communication skills. writing skills. and an eye for detail.

Challenges:~ One of the key challenges is to match the pace of development in law. This necessitates. among other things. regular reading. and awareness of law. amendments to the law in India. and elsewhere. cases. precedents. and development in the industry. A student must be prepared to continue reading. and learning. not forgetting that education begins once you join the profession.

Prospects:~ Students by way of degrees in science or engineering accompanied by a degree in law can consider a career in patents and/or design. litigation or prosecution. Students from a non-science background could consider trademarks. copyright. prosecution. licensing.. and litigation.

Starting salary:~ A fresh graduate typically gets paid in the range of Rs 4 lakh to Rs 5 lakh (per annum) in a big firm. and between Rs 2.4 lakh. and Rs 4 lakh (per annum) in a mid-sized firm.

CHAPTER-6
JUDICIAL RESPONSES IN CYBER LAW

CHAPTER-6

SOME IMPORTANT CASES CONCERNING CYBER-CRIMES IN INDIA

There have been various cases that have been reported in India. and which have a bearing upon the growth. and revolution of Cyber law in India. The present page encapsulates some of the important landmark cases that have impacted the evolution. and growth of Cyber law jurisprudence in India The following are some of the important cases impacting the growth of Cyber law in India

6.1 ARIF AZIM CASE

ArifAzim case was India's first convicted Cyber Crime case. A case pertaining to the misuse of credit cards numbers by a Call Center employee. this case generated a lot of interest. This was the first case in which any Cyber Criminal India was convicted. However. keeping in mind the age of the accused. and no past criminal record. Arif Azim the accused was sentenced to probation for a period of one year.

6.2 FATIMA RISWANA V. STATE REP. BY ACP.. CHENNAI & ORS AIR 2005 712.

The appellant is a prosecution witness in S.C. No. 9 of 2004 wherein respondents 2 to 6 are the accused facing trial for offences punishable under Section 67 of Information Technology Act. 2000 r/w Section 6 of Indecent Representation of Women (prohibition) Act. 1986. Under Section 5 & 6 of Immoral Traffic (Prevention) Act. 1956. Under Section 27 of Arms Act. 1959. and Sections 120(B). 506(ii). 366. 306 & 376 I.P.C. The

said trial relates to exploitation of certain men. and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos. and videos in various acts of sexual intercourse. and thereafter selling them to foreign websites. The said session's trial came to be allotted to the foreign websites. The said Session's trial came to be allotted to the V Fast Track Court. Chennai which is presided over by a lay Judge. When the said trial before the V Fast Track Court was pending certain criminal revision petitions came to be filed by the accused against the orders made by the said court rejecting their applications for supply of copies of 74 Compact Discs (CDs) containing pornographic material on which the prosecution was relying. The said revision petitions were rejected by the Madras High Court by its order dated 13th February. 2004 holding that giving all the copies of the concerned CDs might give room for copying such illegal material. and illegal circulation of the same. however the court permitted the accused persons to peruse the CDs of their choice in the Chamber of the Judge in the presence of the accused. their advocates. the expert. the public prosecutor. and the Investigating Office. and also observed that the case be transferred to another court by way of competent jurisdiction presided by a male officer at the option of the sessions judge. and taking the same the accused filed a revision petition for transferred to Fast track 4 court presided by the male officer. and the Appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer. and that the lady sessions judge didn't object or the trial of the case. and the Appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer. and that the Lady sessions

judge didn't object to the trial of the case in the fast track 4.22. and the high court has erred in transferring the case. and the Appellant was not given any opportunities of being heard before the alleged transfer. The learned counsel for the respondents contended that the Appellant learned though erred as witness is for all purpose an accused herself. and law officer appearing in the case had expressed their embarrassment in conducting the trial before a lady Presiding Officer. and even though the Presiding Officer did not expressly record her embarrassment. it was apparent that she too wanted the case to be transferred to another court. therefore. this Court should not interfere by way of the order of transfer. It was held that this appeal has to be allowed in the sessions case No. 9 of 2004 now transferred to the IV Fast Track Court Chennai be Transferred back to the V Fast Track Court. Chennai.

6.3 RITU KOHLI CASE - AN IPC CASE

RituKohli Case. being India's first case of cyber stalking. was indeed an important revelation into the mind of the Indian cyber stalker. A young Indian girl being cyber stalked by a former colleague of her husband. RituKohli's case - took the imagination of India by storm. The case which got cracked however predated the passing of the Indian Cyber law. and hence it was just registered as a minor offence under Section 509 the Indian Penal Code**.**

6.4 SANJAY KUMAR VS STATE OF HARYANA ON 10TH JAN. 2013 CRR NO.66 OF 2013 (O&M) 1

Present criminal revision has been preferred by the petitioner against judgment dated 21.08.2012 passed by the learned Sessions Judge.

Faridabad. whereby an appeal preferred by the petitioner has been dismissed. and judgment of conviction dated 01.09.2011. and order of sentence dated 03.09.2011 passed by learned Judicial Magistrate First CRR No.66 of 2013 (O&M) 2 Class. Faridabad. has been upheld. vide which the petitioner has been convicted for offences punishable under Sections 420. 467. 468. 471 of the Indian Penal Code. and Sections 64.22. and 66 of the data & Technology Act. 2000. and sentenced to undergo rigorous imprisonment as follows:~-

Under Section Period Fine 420 IPC Two years Rs.1.000/- 467 IPC Three years Rs.2.000/- Under 468 IPC Two years. and Rs.1.000/- Under 471 IPC Two years. and Rs.1.000/- 65 Under I.T. Act. Two years. and Rs.1.000/- 66 I.T. Act Two years. and Rs. 1000/- In default of payment of fine. the petitioner shall further undergo simple imprisonment for a period of two months. All the sentences were ordered to run concurrently.

6.5 STATE OF MAHARASHTRA V. ANAND ASHOK KHARE

This case related to the activities of the 23-year-old Telecom engineer Anand Ashok Khare from Mumbai who posed as the famous hacker DrNeuker. and made several attempts to hack the Mumbai police Cyber Cell website.

6.6 STATE OF UTTAR PRADESH V. SAKET SINGHANIA

This case which was registered under Section 65 of the IT Act. related to theft of computer source code. SaketSinghania an engineer. was sent by his employer to America to develop a software program for the company. Singhania. instead of working for the company. allegedly sold the source

code of the programme to an American client of his employer by which his employer suffered losses

6.7 STATE V. AMIT PRASAD

State v/s Amit Prasad. was India's first case of hacking registered under Section 66 of the Information Technology Act 2000. A case by way of unique facts. this case demonstrated how the provisions of the Indian Cyber law could be interpreted in any manner. depending on which side of the offence you were on.

6.8 STATE OF CHATTISGARH V. PRAKASH YADAV. and MANOJ SINGHANIA

This was a case registered on the complaint of State Bank of India. Raigarh branch. Clearly a case of Spyware. and Malware. this case demonstrated in early days how the IT Act could be applicable to constantly different scenarios.

6.9 STATE OF DELHI V. ANEESH CHOPRA

State of Delhi v/s Aneesh Chopra Case was a case of hacking of websites of a corporate house.

6.10 THE ARZIKA CASE

Pornography. and obscene electronic content has continued to engage the attention of the Indian mind. Cases pertaining to online obscenity. although reported in media. often have not been registered. The Arzika case was the first in this regard.

6.11 STATE OF TAMIL NADU V. DR L. PRAKASH

State of Tamil Nadu v/s Dr L. Prakash was the landmark case in which Dr L. Prakash was sentenced to life imprisonment in a case pertaining to online obscenity. This case was also landmark in a varieties of ways since it demonstrated the resolve of the law enforcement. and the judiciary not to let off the hook one of the very educated. and sophisticated professionals of India.

6.12 THE AIR FORCE BAL BHARTI SCHOOL CASE

The Air Force Bal Bharti School case demonstrated how Section 67 of the Information Technology Act 2000 could be applicable for obscene content created by a school going boy.

INTERNATIONAL ORGANIZATIONS

BATTLING CYBERCRIME

The global world network which united millions of computers located in different countries. and opened broad opportunities to obtain. and exchange information. is used for criminal purpose more often now a days. The introduction of electronic money. and virtual banks. exchanges. and shops became one of the factors of the appearance of a new kind of crime-transnational computer crimes. Today law enforcements face tasks of counteraction. and investigation of crimes in a sphere of computer technologies. and cyber crimes. Still. the definition of cyber crimes remains unclear to law enforcement. through criminal action on the Internet pose great social danger. Transnational characters of these crimes give the ground today in the development of a mutual policy to regulate a strategy to fight cyber crime. [44]

One of the most serious steps to regulate this problem was the adoption of Cyber Crimes Convention by European Council on 23rd November 2001. the first ever agreement on juridical. and procedural aspects of investigating of cyber crimes. It specifies efforts coordinated at the national. and international levels. and directed at preventing illegal intervention into the work of computer systems. The convention stipulates actions targeted at national. and international level. directed to prevent unlawful infringement of computer systems functions. The convention

[44]Vladimar Go lubev. International cooperation in fighting cybercrime; Co mputer Crime research Center.

divides cyber crimes into four main kinds:~ hacking of computer systems. fraud. forbidden content. and breaking copyright laws. [45]

By ways. and measures these crimes are specific. have high latency. and low exposure levels. There is another descriptive feature of these crimes. they are mostly committed only by way of the purpose to commit other more grave crimes. for example. theft from bank accounts. getting restricted information. counterfeit of money or securities. extortion. espionage. etc. [46]

There are various initiatives taken by the organization worldwide from time to time to control the growing menace of cyber crime. Some of the initiatives taken by various organizations are-

6.1 THE UNITED NATION

A resolution on combating the criminal misuse of data technologies was adopted by the General Assembly on December 4th. 2000[47] (A/res/55/63).[48] including the following

(a) States should ensure that their laws. and practice eliminates safe havens for those who criminally misuse data technologies.

(b) Legal systems should protect the confidentiality. integrity. and availabilities of data. and computer systems from unauthorized impairment. and ensure that criminal abuse is penalised.

6.2 THE COUNCIL OF EUROPE

[45]Carter D L. and A J Kat z. "Co mputer Crime:~ An emerging challenge for law enforcement. FBI Law rules bulletin http:~//www.fbi.gov/leb/dec961.t xt.

[46]Stambaugh. H.. et al. Electronic Crime needs assessment for state. and local law enforcement. National Institute of Justice Report. Washington. DC. US Department of Justice.

[47]The Global Legal Framework. The United Nat ion. http:~//wwwcybercrimelaw.net/content/Global/un.html.

[48]www.un.org.

Convention on Cyber Crime of 2001 is a historic milestone in the combat against cyber crime. Member states should complete the ratification. and other states should consider the possibilities of acceding to the convention or evaluate the advisabilities of implementing the principles of the convention. The council of Europe established a Committee of experts on crime in Cyber-space in 1997. The committee prepared the proposal for a convention on Cyber-crime.. and the Council of Europe convention on Cyber Crime was adopted. and opened for signatures at a conference in Budapest. Hungary in 2001. The total no. of ratifications/ accessions at present is 21.[49]

6.3 THE EUROPEAN UNION

In the European Union. the Commission of the European Communities presented on April 19. 2002 was a proposal for a council framework decision on attacks against data systems. The proposal was adopted by the Council in 2004.22. and includes Article 2:~ Illegal access to data Systems. Article 3:~ Illegal Systems Interference. and Article 4:~ Illegal Data Interference.

6.4 ASEAN

The Association of South East Asian Nations (ASEAN) had established a high level ministerial meeting on Transnational Crime. ASEAN. and China would jointly pursue a joint actions. and measure. and formulate a cooperative. and emergency response procedures for purposes of maintaining. and enhancing cyber-security. and preventing. and combating cybercrime.

[49]Albania. Armenia. Bu lgaria. Bosnia. Croatia. Cyprus. Den mark. France. Hungary. Netherlands. and USA among some of them.

6.5 APEC

The Ministers. and leaders of the Asia Pacific Economic Cooperation (APEC) had made a commitment at a meeting in 2002 which included. " An endeavor to enact a comprehensive set of laws relating to cyber-security. and cybercrime that are consistent by way of the provisions of international legal instruments. including United Nations General Assembly Resolution 55/63. and the Convention on Cyber Crime by October 2003.

6.6 G-8 STATES

At the Moscow meeting in 2006 for the G8 Justice. and Home Affairs Ministers discussed cybercrime. and issues of cybercrime. In a statement it was emphasized. "We also discussed issues related to sharing accumulated international experience in combating terrorism. as well as comparative analysis of relevant pieces of legislation on that score. We discussed the necessities of improving effective countermeasures that will prevent IT terrorism. and terrorist acts in this sphere of high technologies. For that it is necessary to set a measure to prevent such possible criminal acts. including on the sphere of telecommunication. That includes work against the selling of private data. counterfeit information. and application of viruses. and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality.. and we will need an international legal base for this particular work.. and we will apply all of that to prevent terrorists from using computer. and internet sites for hiring new terrorist. and the recruitment of other illegal actors."[50]

[50]http:~//www.usdoj.gov/criminal/cybercrime/g82004/ 97Co mmun ique.pdf

LAW TO KEEP PACE BY WAY OF EMERGING TRENDS

6.2.1 INITIAL LAW

India got its first codified Act in the Information Technology Act. 2000 ("IT Act). which fell far short of the Industry's requirements to meet global standards. The focus if the IT Act was however recognition of electronic records. and facilitation of e-commerce. Barely ten sections were incorporated in the IT Act to deal by way of Cyber Crime. At the time when the IT Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks. data theft. illegal access to data / accessing. and removal of data without the consent of the owner. etc.. were listed as civil penalties under the IT Act. The IT industry continued to rely on self-regulation. and contractual undertakings to appease its global clients. as it has done before the passing of the IT Act. The primary offences under the IT Act were :~

- Tampering by way of source code.
- Delecting. destroying or altering any data on any computer resource by way of mala fide intent to cause wrongful loss or to diminish its value.
- Publishing or transmitting pornographic material through a computer resource;
- Provisions pertaining to encryption technology the right of the Government authorities to intercept. and decrypt such data. and to call upon any entities or individual to decrypt such data were also

included in the IT Act. Certain acts affecting the integrity. and sovereignties of the nation were classified as offences.

The saving grace of the IT Act were the amendments carried dout to the IPC. and Evidence Act. which to some extent provided for prosecution of rampant offences like the Nigerian Scams. Phishing. and other Banking frauds may be prosecuted. Cyber Crime prosecution was however not resorted to in many instances due to lack of awareness (amongst both the victims. and the enforcement authorities) about the applicabilities of such general Laws to cyber crimes (like Phishing). To add to this. administrative delegation of powers treated offences under the IT Act differently to those falling under general laws.

Further. crimes like data theft. illegally accessing / removal of data. virus attacks etc. could not be prosecuted due to the lack of relevant penal provisions. Sec. 66 of the Act misleadingly titled "hacking" is one of the most misused. and abused provisions in India. Recently i.e. in September 2009 the Delhi High Court" has quashed the criminal proceeddings initiated in or about July 2004.22. under Sec.66 of the IT Act by M/s Parsec Technologies Ltd.. against some of its former employees. who left. and started their own Company. holding that the continuation of the proceedings would amount to abuse of process of Law. Likewise the IT ACt dis not give sufficient recourse for women. and child victims of cyber crimes like Cyber Stalking. and paedophilia.

Controversy has dogged the IT Act from its inception. The Ministry of Information Technology prepared. and posted proposed draft amendments

to the IT Act in 2004. In 2006 the IT Bill by way of substantial changes brought about as a result of the objections to the proposed amendments of 2005 was tabled before the Parliament.

In December 2008 as a knee-jerk reaction to the November 2008 terror attacks in Mumbai. India. the Information Technology (Amendments) Act. 2008 (Amendment Act 2008) was hastily tabled before the Parliament. and was passed hastily. and without any debate whatsoever. Unlike the IT Act of 2000. the focus of the new Amendment Act 2008is clearly on Cyber Terrorism. and to a significant extent. Cyber Crime.

6.2.2 Data Protection

The IT industry has been lobbying for a law to protect Data. and the new legislation hs addressed the industry's demands to a certain extent particularly since Mphasis Limited. a Pune based Company suffered the notireties of puncturing the Indian BPO fairly tale in April 2004. when some of its employees stole confidential credit cardd data of clients. and used it to siphon substantial amounts. Apart from highlighting the securities lapses within the Company. this case also brought to the limelight the lack of suitable Data Protection Laws in India. Several cases have now been reported where former employees are accused of data theft. and misuse of Confidential. and proprietary Information. and data. In one instance. a BPO Company purportedly closed down due to rampant data theft. The Indian Legislature's response to the hue. and cry raised is the transposition of certain civil penalties into criminal offences. and the addition of oen section under civil penalties as et out hereunder :~

The only provision under the IT Act for data protection was S43. which only imposed Civil Penalties in the event of the commission of certain acts without the permission of the owner or person in charge of the computer or computer systems such as (i) securing access (without permission). (ii) downloading or copying of data stored in a computer or computer system. (iii) introducing computer viruses. (iv) damaging computers. and or data stored therein; (v) disrupting computers. (vi) denial of access. (vii) abetting such acts. or (viii) illegal charging for services on another's account.

Sec 43A has now been added under the amendment act 2008to address the data protection requiremjent of the industry s43a stimulates that any "body corporate" possessing. Dealing by way of or handling any "sensitive personal data or information" in a computer resource it owns. Controls or operates. Is liable for negligence. If it fails to maintain "reasonable securities practicies andd procedures". And thereby causes wrongful loss or wrongful gain to any person. What amounts to reasonable securities practices. And procedures remains to be ffinalized by the central government.

Apart from the above addition under Civil penalties. the Civil wrongs set out under Sec 43 of the IT Act have now been qualified as criminal offences under the Amendment Act 2008 under Sec. 64.22. A reverse transposition has further been carried out under the Amendment Act 2008of two criminal provisions from the IT Act (Sec 66. and Sec. 65) as civil penalties under Sec. 43 (i) & Sec. 43 (i) respectively.

Any act set out under Sec. 43. if committed "dishonestly or fraudulently" would amount to a criminal offence. punishable by way of punishment of up ot three years or fine of a maximum of rupees Five Lakhss or both. under the Amendment Act 2008. Though Sec. 66 of the IT Act has purportedly been deleted. the addition of Sec. (43) under the Amendment Act 2008has in effect resulted in the retention of the contentious Sec. 66 of the IT Act. However retention of Sec. 65 of the IT Act without any modification despite its transposition into S43 appears to be a tautology. which could be due to oversight.

Sec. 66B inserted by the Amendment Act 2008 is on the lines of similar provisions in the Indian penal Code (IPC) which provides for punishment of the receiver of stolen properties Sec.66B makes the receipt or retention of a stolen computer resource or communication devidce punishable by way of imprisonment up to three years or by way of fine up to Rupees One Lakh or both. Whilst Sec.66B may seem to also apply to hardware. which is also covered under the IPC. the term "computer resource" is defined under the IT Act as a "Computer. computer system. computer network. data. computer database or software." The extension of the above provision to the receiver of stolen data. softwarer et. may prove to be substantially useful when faced by way of issues of Corporate Espionage.

6.2.3 DATA PROTECTION LEGISLATION

Although the data protection provisions introduced by the Amendment Act 2008 (as described above) may not comprehensively address the industry specific requirements applicable to data providers. and handlers.

nevertheless this is an important head start on introduction of specific data protection legislation in India. which is absolutely esse3ntial in todays's business environment.

One of the important outcomes of the Amendment Act 2008 amendments is the clarities on whether Data theft is considered a criminal offence. Commission of acts provided in Sec. 43 to 66 dishonestly or fraudulently. clearly implies "Data Theft" as an offence in such instances. However these acts would amount to a punishable offence only if such data is "downloaded. copied or extracted" from a computer resource. Therefore it may be argued that the provisions of Sec. 43 (b) are not inclusive as they do not give for removal of data through uploading. Criminal provisions give rise to liabilities only in cases of unambiguity. If a provision has to be applied through interpretation.. then such interpretation. which favours the Accused. would have to be applied.

When the addition of Sec.43A the Amendment Act 2008. the onus of implementing "Reasonable Securities Practices" is on the business entity. Whilst this may be a known liabilities that parties agree upon. unssupecting companies or firms may get mulcted by way of liabilities if duties. and obligations are not specified. as the Central Government guidelines will. then become applicable. As of now. violations under S43A are however not criminal offences.

6.2.4 CONFIDENTIALITIES & PRIVACY

India was shocked out of its complacent conservation due to the widespread circulation of a MMS clip shot by a Delhi schoolboy. This

case took an unexpected twist when this clip was circulated on Bazee com. and its Chief Executive Officer of American origin was arrested. Sec.66E has now been introduced under the Amendment Act 2008 for the protection of physical or personal privacy of an individual. This section makes intentional capturing of the images of a person's private parts without his or her consent in any medium. and publishing or transmitting such images through electronic medium. a violation of such person's privacy punishable by way of imprisonment of up to three years or by way of fine up to Rupee Two Lakhs or both.

A case of posting of the personal information. and obscence material on a Yahoo Site was touted as the fastest trials nd conviction of a cyber crime case in Chennai. It appears that this conviction has recently been reversed Sec.72A of the Amendment Act 2008 now explicitly provides recourse against dissemination of personal data obtained without the individual's consent thrrough an intermediary or under a services contract. by way of intent to cause wrongful loss or wrongful gain. The maximum punishment prescribed for this offence is three years imprisonment. or fine up to Rupees Five Lakhs or both.

Other Cyber Crimes including Cyber Terrorism

Provisions to combat frauds have now been introduced under the Amendment Act 2008. However certain issues relating to protection against banking fraids such as Phishing. money transfers through online hacking. email frauds. and cyber squatting (including though wilfully misleading domain names) to name a few have not been addressed

separately in the Amendment Act 2008. even though these are significantly increasing problems.

Sec.66C inserted by the Amendment Act 2008makes dishonest or fradulent use of a person's electronic signature or identity. password or nay other unique identification feature punishabvle as theft by way of imprisonment of up to three years. and fine up to Rupees One Lakh.

Sec.66D inserted by the Amendment Act 2008makes cheating by personating through a computer resource punisable by way of imprisonment of up to three years. and fine up to One Lakh rupees. It may be noted that S419 of IPC already provides for punishment for cheating by personating but does not give for the maximum fine imposable.

In addition to Sec.67 of the IT Act. Sec.67A. and Sec.67A have been included bythe Amendment Act 2008 inter alia to combat child pornography. Sec.67A makes transmission of a sexually explicit act or conduct punishable. and Sec.67B makes publishing. and transmission of child pornography an offence. punishments for which range from five to seven years. and fine. Several exceptions have also been set out to Sec.676. and Sec.67A including for depiction in any book. pamphlet. paper. writing. drawing. painting representation or figure in electronic form.

Further Sec. 67C introduced by the Amendment Act 2008 imposes liabilities on Intemediaries for retention. and production of information. However the duration manner. and fomats of retention of such data are still subject to prescription by the Central Government. This section appers to

be directed mainly against Cyber Cafes. and has already been subject to dissension. Failure to comply by way of such requirements is punishable by way of imprisonment up to three years. and also fine.

6.2.5 OBSERVATIONS ON THE CYBER CRIME PROVISIONS UNDER THE AMENDMENT ACT 2008

Sec. 43 was included in the IT Act. 2000 to address certain kinds of illegal acts. However. the Legislature has not looked beyond Sec. 43 to address recent trends in Cyber Crimes. and for dealing by way of such issues.

Sec. 66C of the IT Act. under the heading "Hacking" which was misleading was criticized for its ambiguity. and for the possibilities of abuse. However. whilst the proposed amendments sought for its delection. this section has been transposed to not only being applicable as a civil penalties but is also retained as a criminal offence. by way of the retention of S66 of the IT Act. one of the main issues that need to be addressed in the criminalities of actions resulting in "diminishing of value" of any data residing in a computer resource. Even if the law makers thought fit to retain this provision. its use. and abuse since 2000 ought to have been evaluated when redefining this provision.

Sec. 66C only addressed some kids of cyber frauds. and not all such frauds committed without using digital or electronic signatures. Further Sec. 66D may be considered redundant in the light of the amendments made to the IPC after the enactment of the IT Act in 2000. save. and except for the maximum fine imposable under the Amendment Act 2008.

Sec. 67A is a much needed introduction to the IT Act. and would help in combating the pernicious offences of child pornography as observed in some recent shocking incidents involving school children.

Several new provisions have been introduced under the Amendment Act 2008 to combat cyber Terrorims. These provisions appear to be a necessary have been introduced under the Amendment Act 2008to combat cyber Terrorism. These provisions appear to be a necessary. and welcome addition thought there are apprehensions about their abuse. and whether the Government authorities are well equipped to handle. and protect the information. acquired by it in compliance by way of such provisions.

6.2.6 ENCRYPTION & DATA PRIVACY

Mid 2008 customers in India thought twice about buying Blackberry phones - no reflection on the performance of the phones but due to a suddeen conflict between the Department of Telecommunication of the Indian Government ("DoT". and Research in Motion (RIM) Blackberry Services DoT requested RIM to share its encryption codes by way of the department stating securities concerns over data transmitted through email services on Blackberry phones or to set up servers in India. and permit DoT to monitor such transmissions. After several rounds of talks the Government of India dropped its request reversing its stand on the issue of a securities threat.

The Indian Telegraph Act. 1885 vests extensive. and absolute power on the DoT inter alia to deal by way of monitor. and regulate transmission of message within India. These provision therefore stand automatically

extended to transmission of encrypted Data also. The Guidelines issued by the DoT for transmisswion of encrypted data. and the ISP license requirements permits transmission of encrypted data of 40 bit key length in RSA algorithims or its equivalent in other algorithms without having to obtain permission from the Telecome Authority. However. if encryption equipment higher than this limit are to be deployed (which would be the case for most encrypted data) individuals/groups/organization require prior written permission of the "DoT. and may be further called upon to deposit the decryption key. split into two parts. by way of the DoT. these provisions appear to have prompted the Blackberry case. Now in addition to the above powers vested in the Telecom Authorities of India. certain Telecom Authorities in India.

6.2.7 OTHER RELEVANT PROVISIONS

With the increase in cyber crimes amounting to offences under the AMENDMENT ACT 2008 the power to investigate offences under this Act has been vested by way of an Inspector instead of the Deputies Superintendent of Police. This may reduce the confusion relating to jurisdiction for registered of offences. Further this would entail commencement of extensive. and immediate cyber law awareness measures by the investigation agencies throughout India. There is however anxieties in the minds of the industry about the abilities of the police official of such rank being able to handle such additional responsibility.

6.2.8 CONCLUSION

Though the Amendment Act 2008 has been passed by the parliament. the Amended Act is still not the law of the land. The Amendment Act 2008 will come into effect only from the date notified by the Government of India. which still remains pending as on the date of publication of this paper.

Introduction of several provisions in the IT Act by the Amendment Act 2008. relating to data protection. are extremely essential in today's business environment as several Indian companies providing services to or in conjunction by way of foreign entities handle large amounts of data that are accessed. and /or processed by the employees. Such cross border exchange/transmission of data further mandates compliance by way of the provisions of foreign enactment on Data Protection. The increased accountabilities of data handlers. and data aggregators. and the enhanced punitive measures therefore meets such requirements to some extent.

JUDICIAL DRAWBACKS & LACUNAE IN LAW

The ICT Trends of India 2009 have proved that India has failed to enact a strong. and stringent Cyber Law in India. On the contrary. the Information Technology Act 2008 (Amendment 2008) has made India a safe haven for cyber criminals. say cyber law experts of India. The problem seems to be multi- faceted in nature. Firstly. the cyber law of India contained in the IT Act. 2000 is highly deficient in many aspects. Thus. there is an absence of proper legal enablement of ICT systems in India. Secondly. there is a lack of cyber law training to the police. lawyers. judges. etc in India. Thirdly. the cyber security. and cyber forensics capabilities are missing in India. Fourthly. the ICT strategies. and policies of India are deficient. and needs an urgent overhaul. Fifthly. the Government of India is indifferent on the ICT reforms in India.

This results in a declining ranking of India in the spheres of e-readiness. e-governance. etc. While International communities like European Union. ITU. NATO. Department of Homeland Security. etc are stressing for an enhanced cyber security. and tougher cyber laws. India seems to be treading on the wrong side of weaker regulatory. and legal regime. Praveen Dalal. Managing Partner of Perry4Law. and the leading Techno-Legal Expert of India sent an open letter to the Government of India including the Prime Minister of India.

President of India. Supreme Court of India. Ministry of Parliamentary Affairs. etc. and brought to their attention the growing menace of cyber crimes in India. At last. somebody in the government has shown some concern regarding the growing menace of cyber crimes in India.

However. the task is difficult since we do not have trained lawyers. judges. and police officers in India in respect of Cybercrimes. However. at least a step has been taken in the right direction by the law minister of India.

Police in India are trying to become cyber crime savvy. and hiring people who are trained in the area. The pace of the investigation however can be faster. judicial sensitivity. and knowledge needs to improve. Focus needs to be on educating the Police. and district judiciary. IT Institutions can also play an integral role in this area. We need to sensitize our prosecutors. and judges to the nuances of the system. Since the law enforcement agencies find it easier to handle the cases under IPC. IT Act cases are not getting reported. and when reported are not dealt by way of under the IT Act. A lengthy. and intensive process of learning is required. A whole series of initiatives of cyber forensics were undertaken. and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems are invented. We need to move faster than the criminals. The real issue is how to prevent cyber crime. For this there is a need to raise the probabilities of apprehension. and conviction. India has a law on evidence that considers admissibility. authenticity. accuracy. and completeness to convince the judiciary. The challenges in cyber crime cases include getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation by way of specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of

crime. is the same that has been analysed. and reported in the court based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance. and the will to fight it.

Criminal Justice systems all over the world. must also remember that because of certain inherent difficulties in the identification of the real cyber criminal. cybe r law must be applied so as to distinguish between the innocent. and the deviant. A restraint must be exercised on the general tendency to apply the principle of deterrence as a response to rising cyber crime. without being sensitive to the rights of the accused. Our law makers. and the criminal law system must not forget the basic difference between an accused. and a convict. There is only a delicate difference between the need to ensure that no innocent is punished. and the need to punish the cyber criminal.

Thus lastly. there were two research questions which were proposed by the researcher for the purpose of the project. The first one being. is the Information Technology Act. 2000 effective. and efficient enough for controlling the recent developments in Cyber Crimes in India? The Hypothesis for the question was „No". and it has been proved.

The second research question was. Will the recent proposed amendment to the Information Technology Act. 2000 answer the contemporary complications in the cyber crime arena in India? The hypothesis for the same was „No". and to conclude the researcher has proved it.

CHAPTER-7

CONCLUSION AND SUBMISSION

CHAPTER-7

CONCLUSION AND SUBMISSION

1 INTRODUCTION :~

Technology development is very high. India is on the top of the world. India has shown path in software. Internet. and Electronic Associated subject. But India is lagging behind in making laws. modifying these. and throwing away the old laws.

There is exponential growth in law. and technology in India. and World over. But we are lagging behind in law making. There are three following characteristics in India :~-

2 LAGGING BEHIND IN LAW MAKING

Drafting the laws starts in India only when lot of water has flown down in river Ganges. It is unfair. We have to formulate our thinking well ahead of occurrence of events. Law must closely move along by way of development of technology. It is not happening. My feeling is that the lawmakers should take up. and large gap of time existing now should be reduced to minimum.

3. LIVING BY WAY OF CENTURY OLD LAWS

We believe in living by way of old laws very happily when these are centuries old. and others well beyond. This is not adequate. We must be quick enough to discard the old ones. and adopt new ones.

4. MODIFICATION OF LAWS IS CARRIED OUT VERY LATE.

Issue of amendments of laws is taking a long time. We should be sensitive to issue the amendments. We must have synchronization of events in India & abroad by way of law.

4 DRAFTING OF LAWS

This attitude of legging behind in law framing. lacking courage to modify law by way of the happening of events in India. and world over. and finally not discarding of. and replacing century old laws should change so that Indian societies feels proud. and tuned to current legal laws to handle current matters.

BIBLIOGRAPHY

BIBLIOGRAPHY

PRIMARY SOURCES :~

Bare Act

- Information Technology Act. 2000
- Indian Telegraph (Amendment) Act. 2003
- Indian Penal Code. 1860
- Copyright Act. 1957
- Patent Act. 1970

List of Report

- United Nation Commission
- The Council of Europe Convention
- The European Commission
- Asian of South East Asian Nations
- Asia Pacific Economic Corporation

SECONDARY SOURCES :~

Books:~

- Andrew Grant-Adamson. Cyber Crime. Mason Crest Publishers. 2003.
- David Bowen. Viruses. Worms. and Other Nasties. Protecting yourself online; Department of Inter discplinary Studies. 2003.
- Dudeja V D. Crimes In Cyberspace- Scams. and Frauds (Issues. and Remedies) Commonwealth Publishers. New Delhi. 2003.
- Eric S. Raymond:~ A Brief History Of Hackerdom (2000)
- John Townsend. Cyber Crime. Raintree. 2004.
- Laura E. Quarantiello. Cyber Crime:~ How To Protect Yourself From Computer Criminals. Tiare Publications. 1994.22.

- Smith RG. Grabosky PN. and Urbas GF 2004. Cyber criminals on trial. Camridge Universities Press.
- Stambaugh. H.. et al. Electronic Crime needs assessment for state. and local law enforcement. National Institute of Justice Report. Washington. DC. US Department of Justice.
- Tan. Koon. Phishing. and Spamming via IM. Internet Storm Center. December 5th. 2004.22.
- Vladimar Golubev. International cooperation in fighting cybercrime; Computer Crime research Center.
- Cyber Crimes - Dr. Talat Fatima. Eastern Book Company.
- Cyber Law - Mr. Anirudh. Rastogi. Nexis.
- Information Security. and Cyber Laws - K.K. Singh & Akansha Singh. Umesh Publication.
- Introduction to data Security. and Cyber Laws - S.P. Tripathi. Dream tech.
- Cyber Laws - Aparna Vishwanathan. Lexis Nexis.
- Stambaugh. H.. et. al. Electronic Crime needs assessment for state. and local law enforcement. National Institute of Justice Report. Washington. DC. US Department of Justice.

Articles:~

- Adam.. and McLaughlin. Charles. “Malware:~ What It Is. and How To Prevent It” Ars Technical. 2004. http:~//www.ncsl.org/programs /lis/cip/ viruslaws.html.

- Aderucci. Scott. Salami Fraud. www.all.net/CID/attack/papers/Salami .html..
- B. Michael Hale. Salami Attacks. http:~//all.net/CID/Attack/papers/Salami2.html.
- Buskin J. The Webs Dirties Secret. Wall Street Journal. Available:~ Proquest:~ ABI/ Inform Global. 2000.
- Carter D L. and A J Katz. "Computer Crime:~ An emerging challenge for law enforcement. FBI Law rules bulletin http:~//www.fbi.gov/leb/dec961.txt.
- Carter David L Computer Crime Categories. How Techno Criminals Operate. FBI Law Enforcement Bulletin. July. 1994.22.
- Tan. Koon. Phishing. and Spamming via IM. Internet Storm Center. December 5th. 2004.22.
- Vladimar Golubev. International cooperation in fighting cybercrime; Computer Crime research Center.

ELECTRONIC SOURCES :~

Websites :~

- http:~//cybercrime.planetindia.net/worms.html.
- http:~//etd.rau.ac.za/thesis/available/etd-05252005-120227/resticted/AppendixA.pdf.
- http:~//webzone.k3.mah.se/k3jolo/HackerCultures/origins.htm
- http:~//www.asainlaws.org/Cyber-law/library/cc/what_cc.html.
- http:~//www.asianlaws.org/Cyber-law/library/cc/what_cc.html.
- http:~//www.cert.org/advisories/CA-1997-28.html.
- http:~//www.cert.org/tech_tips/e- mail_bombing_spamming.html.

- http:~//www.cyberpolicebangalore.nic.in/cybercrimes.htm
- http:~//www.financialexpress.com/news/Cyber-crimes-cost-Indian-firms-Rs-58-lakh- in-2009/588864/
- http:~//www.lse.ac.uk/itservices/help/spamming&spoofing.html.
- http:~//www.mailsbroadcast.com/e-email.broadcast.faq/44.22.e-mail.spoofing.html.
- http:~//www.nrps.com/community/comprev.asp.
- http:~//www.uncitral.org/english/texts/electcom/.
- http:~//www.usdoj.gov/criminal/cybercrime/g82004/97Communiq ue.pdf.
- http:~//www/fbi.gov/quickfacts.htm
- http:~//www/trai.gov.in
- Introduction to Cyber Crime.
- http:~//cybercrome.planetindia.net/cybercrime_cell.htm
- Kabay. M E Salami fraud. www.nwfusion.com/newsletters/sec/2002/01467137.html
- Love. David. Cyber Terrorism:~ Is It A Serious Threat To Commercial Organisation? www.crime-research.org/news/2003/04/Mess0204.html.
- M E Kabay. Logic bombs. Part 1. Network World Securities Newsletter.
- Meaning of logic bomb. http:~//en.wikipedia.org/wiki/logic_bomb.
- Ollmann. Gunter. The Phishing Guide:~ Understanding. and Preventing Phishing Attacks:~ Technical Info. 2004.22.

- Rohas Nagpal. Asian School of cyber Law. http:~//www.asianlaws.org/press/esecurity.html.
- SamuelJay Keyser. "Where The Sun Shines. There Hack They". http:~//hacks.mit.edu/Hacks/books/articles/where_the_sun_shines.html.
- The Computer Ethics Institute. a leader in the field. has comprised a guideline to help computer users in their ethical decisions. They have called this guideline "The Ten Commandments". http:~//www.computerethicsinstitute.org/images/TheTenCommandmentsofComputerEthics.pdf
- The Global Legal Framework. The United Nation. http:~//wwwcybercrimelaw.net/content/Global/un.html.
- Tom Merritt. What is Email Spoofing? See www.g4tv.com.
- Understanding Denail of Service Attacks (US CERT). http:~//www.us-cert.gov/cas/tips/ST04-014.22.html
- US Department of Justice. Criminal Division. Fraud Section. http:~//www.usdoj.gov/criminal/fraud/internet.
- www.cybercrimelaw.net/content/history.html.
- www.symantec.com/content/en/us/about/.../SES_report_Feb206.pd
- wsww.un.org.