"CYBER CRIME AND CYBER TERRORISM IN INDIA"

DISSERTATION

Submitted in the Partial Fulfillment for the Degree of

MASTER OF LAW'S (LL.M.)

SESSION: 2019-20

BBD UNIVERSITY

UNDER SUPERVISION OF:

Ms. Sonali yadav
Associate Professor
SoLS,BBDU

SUBMITTED BY:

Lubna Bano
Roll No.1190997032
LL.M II Semester
CRIMINAL AND SECURITY LAW

BABU BANARASI DAS UNIVERSITY LUCKNOW

DECLARATION

Title of Project Report **"CYBER CRIME AND CYBER TERRORISM IN INDIA"**

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

LUBNA BANO

I declare that

(a) The work submitted by me in partial fulfillment of the requirement for the award of degree **LLM** Assessment in this **DISSERTATION** is my own, it has not previously been presented for another assessment.

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

(c) I have not used this work previously produced by another student or any other person to submit it as my own.

(d) 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.

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

LUBNA BANO

Roll No.1190997032

Date:-…..

LL.M. (2019-20)

ACKNOWLEDGEMENT

I acknowledge the heartfelt thanks to the Institute of legal Studies, **Babu Banarasi Das University Lucknow** to provide me the opportunity to complete my dissertation for the Partial Fulfillment of the Degree in Master of Laws.

I am thankful to my Supervisor **Ms.Sonali yadav, Ma'am** for not only helping me to choose the dissertation topic but also for his valuable suggestions and co-operation till the completion of my dissertation. He 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.

Thank you

Lubna bano
LL.M. (Criminal and Security Law)
Roll No.1190997032
School of Legal Studies
BBDU

ABBREVIATIONS AND ACRONYMS

$	Dollar
£	Pound
3GPP	3"'^ Generation Partnership Project
AIR	All India Reporter
AVI	Audio Video Interleave
CD	Compact Disk
CDA	Communication Decency Act
CEO	Chief Executive Office
Cr. PC	Code of Criminal Procedure
DSCI	Data Security Council of India
ICCIS	International Code of Conduct for Information Security
IGC	Institute for Global Communications
FBI	Federal Bureau of Investigation
FLV	Flash Live Video
GGE	Group of Governmental Experts
GIF	Graphic Interchange Format
HC	High Court
SC	Supreme Court
SCC	Supreme Court Cases
Sec.	Section
ICT	Information Communication Technology
IGC	Institute for Global Communications
IGNOU	Indira Gandhi National Open University
IP	Internet Protocol
IPC	Indian Panel Code
IT	Information Technology
www	World Wide Web

TABLE OF CASES

R. v. Woods

Rajagopal v. State of Tamil Nadu

Ranjid D. Udeshi v. State of Maharashtra

Rayala M. Bhuvaneswari v. Nagaphanender Rayala

Regina v. Hicklin

SMC Pneumatics Ltd. v. Jogesh Kwatra

Smt. Mathri v. State of Punjab

Tata Sons Limited v. Greenpeace International & othr

The Hearst Corp. v. Goldberger

US v. Thomas and Minnesota v. Granite Gate Resorts

Vinod Kaushik and Ors. V/s Madhvika Joshi and Others.

Zippo Manufacturing Company v. Zippo. Com, Inc

Zippo Mfg. v. Zippo Dot Com. Inc

Table of Contents

CHAPTER I
INTRODUCTION

1.0 INTRODUCTION

Cyber crime is a crime which involves the use of digital technologies in commission of offences, directed to computing and communication technologies. The modern techniques that are proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity.

The rapid development of internet stands as an example of such change, just ten years ago it was in its infancy, yet it is now a fact of life for billions of people around the globe. It has brought in its wake significant changes in the ways we work, trade, study, learn, play, consume,
Communicate and interact. At the same time, a whole host of crime problems has emerged in
tandem with life online. The activity involves like attacking on information center data system, theft, child pornography built image, online transaction fraud, internet sale fraud and also deployment in internet virus, worn and third party abuse like phishing, email scams, hacking, spoofing, phishing viruses, Trojans, malware, piracy, downloading, spyware, chat room grooming, and so on.

The internet has opened up a world of opportunities in e-commerce and information sharing, on the flip side the internet has its own threats and abuses which are perpetrated by a new breed of criminals known as cyber criminals. Just as you know that our world is unsafe and criminals lurk in dark alleys, in the cyber space too criminals lurk and the danger is all the more high with new and novel methods employed by cyber criminals. With the internet being touted as no one being in-charge and one can do whatever one wants, cyber criminals started having a field day with a range of crimes like cyber terrorism, cyber stalking, cyber warfare, invading your privacy, cyber pornography or obscenity etc.

Computers and therefore the Internet still pervade human life in everything from automobiles to kitchen appliances. With the invention of computers, its increasing use and human dependency over Internet, while we've gained manifolds in terms of efficiency and management, it's also delivered to the front many negative effects and drawbacks . Individuals or groups can now use Cyberspace to threaten International governments, or terrorize the citizens of a Country. The crime of "cracking" can escalate into terrorism when a private "cracks" into a government or military-maintained website. Cyber-terrorism might be hacking into a hospital computing system and changing someone's medicine prescription to a lethal dosage for an act of revenge.

Good and bad has co-existence since the beginning of the world. Where first one comprises all things which are essential for wellbeing of all whereas other ones connotes negativity. Unfortunately technology cannot be mention as an exception of this rule. The internet and its technologies have opened up many opportunities for all countries to develop their economies. On one hand our scientist, technocrats are using this advanced stream of science for betterment of all and to make India self-dependent and secure from attack of our enemies while on the other hand a very well structured groups (Independent or Nation sponsored) are also using these technologies as a tool to make INDIA weak and helpless. Cyber criminals perform various acts like cyber stalking, on-line harassment, on-line defamation, hacking, and so forth collectively we call it cybercrime. When these activities are managed by organized group systematically and deliberately we term it as CYBER TERRORISM. Cyber terrorism is a well-planned and organized use of technologies by cyber experts resides inside and outside the country for anti national activities. Although our government is well capable to fight against such challenges it requires support, awareness and alertness from people.

1.1 Evolution of computer Industry

Charles Babbage of England is considered as the father of modern computer technology who in 19th century conceived an idea to develop the computer by mechanical assignment of shafts. However, this idea did not materialize immediately and it took nearly a century to develop a digital computer with highly precision devices. George Steinitz of Bell Labs made the first successful attempt by using teletype tape which contained information (the pattern of holes in the top) that could be read at approximately ten “digits” per second. The chief characteristic of the tape tester was the use of binary code instead of the decimal system still in use in other machines and use of electric storage. This binary code was afterwards used by George Steinitz in telephone U-type relay which saw a series of modifications at Bell Labs from the late 1930’s to the mid 1940’s. Each device produced during this period showed improvement over the earlier one with the main difference that earlier devices were mainly used for calculations of complex numbers, whereas the models produced afterwards introduced a logic unit using the operators IF, OR, AND THEN. Another stage of development was reached with the finding that the calculation devices and the money storage need not to be equivalent in structure. Thus, John At an or off of Iowa Stage College, concentrated on the use of recharging capacitors for dynamic

memory storage and vacuum tubes for calculating processing. He succeeded in developing the first "electronic" computer, the ENIAC composed of 18,000 vacuum tubes and 6000 flip flop switches that were either on or off.[1] These vacuum tubes need high voltage of power that was producing undesirable heat and also resulted in frequent tube failure. This heralded the introduction of the transistorized computer. This made a first significant development in the computer technology. The transistor is less than but similar to a pea containing three wires embedded in a drop of semi-conductor material.[2]

1.2 History and development of Internet

"No words can better describe the present scenario of technology than the following stated by Cosmos-the villain in the movie **"Sneaker".**

The world is not run by weapons any more energy or money. It is the run by ones and Zeroes-little bits of data. It is all electrons. There is war out-a world war. It is not about who has the most bullets. It is about who controls information. What we see and hear, how we work, what we think. It is all about information. (Sneakers MCA/Universal, 1992).

In a development world present generation cannot imagine a life without computers .The new Development are posing challenges to the fundamental principles f law, which worked well before the advent of this technology. The problems have been compounded by the introduction of internet. There is already debate whether entirely new laws should be framed or whether old laws may be effectively adopted to address these new issues.[3] In a Digital world everything is recorded in digits, without any respect for political boundaries and can be modified, altered and replaced without any murmur. There is a genuine feeling that the new world of digits demands training not only to the Bench and Bar but also to Law enforcement agencies as new language has been introduced which has given new meaning to old words.

1 See Lurens R Schwartz, computer law hand book p.g1
2.Michael D.Rostoker, Rober H. Rines; computer jurisprudence p.8
3.See Kent D. Stuckey, Internet and on line law (4th ed. 1999)

Internet has transformed the world into a Global Information Village. Internet made this world a virtual sleepless global market place. Internet is a global network of computer. Internet and online services, sometimes called as new media services as in many respects similar to the traditional media as it also includes production oriented material such as music, audio, video, graphics, text and games. It works in communication forms also likewise messaging, chatting, video conferencing etc.

The internet's roots can be traced from 1950's. In 1957 the Soviet Union launched tiles First Satellite, Sputnik I, triggering US president Dwight Eisenhower to creating the ARPA agency to arms race. So, the evolution of internet can be said to be started with the use of ARPANET sponsored by US mystery, which was set up in 196913. The first communication touch place between research Center at the University of California at Los Angles and the Stanford research Institute. The ARPANET was as joint venture of Massachusetts Institute of Technology and the American Department of Defense Advance Research Project Administration as a source to establish continued communication between remote computer resources in the event of war. The communication links were confined to military, defense contractors and university laboratories involved in defense related research.

In early 1970's further innovations took place, such as electronic mail possibilities have grown. During this period other network equivalent to ARPANET being established such as the United Kingdom's Joint Academic Network (JANET) and the United States National Science foundation Network (NSENET)[4].

In the year 1990 the US authorities released ARPANET and transferred it to National Science Foundation network (NSFNET). In the year 1993 Time Bemers-Lec's he is the person who developed the World Wide Web (www) in the European Laboratory for particle physics (CERN). The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet explorer the preceding year. So, there browsers made Internet access possible from personal computers. From the year mid 1990's various commercial Internet Services Providers (ISP) entered the market and offered the Internet connection through conventional telephone line[5].

4. Majid-Yar, Cybercrime & Society ed-l"2006, New Delhi, SAGE India Publication Pvt. Ltd., p-7
5. Ibid, PP.7&8.

On 24 October, 1955 Federal Networking Council (NFNC) unanimously passed a resolution defining the term Internet. This definition was developed in consolation with members of the Internet and Intellectual property Rights communities. The term internet defined as: "Internet" refers to the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extension or follow-on's (ii) is able to support communications using the transmission control protocol/internet protocol (TCP/IP) suit or its subsequent extensions/follow-on, and or other IP compatible protocols and (iii) provides, uses or makes accessible either publicly or privately, high level service layered on the communications and related infrastructure described herein.

1.3 Statement of the Problem

- The real issue is how to prevent cyber crime?
- For this there is a need to raise the possibility 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 smithy in a foreign court.
- For this India needs total international cooperation with specialized agencies of different countries. The police have to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analyzed and the report presented in court is based on the evidence. It has to maintain the chain of custody.
- Besides above mentioned problem or issue, the other issue is that the threat is not from the intelligence of criminals, but from our ignorance and what is needed is the will to fight it.
- The law is stricter now on producing evidence. Specially where electronic documents are concerned.
- Under Indian Law, cyber crime has to be a voluntary and willful act or omission that adversely affects a person or property.
- The Information Technology Act 2000 provides the backbone for e-commerce and India's approach has been to look at e-governance and e-commerce primarily from the proportional aspects. Looking at the vast opportunities and the need to sensitize the population to the

possibilities of the information age, there is a need to take into consideration the security aspects.

- In the present global situation where cyber control mechanisms are important, we need to push cyber laws.
- Police in India are trying to become cyber crime savvy and hiring people v/ho are trained in the area. Many police stations in various parts of India have computers, which are connected to their respective head quarters.
- Cyber police stations are functioning in major cities all over the country. The pace of the investigations can become faster, judicial sensitivity, and knowledge need to improve.
- Focus is needed to sensitize our investigators and judges to the importance of the system.

1.4Objective of the study

The objective of the present study are follow.

- ❖ The main object is to specify the e-danger. The legal world familiar with theft and murder but now it is smuggling to macro terrorism from selling secrets to subverting systems from hijacking to hackling. The face of time has undergone a big change, its definition has changed its modus operendi has changed and the perpetrators are no longer Lombroso's bearded and hard looking criminal but a white collar criminal a fiddler or by an egomaniac. Determine the safety networks particles on prevent cyber Terrorism and Analyze the impact of the Attack.

- ❖ The object of this research is to highlight the formidable problems face by the legal world, which have raised their heads due to information explosions. If cyber space is left ungoverned, it will lead to disastrous end where cyber space shall turn into veritable Siberia where greed, gambling, pornography and sex will reign supreme. The object is therefore to circumscribe within the limits of research work problem like jurisdiction question, overlapping of laws, multiplicity of laws, transnational nature of cyber crimes and various problems relating to investigation and lack of visual evidence.

- Emphasis has been made to educate the investigating officers, prosecutors and judges about the need for amending the existing provisions of penal law to ensure efficiency prosecution and trials.

- Measures adopted by various countries including the U.S. the home land of the internet other western countries having a high standard of connectivity and convergence are more vulnerable to cyber crime, thus they have a good number of cyber acts. India too passed IT Act 2000 and other relevant Acts. The object is to analyse various legislations in this area and to explore the possibilities of a stricter
  legal framework.

1.5 Need of the study

The term "cyber crime" and "cyber terrorism" at the present time, many organization have made efforts to combat this threat. Since cyber terrorism is an International crime, local regulations alone are not able to defend against such attacks. There are various laws in Indian scenario keeping in mind the position of cyber crime in India. Therefore, this dissertation needs to study the sanerio of cyber crime and cyber terrorism in India and to eradicate loopholes in best possible ways.

1.6 Hypothesis

The research carried on the following hypothesis;

There is no comprehensive legislation in our country which deals with cyber crimes. Cyber crime has entered into popular demonology and today no one can claim to remain in affected
by it as individuals, business organizations, governments & states all are in the net.

The judicial system in our county is not conducive to affective enforcement of any law as a
result the laws have failed to achieve their objectives. Our legislature is yet to respond to

Seriousness related to cyber crimes.

Computer and Information technology revolution has brought in unprecedented advantages to the society. The exponential growth of internet has change live of the people. There is no sphere of human endeavor, which remains untouched by the information technology while the technology is ushering in all round economic progress, bestowing great benefits to the humanity. The criminal activities are not lagging behind; suddenly a set of new criminal activities called cyber crimes has become a new challenge to the society. No longer the nation states can sit and watch this phenomenon. In some aspects computer crime is much more dangerous than traditional crime. It is easy to commit and difficult to prevent.

i) It is hypothesized that the law has prohibited the phenomenon of cyber crimes but the operation of law has no preview over the cyber criminals.

ii) Cyber crime is a socio legal problem and various difficulties arise in investigation and legal framework. So there is a need of a sufficient legislation to prevent this social evil.

iii) How the internet has become a dangerous area for children and finally strategies, nations are adopting in combating this crime.

iv) That despite of adequate safeguards and number of legislations the problem of cyber crime continues unabated because of the poor machinery in our country and the major problem of jurisdiction.

v) The problem is multi-fold and it covers the crime related to economy as well as other crimes such as pornography which has its basis, certain moral standards and uses parameters like indecency and obscenity.

1.7 Research Methodology

Law is a normative science that is, a science which lays down norms and standards for human behavior in a specified situation or situation enforceable through the sanction of the state. What distinguishes law from other social science is its normative character. This fact along with the fact that stability and

certainty of law are desirable goals and social values to be pursued, make doctrinal research to be of primary concern to a legal researcher. Doctrinal research, of course, involves analysis of case law, arranging, ordering and systematizing legal propositions, and study of legal institutions, but it does more it creates law and its major tool (but not only tool) to do so is through legal reasoning or rational deductions. The present study is based on the doctrinal method of research. The researcher has drawn help from various books, Articles, newspapers, gazettes, report of commissions and committees and judicial decisions.[6]

1.8. Literature Review

The literature available on the subject reveals that there are a number research studies being conducted on the cyber crime and its impact on the society. Most of the studies have tried to find out the menace of cyber crime and its possible control through the available legislation. The studies tried to find out that, how the cyber crime are committed and what are the distinctive modes of controlling them in the interest of the society. Another important observation is that an over helming number of studies have adopted the method of content analysis.

R. K, Chaubey (2009)[7] Cyber crime is the latest type of crime which affects many people. It refers to criminal activity taking place in computer networks, knowingly or intentionally, access without permission, alters, damage, deletes and destroys the database available on the computer or network. It also includes the access without permission to the database or programmed of a computer or network in order to devise or execute any unlawful scheme or wrongfully control or
Obtain money, property or data. It poses the biggest challenge for police, prosecutors and Legislators.

Justice Yatindra Singh (2012).[8] The proper analysis of Cyber Laws, the author lucidly explains the science behind the technology in order to sort out the legal issues. The internet has introduced another

6 Jain, S.N., 'Doctrinal and Non-Doctrinal Legal Research.' Indian Law Institute Journal. Vol.17*, 1975, p. 519.
7 An Introduction to cyber crime & cyber law. ed-2008, Kamal Law House, Kolkata, 2009.
8 Cyber Law Jain Book, New Delhi, 2012.

technology known as webcasting or internet broadcasting which involves streaming of audio/video on internet called internet radio. These are retransmission of over the air broadcasts through internet. The internet has brought forward a new class of persons, known as intermediaries, who provide physical facilities to transmit or route the information, also known as Internet Service Providers. The study is an asset to companies dealing in computer software or providing software solutions, web page providers, Internet service providers, Banks, Insurance companies and other bodies providing online services, government departments implementing information technology, police officials dealing with investigation of cybercrimes, teachers, students, lawyers and judges.

Vakul Sharma (2004)[9] the study comprise of numerous illustrations, concept notes and examples make the subject interesting and comprehensible. It attempts to interpret the true legislative intent behind the Act by referring to and applying the Supreme Court judgments for better assimilation and understanding of its various provisions relating to cyber crime. The author has tried to assimilate the thoughts of Judges, Lawyers, Civil Servants, Police Officers, Technocrats and Students whom he met during his public lectures, discussions, workshops, seminar across the length and breadth of the country over the past many years. The critical appraisal of powers and functions of the Cyber Regulatory Appellate Tribunal,Controller of Certifying Authorities, Adjudicating Officers and Police Officers under the Information Technology Act has been attempted.

Chris Reed (20007)[10]**.** Other available materials on Internet Law explain the law of a particular country. This work is unique in that it examines the law globally. Its main importance is its fundamental analysis of legal problems and principles which are common to all countries. From the analysis of the book supra the researcher have been able to understand the true nature of a particular legal problem, and thus be able to research and apply the appropriate national law rules to that problem.

Nandan Kaniath (2008)[11]**.** Internet has emerged as a medium with immense potential, posing many new and interesting challenges. There have been many attempts to regulate and control this medium, especially through the laws and regulations. This exciting publication explores the various aspects of cyber law and

9 Information Technology law and Practice: Cyber Law & E. Commerce. Universal Law Publishing Co.Pvt. Ltd. Delhi, 2004.

10. Internet Law Text and Materials. Butterworths, London, 2000.

11. Law relating to Computes, Internet and E-commerce. ed.-2"", Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2008.

cyber regulations, taking the reader through a multitude of legal and policy issues that the Information Age poses. Topics covered in this book range from evidentiary aspects and digital signatures to intellectual property concerns such as copyright liability and rights in domain names; from cyber crime and cyber pomp to the regulation of free speech on the Net and the right to privacy. A new chapter on Cases on Computers, Internet, email etc. has been added. Employing a comparative law approach, this book, in its fourth edition, not only takes into consideration the changes brought about by the Information Technology Act of 2000, but also contains the latest developments along with a comprehensive guide to this legislation. Being wide-ranging as well as in depth in its coverage of Indian Cyber law, this publication is a must-read for judges, lawyers, Policy makers, researchers, investigators and students as it is for anyone who would like to keep abreast of new developments in the legal system, concerning Information Technology.

Pavan Duggal (2013). The emerging developments in cyber law along with the dark side of Internet and the World Wide Web and its consequent legal consequences have made the thing Interesting in understanding the cyber crime and its control mechanism. Cyber law is a phenomenon has evolved in our own lifetimes. In the last decade and a half, huge developments have taken place which impacts every user of a computer, computer resource and communication device. Cyber law is one of the latest and most complex disciplines of legal jurisprudence.

CHAPTER II

CONCEPT OF CYBER CRIME

Cyber crime

2.0 Introduction

Presently in India as well as in the world the computers have become an emerging part of the fast developing society. The computers are being used in various aspects such as in Banking, Manufacturing, health care, defense, insurance, scientific research, strategic policy making, law enforcement etc[12].

If we think presently about the society without the computer everything seems to be impossible for example Railway Ticketing system. Airline Ticketing as well as traffic control. Electricity bill, Telephone Bill office works etc, all are seems to be impossible without the computer.
Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The internet is like life in the real world being extended and carried on in another medium that cuts across boundaries space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. Every coin has two side likewise, internet having all benefits of anonymity, a liability, and convince has become as appropriate place for pensions interested in making are of the net for illegal gainful purpose, either monetary or otherwise[13].

Internet has transformed the world into a Global Information Village. Internet has also made this world a virtual sleeper's global market place. History is a witness to the most fact that all the technological inventions have been put to as much destructive use as constructive one. Information technologies are no different, while good people are using Information technology for finding better alternatives which can improve the quality of human life while bad elements are using it for harming individuals, cheating others of their hard earned money, subverting and defrauding the business and to hide their crimes[14]

12 Dr Gandhi, K.P.C, 'Introduction to computer: related crimes.' Delhi, CBJ Bulletin. 1996, p.6.
13 Verma, S.K. & Mittal, Legal Dimensions of Cyberspace. New Delhi, ILI Publisher, 2004, p. 228.
14 Cloniel Prasad, R.S, Cybercrime-An Introduction. Hydrabad, ICFAI Publications, ed.l' 2004, p-II.

2.1 Definition of Cyber crime:-

The Indian assembly doesn't offer the precise definition of Cyber crime in any statute, even the data Technology Act, 2000; that deals with cyber crime doesn't outlined the term of cyber crime but normally the term cyber crime means that any criminal activity that is carried over or with the assistance of net or computers.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"

The oxford Dictionary defined the term cyber crime as "Criminal activities carried out by means of computers or the Internet."

"Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"

"Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them"

Professor S.T. Viswanathan has given three definitions in his book The Indian Cyber Laws with Cyber Glossary is as follows –

1. Any illegal action in which a computer is the tool or objects of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,
2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

3. Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data. Cyber crime becomes a worldwide development and thence the nationwide generalization of crime cannot viable in gift state of affairs. Our understanding and regulation of cyber crime cannot be national however needs to be international. We've got to enact new laws and prepare preventive and defensive mechanism globally, solely then ready to able to shield our society from this evil referred to as 'Cyber Crime'.

2.2 Evolution Nature and scope of Cyber Crime

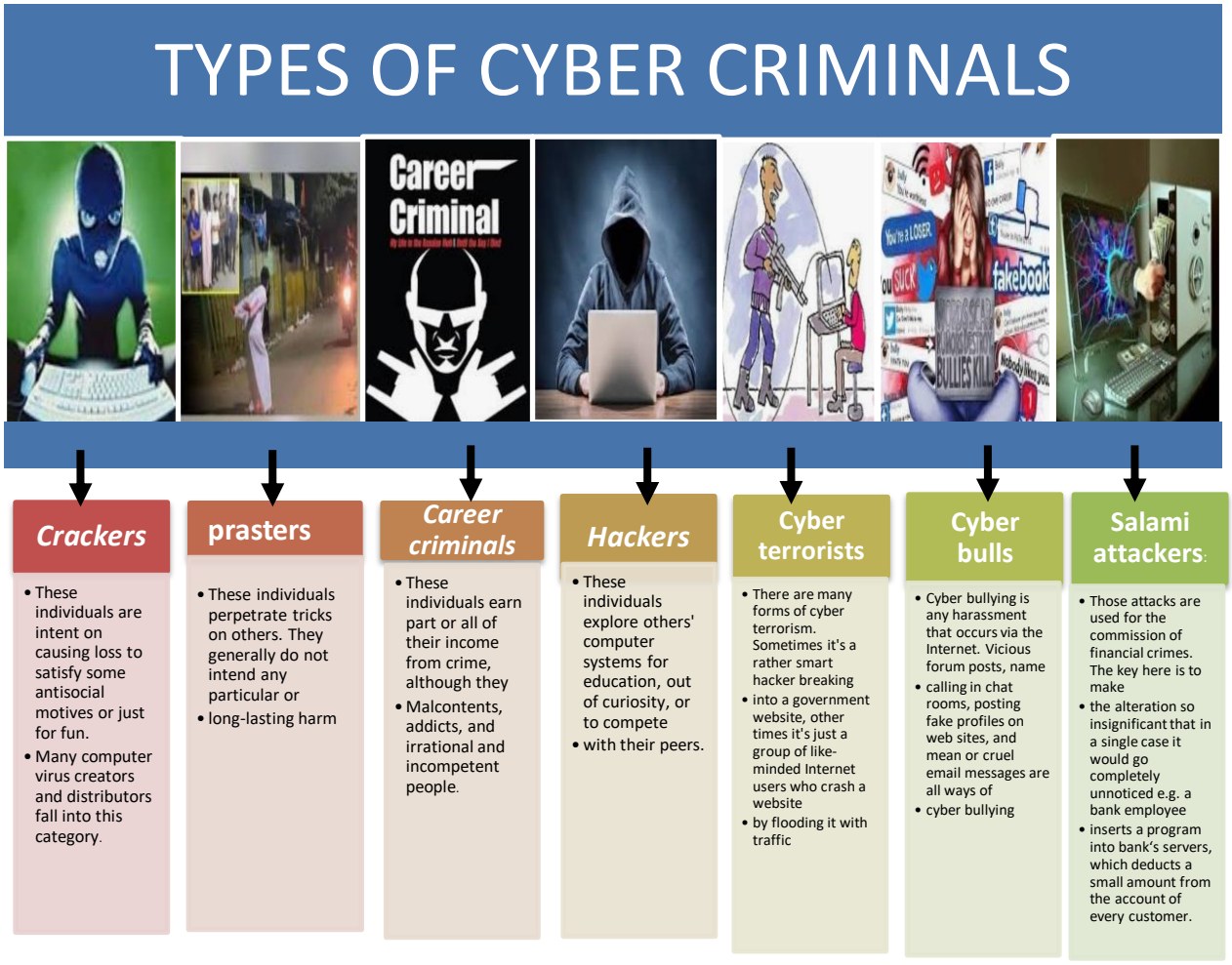
Cybercrime is the deadliest epidemic confronting our planet in this millennium. At present when everything from microwave ovens and refrigerators to nuclear power plants are being run or computers cybercrime has assumed rather sister implication. It has raised its head as multi headed hydra. Where if one is being cut other and newer kinds of crimes are appear or develop suddenly cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud forgery, defamation and mischief. The above of computer has also providing an scope of new age crime such as hacking, web defacement cyber stalking, web jading etc.

Cyber crime is a twentieth century fetus of technological development, now which grown up like as epidemic and has become uncontrollable in the twenty-first century[15]. The first cyber crime took place in the year 1820. Joseph-Marie Jacquarid's, a textile Unmanufactured in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquardi employed that their traditional employment and livelihood were being threatened. They committed the acts of sabotage to discharge Jacquard from further use of the new technology. So, this is the first recorded cyber crime[16]

2.3 **Cyber-criminals**

Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to Cyber-crime. Some of the kinds of Cyber-criminals are shown in figure 1.1

15Manupatra Newsline, Aug & Sep 2008.
16 Supra 9.



Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities.

2.4 DIFFERENT REASON BEHIND CYBER CRIME:-

There are many reasons why cyber-criminals are doing cyber-crime some important reasons are mentioned below[17]:-

A. For the sake of recognition.
B. For the sake of quick money.
C. To fight a cause one thinks he believes in.
D. Low marginal cost of online activity due to global reach.
E. Catching by law and enforcement agency is less effective and more expensive.

17. Charles Goredema, "Inter-State cooperation", in African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries (African Human Security Initiative, 2004).

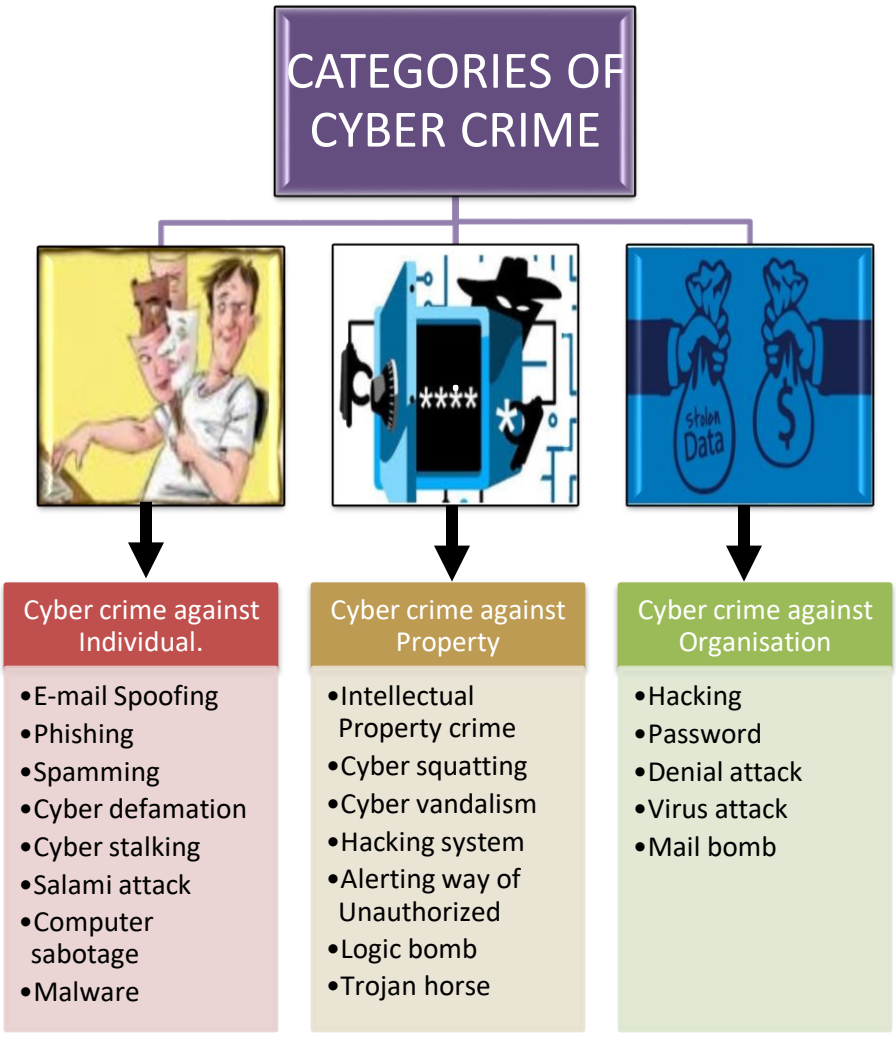
F. New opportunity to do legal acts using technical architecture.
G. Official investigation and criminal prosecution is rare.
H. No concrete regulatory measure.
I. Lack of reporting and standards
J. Difficulty in identification.
K. Limited media coverage.

2.5 Categories of cyber crime:-

Broadly speaking, the cyber crimes refer to all activities done with criminal intent in cyber space.

There are Three main categories of cyber crimes is crime and individual, against property, against organization..

For better understanding they are shown in figure 1.2:-



2.5.1 Crime against individual:-

The first category of cyber crimes committed against person include various like transmission of Child-pornography, sexual harassment of any one wraith the use of a computer, such and e-mail spoofing and cyber stalking. Any unwanted contact between two people that directly or indirectly communicates a heart or place the victim in fear can be considered stalking. The Trafficking, distribution, posing and dissemination of absence material including pornography, indecent exposure and child pornography constitutes one of the most important cyber crimes know today. The potential harm of such a crime to humanity can hardly be over stated[18].

Similarly the cyber harassment is a distinct Cyber crime various kinds of harassment can and does occur in cyber space or through the cyberspace. The internet is a wonderful place to work, play and no less than a miter of the real world and that means it also contains electronic versions of real life problems, stalking and harassment are problems that many also occur on the internet.

2.5.2 Cyber Crime against property

The second category of cyber crime is that of cyber crimes against all types of property. These crimes includes Hacking is unauthorized use of computer and network resources and cracking some breaks into someone else computer system often on a network or intentionally breaches computer security, Vim's is a computer programmed that can reproduce itself and causing destruction of data contamination, copy-right protects creative or artistic works. You should only copy or copyrighted work with the copyright owner's permission infringement, potent is a set of exclusive rights granted by a state to an inventor or his assign for a fixed period of time in exchange for a disclosure of an invention. Infringement, impersonation or cyber fraud, cyber squatting is registering, trafficking in or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else etc. In these Hacking and cracking are among the gravest cyber crimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent has tampered with precious confidential data and information. Coupled with this, the reality is that no

18 Dr. Patel, S. Band, 'Cyber Crime: A burning problem.' Reading Kdaterial: 3 day workshop cum conference, IT Laws and related Intellectual Property, Law centre 1, Delhi University, p. 184.

computer system in the world is hacking proof. So, it is unanimously agreed that any and every system in the world can be hacked . Sophisticated structure, together with access to the core operations granted only to tested associates, prevents organized cybercrimes groups from being detected and infiltrated by law enforcement.

2.5.3 Crime against organization

Organizations, too, reflected a variety of goals, including defiance of authority, freedom of information, sexual gratification of members, and technological challenge. However, the profit motive was more apparent in the organization cases than with individual Offenders. Every new technology and every new application will create an opportunity that criminals will soon seek to exploit. Some examples of cyber crimes against organizations are Possessing unauthorized information, Cyber terrorism against a government organization, distributing pirated software, hacking, password cracking, virus attack, mail bomb, etc.

2.6 Cyber Crime and Organized Crime

The internet revolution has transformed the society in general and the commercial world in particular. While commercial dealing is rampant on the internet due to its reach worldwide in low cost. So organized crime also found the new opportunities and benefits on internet that are very useful for furthering the criminal activities organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. Some traditional criminal groups are seeking the co-operation of criminals with the necessary technical skills, newer types of criminal networks operating in the area of e-crime have already
Emerged[19].

According to Phil Williams of university of Pittsburgh 'organized crime is primarily about the pursuit of profit and can be understood in Clausewitz Ian terms as a continuation of business by criminal means'

19 Dr. l>opina, Tatiama, available at; http://ww\v. freedorafromfear magazine.org, (Visited on August 2, 2010)

the objective of organized crime is also to earn profits though businesses, but the only difference is that the business activity or means of contracting the business may be illegal.

Criminal organizations are constantly on the lookout for new opportunities as well as new ways of keeping themselves safe and away from the law enforcing authorities. Internet offers a number of services for the common man and criminals could abuse many of those services to their advantage. Internet is most inexpressible and realizable Id. These attributes attract the criminals as well as also help them in speeding up their activities. The structure of these criminal organizations is different from traditional organized crime organization. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on "Stand alone" basis, as members rarely meet each other is person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to tasted associates, prevents organized cybercrimes groups from being detected and infiltrated by law enforcement.

2.7 Cyber Crime and Legislation of Nations

To meet the challenges posed by new kinds of crime made possible by computer technology including telecommunication, many of the countries largely industrialized and some of those which are moving towards industrialization have in part few years reviews their respective domestic criminal laws from the point of adaptation, further development and supplementation so as to prevent computer related crime. A number of countries have already introduced more or less extensive amendments by adding new statutes in their substantive criminal law[20].

According to McConnell International some counties laws are substantially or particularly updated laws, while some others have no updated law. There is no uniformity in the legislation among the nations.

(A) Australia: Has included offence related to computers in the Australian crime Act. The penalty for damaging data in. computers is imprisonment up to 10 yrs and for unlawful data in computers imprisonment from 6 months to 3 years.

[20] Gurjeet Singh & Vidhy Sandher, 'Emerging of Cybercrime A challenge for new millennium' Aligarh Law Journal. Vol. XIV & XV, year 1999-2000, p. 33

(B) Canada: Has named three Computer Crimes (a) Possession of devices to obtain unauthorized telephone facilities; (b) unauthorized access to computer; (c) Committing mischief with data.
The imprisonment varies from 2 years to upto 10 years depending the nature of the crime.

(C) Germany; Classified Compute Crime Like data spying, computer fraud, alternation of data and computer sabotage. The punishment varies from 2 years to 5 years depending upon the nature of crime.

(D) Singapore: Computer Misuse Act refers to unauthorized access to computer system with internet to commit or facilitate commission of offence, unauthorized modification of computer material etc. Punishra.ent is Imprisonment from 2 years to up to 5 years with fine.

The Electronic Communication privacy Act 1997, The Electronic Theft Act 1997, The Child Online Protection Act 1998, the Internet Tax Freedom Act 1998, The U.S. Trademark Copyright prevention Act, in Global and National Commerce Act (E-Sigh) 2000, The Uniform Computer Information Transaction Act 2000, and The Children Internet Protection Act 2001[21].

These acts classified computer crimes, as (a) willful unauthorized access of computer related to national defense or foreign relation (b) intentional access of computer without authorization to obtain financial information, (c) unauthorized access of computer of a government department or an agency, (d) unauthorized access of computer federal, internet with internet to defraud, (e) Knowingly causing transmission of data/programmed to damage a computer network or deny use of computer, network etc, (f) Knowingly causing transmission of data/programmed with risk that transmission will damage a computer network, data or program or without or dent use of computer, network etc. and (g) Unauthorized access of computer with intent to defraud[22].

2.8 Cyber crime and Indian Position

The first cyber crime took place as early as in the year 1820. The crimes have however gained Momentum in India only in the recent past. As an upshot, the Indian Parliament gave effect to a resolution of the General Assembly of the United Nations for adoption of a Model Law on Electronic Commerce. The consequence

21. Aligarh Law Journal 1999-2000, p
22. Ibid.

was the passing of Information Technology Act 2000. The Act aims to regulate and legalize E-Commerce and take cognizance of offences arising there from. The Information Technology Act deals with the following cyber crimes along with others

(A) Tampering with computer source documents

A person who knowingly or intentionally, conceals (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable. For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file.

(B) Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks.
Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by means is said to commit hacking.

Vinod Kaushik and Ors. V/s Madhvika Joshi and Others[23].

The main issue in this case is whether accessing a husband's and father-in-law's email account without their permission amounts to 'unauthorized access'. In this case, the first respondent had accessed the email account of her husband and father in law, in order to acquire evidence in a Dowry harassment case. The Adjudicating

23. Before Sh. Rajesh Agawal, Adjudicating Officer, Information Technology Act, 2000, Government of Maharashtra, At Mantralaya, Mumbai- 400032, Complaint No.2 of 2010. available

Officer held that accessing an e-mail account without authorization amounts to a contravention of section 43 of the information Technology Act 2000.

There was no compensation awarded to the complainant as the respondent had only submitted the information so obtained to the police and the court. The Adjudicating Officer, however ordered the first respondent to pay a fine of Rs. 100, as she was held to be in contravention of Section 66-C (identity theft and dishonest use of the password of any other person) of the IT Act 2000.

It is to be noted that there cannot be any defense of bonafide intention, in case of violation of privacy by accessing e-mail accounts without the consent of the user. It will be still construed as 'unauthorized access'. It is also interesting to note that the adjudicating officer relied on the reasoning that the information procured by the 'unauthorized access' was only disclosed to the Coils and the police, therefore the respondent is not liable to pay any compensation to the complainant. However, Section 43 of the IT Act 2000 deals with the penalty and compensation for an 'unauthorized access' to any computer or computer system or computer network. It may be said there is a lacuna in the reasoning of the Adjudicating Officer. It also gives rise to the question whether a person is not liable to pay compensation under Section 43 if the information obtained by 'unauthorized access' is only disclosed before competent authorities such as police or court. The 'unauthorized access' of an e mail account by dishonest use of password of any other person also amounts to violation of privacy. It is covered under Section 66C of the IT Act 2000.

(c) Publishing of information, which is obscene in electronic form

A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and comfit persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produced the effect of publishing), pornographic material in the electronic form.

(D)Child Pornography

Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cyber crime. The Internet is being highly used by its abusers to reach and abuse children

sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cyber crime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start contacting children on their e-mail addresses.

(E) Breach of confidentiality and privacy

Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to be punished under the Information Technology Act.

K.L.D Nagasree v, Government of India, represented by its Secretary, Ministry of Home Affairs and Ors[24].

A writ petition was filed in the Andhra Pradesh High Court challenging the order of the respondent under Section 5(2) of the Indian Telegraph Act 1885.

The respondent gave the order to intercept messages from the mobile phone of the petitioner. The Court examined the procedural safeguards that are in place in case with respect to an order of interception of communication. These safeguards are enshrined in Rule 419-A of the Indian Telegraph Rules 1951 pursuant to the guidelines laid down by the Supreme Court in the case of

PUCL V. Union of India. The Court, while considering the impugned order, decided that the order did not record the reasons for the interception. The Court also discovered that the Review Committee constituted under Rule 419-A (8) had without any reason delayed the review of the impugned order. The Court also laid down in this case that the procedural inconsistencies render any recorded evidence inadmissible in Court. The Court also observed that the enforcement agencies were not observing the

24 AIR2007AP102, (Aiidhra Pradesh High Court).

correct procedure for interception of communications under Section 5(2) of the Indian Telegraph Act. It ordered that any such recording should be destroyed.

It is one of the few instances where the Court has gone on record to say that the enforcement agencies are not following the procedure established by law, with regard to giving out of orders for interception of communication under Section 5(2) of the India Telegraph Act 1885. Disregard to procedural safeguard by the enforcement agency amounts to a gross violation of right to privacy envisaged under Article 21 of the Constitution of India.

Rayala M. Bhuvaneswari v. Nagaphanender Rayala[25]

This case came up before the Andhra Pradesh High Court under a revision petition for a voice test of a tape recording. In this case, the Court discovered that the husband had tape-recorded a telephone conversation of his wife with her friends and parents, without her consent. Subsequently, he had been using this as evidence in the divorce case between the parties. The Court, at the very outset, held that there had been clear violation of privacy of the wife by her husband. It also cited the compilation of Federal Law on "Covertly Recording Telephone Conversation", which makes it unlawful to record telephone conversation except in one-party consent cases. One-party consent cases are those cases where the person can record their own telephone conversation without the consent or knowledge of the other party. But in this case no consent had been given by either party of the telephone conversation.

The Court held that the act of the husband was illegal and unconstitutional, and infringed upon the privacy of the wife. Even if the tapes were accurate, they could not be admissible as evidence.

This is one of cases where the Court has acknowledged that the protection of right to privacy under Article 21 of the Constitution of India is not only enforceable against the State but also against individuals. The Court also held that any recording which infringes upon the right to privacy of an innocent person cannot be admitted as evidence in a court of law.

Nirav Navin Bhai Shah and Ors. v. State of Gujarat and Another[26]

The appellants were accused of hacking into the computer system of the complainant and stealing important data. The main issue was whether criminal proceedings can be quashed on the ground that the

25. AIR 2008 AI' 98 (Andhra Pradesh High Court).
26. Criminal Misc. Application No. 10291 of 2006, Decided On: 28.09,2006 (Gujarat High Court).

parties have reached an amicable settlement. The Court decided that if the 'entire' dispute has been amicably settled then the Court shall quash criminal proceeding to that effect.

In this case the appellants were charged under section 66 and 72 of the Information Technology Act 2000 along with other offences under the Indian Penal Code 1860. The complainant argued before the Court that the criminal proceeding should be quashed as the dispute is civil in nature.

The Court rejected the contention, while stating that the offense cannot be viewed as a civil dispute because offenses under section 66 and 72 of the Information Technology Act 2000 are offenses against the society and camion be condoned. The Court however, quashed the FIR based on the reasoning that there was an amicable settlement of the 'entire dispute'. It also took into consideration that if criminal proceedings were continued, a miscarriage of justice would be the result.

The Gujarat High Court observed that violation of privacy and hacking are offenses against the society and cannot be condoned or treated as a civil dispute. However, if the parties agree to a settlement of the 'entire' dispute then the Court may allow such settlement in the interest of justice.

2.9. Cyber crimes other than those mentioned under the IT Act

Although there is no universally accepted definition of cyber stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using Internet services. Stalking in General terais can be referred to as the repeated acts of Harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

(A) Cyber squatting

Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different).

A trademark owner can prevail in a cyber squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiffs' distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of pocket expenses.

(B) Data Diddling

This kind of an attack involves altering the raw data just before a computer processes it and then Changing it back after the processing is completed. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of finds by manipulating data files to show less receipts and bank remittances.

(C) Cyber Defamation

Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

(D) Trojan Attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(E) **Forgery**

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. It is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

(F)Financial crimes

This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

(G) Internet time theft

This con notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

(H) Virus/worm attack

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

(I) E-mail spoofing

It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends.

(J) Cyber terrorists

There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of likeminded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.

Earlier when IT Act enacted in 2000 the punishment was silent but after amendment in 2008 the punishment has been prescribed.

2.10 Challenges of cyber crime:-

Cyberspace does not recognize geographical boundaries. This has proved a boon to the delinquents who perform illegal activities on the internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the part of law enforcement agencies further complicates the matter. The challenges posed by cyber crime are classified as:

(¡) Legal challenges which are dependent on the statutory provisions to be used as a tool to investigate bad control the cyber crimes.

(¡¡) Operational challenges require a cohesive well trained and well equipped force of investigators operating and coordinating at national and international level.

(¡¡¡) Technical challenges thwarting the efforts of law enforcement agencies' ability to catch and prosecute the online offenders.[27]

Cyber crimes are often committed beyond the national borders. The national standards of criminal behavior vary. Furthermore, it is very difficult to identify the perpetrator of wrong because internet facilitates anonymity. Thus, cyber crime pose challenges that are unique in character unlike traditional crimes. These crimes can not be effectively dealt with by simply passing national legislation. The IT Act has extra-territorial jurisdiction and applies to any offence or contravention there under committed outside India by any person. This feature of the IT is not unusual. Similar provision is found in the IT

27. S.S.H Azami Information Technology, cyber crimes and Solutions,Souvenir International conference on International law in new Milenium:Problem and challenges Ahead, 4-7 October,2001

legislations of other jurisdictions also However, this provision can be effective only when there is a mutual cooperation at the international level amongst enforcement authorities and Governments.

2.11 How to protect yourself against cybercrime

Anyone using the internet should exercise some basic precautions. Here are 11 tips you can use to help protect yourself against the range of cybercrimes out there.[28]

1. Use a full-service internet security suite

For instance, Norton Security provides real-time protection against existing and emerging malware including ransom ware and viruses, and helps protect your private and financial information when you go online.

2. Use strong passwords

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

3. Keep your software updated

This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

4. Manage your social media settings

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

5. Strengthen your home network

It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

6. Talk to your children about the internet

28. https://us.norton.com-from-cybercrime.html

You can teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

7. Keep up to date on major security breaches

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

8. Take measures to help protect yourself against identity theft

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

9. Know that identity theft can happen anywhere

It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

10. Keep an eye on the kids

Just like you'll want to talk to your kids about the internet, you'll also want to help protect them against identity theft. Identity thieves often target children because their Social Security number and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing your child's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.

11. Know what to do if you become a victim

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.

CHAPTER III

LEGAL & TECHNOLOGICAL MEASURE'S TO COMBAT CYBER CRIME

3.0 Introduction

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or committed in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represent the cyber crime as Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data. Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through respective ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialized, has seen the dramatic expansion of cyber space in its brief existence. From its initial avatar as a Network (NW) created by academics for the use of the military, it has now become a global social, economic and communications platform.

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown a pace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and Stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military national security actors at one end and economic-civil society actors at the other.[29]

29. Siddiqui, M. Zakaria, 'Cyber TerrorisiTi: Global Perspective', *The Indian Journal of Criminology' and Criminalistics.* Vol. XXII, No.2, May-Aug 2001, p.49.

3.1 Impacts of Cyber-Crime

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increase in the rate of prosecutions of cyber-criminals. There has been an increase in clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts.[30]

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

3.2 Potential Economic Impact

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crimes in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

30. The FBI is primary investigative agency of United Slate's Department of Justice (DOJ), serving as body a federal criminal investigative body and a domestic intelligence agency. Available at http://www.fbi.gov/quickfacts.htm (Visited on. January 12, 2010).

3.3 Cyber Crime's Impact on Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies that provide cyber-risk policies.[31] For example, a ruling in favor of Ingram Micro stated that physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality.[32] This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches. As the characteristics of security breaches change, companies continually reassess their IS environment for threats. In the past, Chief Investigation Officer's (CIOs) have relied on FUD fear, uncertainty, and doubt to promote IS security investments to upper management. Recently, some insurance companies created actuarial tables that they believe provide ways to measure losses from computer interruptions and hacker attacks. However, these estimates are questionable mostly due to the lack of historical data. Some industry insiders confess that the rates for such plans are mostly set by guesswork." Industry experts stress on the need for improved return on security investment (ROSI) studies that could be used by insurance companies to create hacking insurance, with adjustable rates based on the level of security employed in the organization and by the organization to justify investments in security prevention strategies.

Depending on the size of the company, a comprehensive assessment of every aspect of the IS environment may be too costly and impractical. IS risk assessment provides a means form identifying threats to security and evaluating their severity. In IS, risk assessment addresses the questions of what is the impact of an IS security breach and how much will it cost the organization.'" However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the Following reasons:

1. Many organizations are unable or unwilling to quantify their financial losses due to security breaches.
2. Lack of historical data. Many security breaches are unreported.

---

31. Supra note 4.
32.Saiiii Henu-aj, Rao Yerra Shankar, Panda T.C., International Journal of Engineering Research and Applications (7JERA), Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209; available at http://www.ijera.com/papers/Voi2_issue2/AG22202209.pdf.

Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes, and fear of negative publicity. Companies are also wary of competitors exploiting these attacks to gain competitive advantage.

3. Additionally, companies maybe fearful of negative financial consequences resulting from public disclosure of a security breach.

Previous research suggests that public news of an event that is generally seen as negative will cause a drop in the firm's stock price.

Therefore, there is a need for a different approach to assess the risk of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself.[33] Moreover, managers aim to maximize a firm's market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value.

3.4 Impact on Consumer trust

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, *while* the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer losing confidence in the said site and in the internet and its strengths.

According to reports presented by the Better Business Bureau Online (BBBO), over 80% of online shoppers cited security as a basic concern when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information.

33. Hancock, B., Security Crisis Management-The Basics, Computers & Security, 21(5): 397-401., available at: www.ingentaconnect.com/content/els/01674048/2002/.../art00503,(Visited on September 21, 2009).

The perception, that the Internet is rife with credit card fraud and security hazards, is growing. This has been a serious problem for e-commerce.

3.5 Areas Ripe for Exploitation: National Security

Modem military of most of the countries depends heavily on advanced computers. Information Warfare (IW) including network attack, exploitation, and defense, is not a new national security challenge, but since 9/11, it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration.

The Internet has 90 percent junk and 10 percent good security systems, when intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of the residents of their own country.

Most of such crimes have been originating in developing countries. The wide spread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

3.5.1 Future Trends

One of the biggest concerns is that if there is a hack into the critical systems in government, companies, financial institutions etc? This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently.

The internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the risk of money laundering through over-invoicing and under-invoicing is likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases. Online gambling also makes it possible to move money especially to offshore financial centers.

Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous.
Because mainly information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could argue in favor of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crimes.

Some of the future trends predicted by Stephen Northcutt & Friend are briefly summarized in the following words.

Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional parameter security measures.

Social Media will provide the platform for the cyber crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products, solving all these problems; some of them will stand out by allowing organizations to gradually control and monitor on-line social networking activities, while being mindful of users' privacy expectations.

Humans are the weakest *link*, irrespective of the change in technology attackers know that they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in sophistication and numbers.
Cyber attackers will always take the path of least resistance. Organizations and management will finally start doing something about it to secure the human.

It is the sensitive issue for the people relying on iPhones for their day-today works that without issuing a warning that some worm will eat ail the iPhones and convert the Androids to bricks. However, the biggest issue seems to be applications with spyware. Even the apps that come loaded on the phones, are likely to phone home, it is a sure thing with third party apps.

Memory scraping will become more common in the coming times. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys. The reason they are successful is that they get around Payment Card Industry, Gramm-Leach-Bliley Act, Health Insurance Portability And Accountability Act, (PCI, GLBA, HIPAA, etc.), Security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resistant even after the fact. The data is encrypted on the hard disk, but again, the RAM likely maintains the clear-text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often miss configured, allowing malware to get into a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly.
Audio Visual (AV) products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware. We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point of Sale (POS) systems.

Wireless adoption will continue brandling out into a larger number of purpose-focused protocols that fit the needs of individual technology. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including ZigBee, Wireless HART and Z-Wave, as well as proprietary protocols. With this growing alternate wireless adoption, we are already seeing some of the past mistakes from earlier failed protocols repetition. Based on this exposure, and the trend of Wi-Fi failure and improvement, we will see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies.

Security Continues to become the part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have".

3.6 Internet Governance Challenges and Constraints

The success of the Internet has partly been attributed to its relative openness and low barriers (including minimal security features) to entry.
However, the same Internet Corporation for Assigned Names and Numbers (ICANN), it has done so very reluctantly.

Though it has been a participant in multilateral forum, the United States" agenda invariably has been to ensure that its dominant position is not disturbed.
More recently, approaches to cyberspace have taken ideological hues, with countries ultimately seeking to gain effective control over deciding the form and shape of cyberspace within their national

boundaries. The jockeying to influence Internet governance issues has seen increased actively in recent times. Most of these have taken place at the multilateral level, with countries forming coalitions and introducing resolutions at multilateral forum. While Russia has been introducing resolutions on cyber security at the United Nations since 1998, it recently joined hands with China, Tajikistan and Uzbekistan to introduce an "International Code of Conduct for information Security" (ICCIS). Some of the clauses within this resolution have been criticized as an attempt to increase control over content and information in the guise of securing cyberspace. Proposals by the IBSA forum (India, Brazil, South Africa) have also been seen with similar skepticism. One of the noted goals of the recent Cyber Security Summit held by the British government would be seen as an effort on the part of the advanced economies to regain the initiative in drawing up norms for cyberspace that highlight core Western values.[34]

3.7 Cyber Crimes and the nature of Evidence

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of finger prints, weapon of crime, blood stain marks etc can be traced, in the virtual world such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.[35]

It is considered difficult to expunge the information from the computer system than what is generally contemplated. This can be done with the help of computer forensics who are able to gather evidence or even recover information which may have been deleted intentionally. It is vital that the victim report the

34. Available at: www. idsa.in/systeiri;'files/book_!ndiacybersecurity.pdf, pp 17-18.
35. Supra Note 31

law enforcement agencies about the crime as early as possible. The process of preservation of cyber crime evidence lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence. The most often faced impediment is that the victim-companies are more concerned with restoration of their systems to full operational status rather than allowing proper evidence collection. Thus the timely assistance of the computer forensics expert can help collect evidence from the system within shortest time possible.

Cyber evidence is of physical or logical nature. It is the physical evidence that can be traced easily as the investigator just has to visit the scene of crime and search for and take into his custody computer hardware, which may constitute main frame computers to pocket sized personal assistants, floppy diskettes, electronic chips etc. The facets of the logical component of the cyber evidence are of different nature. This entails a process described as 'Information Discovery' wherein the investigator scrutinizes through the log files, and tries to salvage the data from a computer system which has been affected.

Once the required evidence is identified, then the investigator must ensure that the same is collected by adhering to the legal requirements, such as evidence is collected only after the requisite warrant for it is issued or if the information appears to be outside the scope of the warrant then additional warrant be issued. The evidence collected becomes valid in the courts of law only if the evidence is collected by legal means.[36]

Another quarter which needs to be tested under cyber evidence and which is inevitable is the appreciation of the computer generated evidence by all the authorities associated with the process of administration of justice. Thus not just the judiciary but also the prosecutors, the defense lawyers must become familiar with the technicalities, this is so because till now these authorities were dealing with evidence in the tangible form but the nature of evidence undergoes complete change under the virtual medium, they will have to adjust themselves to appreciate the evidence in logical format.

36Supra Note 36,p197

3.8 Criminal Liability under Indian Criminal Law and the Information Technology Act 2000

The Indian Criminal Law hovers around the Indian Penal Code, though there are other statutes which provide for criminal liability, but the Indian Penal Code is the sole authority in regards of deciding the conditions required to fulfill criminal liability. Various expressions have been used in defining offences under the Indian Penal Code like intention', "Knowledge" etc but in spite of this clinical treatment of mens Rea experience has shown that the court have imported the Common law maxim of mens Rea in the process of interpreting the offence defined under the Indian Penal Code and other special Statutes.[37] Thus the Courts in India have been treating the concept of mens Rea on offence to offence basis. Thus it can be said that the maxim *"actus non facit reum nisi mens sit rea*" as a maxim has no significance to the offences under the Indian Penal Code. Where the code has not indicated any peculiar guilty intent or knowledge etc then the court presume, by considering the general definition that such an omission was made with some specific intention. In such case it would be unfair to import the maxim and arrive at a judgment declaring the offender guilty. The Indian Law Commission in its 47th Report has mentioned that as a result of the transition process that the society w-as going through i.e., from a simple to an industrialized society it has become incumbent to contain the malpractices that were prevailing in the society then as such malpractices were unknown before for instance Unfair Trade Practices, Adulteration in Food, drugs etc, thus to restrain the emerging situation the judiciary and the parliament played a pivotal role in introducing the concept of Strict Liability because it is difficult to prove guilty intension of the offender in such socio-economic crimes. The effect of this was that with the imposition of Strict Liability under Criminal Law the burden of proof shifted from the prosecution to the defendant, and the Guilty mind need not be proved example in crimes like hacking it is almost impossible to prove guilty mind.

In regards of the Cyber Crimes under the Information Technology Act 2000 the Liability is divided into three categories. This has been done in order to avoid broad criminalization of all the wrongful acts in the virtual medium. Firstly there are certain wrongful acts that do not attract criminal liability and

37. The Regina v. Pnnce Case 13Cox CC 138.

mens rea is not applicable to them, such acts are subject to civil penalties and strict liability is imposed on the wrongs of this category e.g. failure to maintain books of accounts or contaminating the computer with viruses etc.

Secondly there are certain acts where mens rea has been made and fundamental part of the definition of the offence, thus expressions like 'Knowledge', 'intension' etc are included in the definition of such offences e.g. tampering with the computer, publishing for fraudulent purposes etc. Lastly there are some [24]acts or omissions that are made criminally liable with strict liability.[38] e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc.

3.8.1 Antiquated Criminal Procedural Laws

The distinctive feature of the cyber crimes has also had their consequence on the criminal procedural laws which have become more obvious in the areas of prosecution and investigation of the cyber crimes. The significant feature of this ever widening space between the law enforcement agencies and the cyber criminals is that the law enforcement agencies of most of the nations are not oriented for the dexterity necessary for investigating the crime in the virtual medium to add to this complexity is the trans-national nature of the cyber crime. The result is that the traditional methods of crime investigation and the evidence collection have become obsolete partially.

Following reasons can be attributed.

As per the traditional criminal procedure as soon as the police officer come to know about the commission of the offence he/she is expected to visit the scene of the crime, and collect the first hand details about the crime.[39] If the offence is of a cognizable nature then he must initiate investigation of the crime, but in case of a non-cognizable crime the officer is required to record the complaint and direct the informant to a Magistrate having power to try such case.[40] The problem faced by the police officer is

38. Sections 71,72,73 of the Information Technology Act 2000,
39. Sections 154,156, 157 of theCr.PC.
40. Section 155 of the Cr.PC., committal of the case for trial.

to begin with is that the victims are not aware of the fact that a crime has been committed against them or that the crime is being committed.

Further the police officer is empowered to ensure the attendance of the person who gives the information or who is acquainted with the facts and circumstance of the case. But in the context of cyber crime it has been noticed that there is very low reporting of the crime to the police, this factor must also be taken into consideration that the non-realization of the commission of the crime. The reasons cited for the Non-reporting of the crime are many, and many of them are of convincing nature e.g. fear of bad publicity, breach of security systems will affect the goodwill and confidence of the customers, fear of insurance cover of the companies been blown off, fear of transparency in the activities of the victim i.e. financial and other trade secrets will be required to be parted with to the investigation authorities etc.

Few steps[41] that have been recommended by Dr.S. V. .Joga Rao in order to facilitate reporting and investigation of" cyber crimes are:

i. Establish an incident response policy

ii. Maintain an up-to-date human resource record.

iii. Archive systems logs.

The next stage of investigation is of Search and Seizure by the Police officers and the collection of incriminating evidence connected with the crime. Again in the present context of cyber crimes the investigation process requires collection of the data, which further needs to be evaluated, which may be stored in a computer system located in some other country in case of a trans-national computer crime. The police authorities find getting access to such data in other country difficult and time consuming. Further the investigation agencies need to be careful as the possible evidence in a computer system can be altered and the genuineness of such evidence is often challenged in the courts of law. The Indian

41. Dr. Rao, S.V. Joga, *Lavj of Cyber Crimes & Information Technology* Law.Lucknow, Eastern Book Company, edition 2004, p. 194.

Information Technology ,Act 2000 has addressed such issues by making amendments to the Indian Evidence Act 1872; the tern electronic records have been included in the definition of the term evidence.[42]

The Degree of power of search is also one important aspect which needs to be addressed. The problem mainly arises in the area of Public International law with respect to search and seizure of databases via an international telecommunications network systems, as any unauthorized penetration in such databases would amount to infringement of the sovereignty of that State where the data is stored, further such unauthorized access to any computer system is an offence in India. Further the major hindrance that is caused in the investigation of cyber crimes is the level of expertise on the cyber forensics, as they must have extensive knowledge of the hardware, software, operating systems and the data-processing systems. Further the security software's, encryption software's limit the process of deciphering the data stored on the computer system. This is despite of the provision made in the criminal procedure code for the surrender of the documents or objects which are necessary for the investigation purpose either before the court or to the investigation officer on his written order.' Along with the above provision there is also a duty cast on the person in-charge of the premises to grant access to the investigation authorities.

Another aspect which needs to be highlighted in light of the search and seizure of data is the tapping of telephone communications lines. This becomes inevitable especially in the case of Internet crimes as data is only transmitted and not stored permanently on the computer system. This may necessitate real time monitoring system to make possible collection of evidence and make possible catching the suspect 'red handed''. But in order to make such provisions in law, care need to be taken about the Right to privacy as unlike in the case of search and seizure, which amounts to perceptible interference which is of a limited nature, interception of the communication amount to gross invasion of the right to privacy. At the moment the power of wiretapping have been provided under section 5 of the Indian Telegraph Act 1885. which lays down a complex procedure and a so that this power is not misused. The Information Technology Act 2000 provided for a specific power to intercept transmitted information through any computer resource under section 69. Comprehensive provisions with detailed procedures were made in the Convergence Bill introduce in year 2000 viz. interception of all kinds of communication like wire, electronic communications etc, however this in due course lapsed and failed to become a law.

42.The Second Schedule of the Information Technology Act 2000.

CHAPTER IV

CYBER TERRORISM

4.0 INTRODUCTION

Cyber terrorism is gaining tremendous attention nowadays due to the increasingly high amount of coverage being given to the subject by the media and various institutions especially those from the public and private sectors. They recognize the disastrous impacts that cyber terrorism is capable of realizing and thus it is very important to increase awareness on the subject among the general public in order to mitigate the threats posed by cyber terrorism more efficiently.

Cyber terrorism is not a movement or just attack but a war. Well planned, well designed and organized war which is more harmful than traditional attack. Hackers attack with bots, viruses and Trojans instead of planes or armored vehicles and missiles and systematically create on-line "trapdoors" to invade servers and computers and steel passwords of high importance .So there must be long-term strategy to fight with this new and advance form of terrorism .Integrated approach is require for this in which cooperation of our Political bodies, Judiciaries, Administration, and above of all common people is inevitable.

The word "Cyber Terrorism" is of recent vintage and was coined by computer whiz Barry C. Collin. A widely acceptable definition of cyber terrorism is " a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda." According to the U.S. Federal Bureau of Investigation, " Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub- national groups or clandestine agents."

Can all cyber crimes be called as cyber-terrorism ? Not really. It is pertinent to note that while all cyber terrorism cases are cyber crimes, not all cyber crimes can be called acts of cyber terrorism ! Only those cyber crimes which are politically or ideologically motivated qualify to be called as acts of cyber terrorism . Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Various terrorist groups are adopting ICT as a tool to disrupt law and order of a country. Cyber terrorism is an organized criminal activity committed by one person or group of persons to disturb a genuine transaction.

This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terrorist threats made via electronic communication.

The goal of terrorism generally is to destroy the public's sense of security in the places most familiar to them. Major targets sometimes also include buildings or other locations that are important economic or political symbols, such as embassies or military installations.

4.1 The real cyber-terrorism

A report published by PCWorld.com online magazine in 2001 stated that the Federal Bureau of Investigation (FBI) and the System Administration, Networking, and Security Institute (SANS) had released a list of the 20 top vulnerabilities of Internet-connected systems and urged organizations to close the dangerous holes in order to avoid major cyber terrorism attacks.

According to Allan Paller who is the SANS Institute Director in the article, "The Internet is simply not ready because of these vulnerabilities; we're not ready to withstand a major attack". [43]

43. Thy bureau, Patrick. “Internet Vulnerabilities to Cyber terrorism Exposed. “ 1 October 2001. URL: http://www.pcworld.com/news/article/0,aid,64224,00.asp (4 June 2003)

Cyber terrorism can be defined as electronic attacks from cyberspace from both the internal and external networks, particularly from the Internet that emanate from various terrorist sources with different set of motivations and are directed at a particular target . The cyber terrorists generally perceive their targets to be either high-profile components of a nation's critical infrastructures or business operations. The main objective of these terrorists is to inflict damage which will either compromise or destruct targets in order to cause major physical and psychological impacts to them.

According to Clifford A. Wilke, "The ultimate threat to computer security is the insider" [44]. It is a well known fact that most cases of security breaches happen from inside the organizations. Thus cyber terrorism can also happen in the form of electronic attacks by authorized insiders, where the terrorists have obtained inside access to networks and systems via various means such as employment with the particular organization and others. This type of internal attacks is much more dangerous that the external ones because of the obvious difficulties in detecting them.

Besides direct internal attacks from insiders, insecure arrangements with outsourcing companies that employ or have been infiltrated by terrorists can prove to be dangerous as well.[45] Thus it is imperative that efforts to tackle cyber terrorism effectively should start from the roots, which means organizations need to place equal, if not more importance on securing themselves internally as well as externally.

In terms of its structure, cyber-terrorism is always organized crime, as opposed to individual cyber-crimes for example, a computer espionage committed by a single person or cybercrimes carried out by a group on an ad hoc basis for example, a computer sabotage committed by three individuals: one that develops malware, another that accesses a database and a third that uses malware to destroy certain data.

In effect, although some authors believe in terrorism carried out by a single person and, thus, could also accept individual cyber-terrorism, the specific "danger" implied by cyber-terrorism, which in part justifies its high punishment in relation to other cybercrimes, lies in the existence of an organized collective that operates systematically to commit an indefinite number of crimes. Such danger does not

---

44. A. Wilkin, Clifford. "Infrastructure Threats from Cyber-Terrorists." 5 March 1999. URL: http://www.occ.treas.gov/ftp/bulletin/99-9.txt (8 June 2003)

45. Glaessner, Thomas; Kellermann Tom; McNevin, Valerie. "Electronic Security: Risk Mitigation In Financial Transactions". June 2002.

exist in the case of an individual or ad hoc group acting alone, even if they employ similar methods (for example, destruction of critical infrastructure through computer networks) commonly used by cyber-terrorist organizations. For the same reason, if a single person gains access to a computer network and modifies the information that is issued and received at the monitoring station of an airport, thereby putting the life or health of people flying on the monitored aircraft at risk, there would certainly be some criminal conduct, but not a cyber-terrorist act based on the arguments outlined earlier.

In this context, to speak of a “criminal cyber-terrorist association”, there would have to exist, as with terrorism, a set number of members, access to resources and funding, and a capacity to sustainably plan and carry out operations over time.

Unlike in the case of traditional terrorism, the perpetration of terrorist and cyber-terrorist attacks through the use of technologies could relativze the requirement that there be an organized collective composed of a certain number of “people.” In fact, it is currently possible for a single person to comprise a botnet, that is, a series of computers called bots or zombies previously captured by that person. This capture is done through botware (Kochheim, 2015), malware designed to build botnets, which allows access and remote control of the various computer systems that make up the botnet (Choo, 2007). Due to this, it would be possible for a single controller of several bots or zombies to systematically commit an indefinite number of crimes.

However, that single person will never have the “organizational density” that is characteristic of terrorism, which implies the existence of a structure (of people) for collective decision making, to coordinate and persist over time. In this sense, although the possibility of action by that single person to harm other people is amplified due to a botnet, they are not comparable with those of a real (cyber)terrorist organization, the only structure really capable of keeping those interests protected by (cyber)terrorism in check. The amplification of damages through the use of technologies can be observed in many cybercrimes, but that in itself does not justify classifying the behaviour individual subjects as terrorist attacks.

The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business

information of the rival competitor is a part and parcel of cyber terrorism. The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace"' is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straight tacked formula or pigeons hole. In fact, the first effort of the Courts should be to interpret the definition as liberally as possible so that the menace of cyber terrorism can be tackled stringently and with a punitive hand. The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world. The laws of India have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which India may not have any reciprocal arrangements, including an "extradition treaty". Cyber terrorism emerges as a lethal pathogen in a shrinking world whereby we are all surrounded by an unknown enemy.

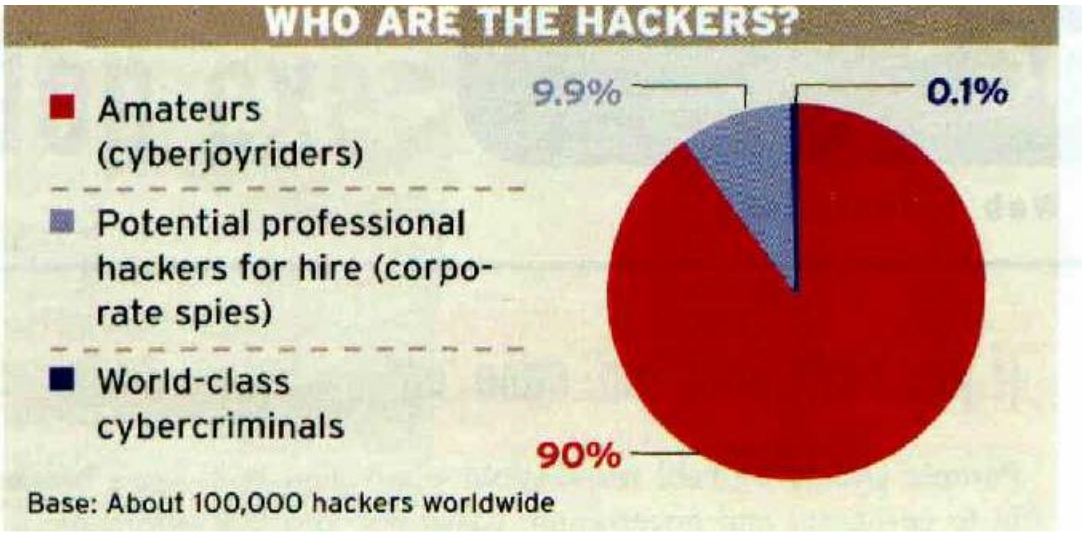
The fanciful notion of cyber terrorism is looming larger than even. It is said, "'..The modem Theft can steal more with a computer than with a gun. Tomorrows terrorist may be able to do more damage with a keyboard than with a bomb"." The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security technology and a law dealing with cyber terrorism is the need of the hour.

4.2 Who are the cyber terrorists?

In order to defend ourselves from cyber terrorists, we will need to identify who they are in the first place. The threats of cyber terrorism can be inflicted by anyone with hostile intents that has access and knowledge of utilizing cyber capabilities such as amateur and professional hackers, disgruntled employees, cyber criminals, cyber terrorist groups and others.

The graphic below shows that amateur hackers are by far the biggest threat on the Internet at the current time. They are responsible for about 90% of all hacking activities [46].

46. Sproles, Jimmy; Byars, Will. “Statistics on Cyber-terrorism.“ 1998. URL: http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm (5 May 2003)



The fact of the matter is, the threats of cyber terrorism can come from so many different sources, and sometimes it would seem to be such an impossible task to actually defend ourselves from it. However, with proper planning and strategic security implementations, we would be able to significantly reduce the chances of cyber terrorism attacks from happening to us.

4.3 Motivations for Cyber Terrorism

There are many different motivations for terrorists to deploy cyber terrorism as a mean to inflict damage or destruction to their targets. The are four main goals for such attacks to be carried out by terrorists: to destroy enemy's operational capabilities, to destroy or misrepresent the reputation of an organization, nation or alliance; to persuade those attacked to change affiliation, and to demonstrate to their own followers that they are capable of inflicting significant harm on their targets [47]

i. To destroy enemy's operational capabilities Cyber terrorism is deployed mainly for this particular reason. The terrorists feel that the usage of cyber capabilities offers them a low cost and effective solution to severely damage or destroy their targets in order to force them to be unable to continue their

47. Axelrod, C. Warren. "Security Against Cyber Terrorism. " 27 February 2002.

normal operations. The consequences of such attacks, if successful can prove to be very damaging in various ways including major collapses in economical and social standings. If critical infrastructures and business operations are hit, it can literally bring an entire nation or business to a halt.

ii. To destroy or misrepresent the reputation of an organization, nation or alliance. This is also one of the main goals of cyber terrorism. Many organizations, nations and alliances are able to operate effectively and are highly respected and regarded because of their unmistakable and strong reputation. If this vital element is tarnished, it could severely impact the normal operations of the targeted entity. The most common methods of destroying or misrepresenting the target's reputation include web site defacements and spreading false rumors concerning the particular target through electronic means such as e-mail, web sites and others.

iii. To persuade those attacked to change affiliation Sometimes cyber terrorism is used in order to force the attacked entities to change their association or affiliation to certain parties. Even though this goal is much harder to be carried out, there has been cases where it has proved to be successful. Defending against such motivated attacks requires the attacked organization to form strong alliances with its partner entities in order to be able to handle the situation better or avoid such situations from happening altogether.

iv. To demonstrate to their own followers that they are capable of inflicting significant harm on their targets Cyber terrorists are also keen to carry out cyber attacks because they want to prove to their followers and the world that they have the capabilities of inflicting severe damages on its targets. There are still a large number of people who are unconvinced about the realities of cyber terrorism and its capabilities. Thus if the cyber terrorists feel that they have a need to prove their capabilities of performing electronic-based attacks to their targets, they might do so to prove their "prowess" to the world.

4.4. Common Traits of Cyber Terrorism

Most cyber terrorism cases share several common traits. It is important to have a clear definition of what a cyber terrorism attack looks like in order to avoid misunderstandings which could lead to confusions

later on. Usually, the victims of cyber terrorism attacks are specifically targeted by the attacker(s) for predetermined reasons.[48] There has been random cases of attacks that have been carried out such as the release of harmful viruses and worms through the internet. However, in reality, the targets have been arranged earlier by the cyber terrorists. This is because most usually, if the attacks are more concentrated and aimed towards a specific target, there is a better chance of inflicting severe damages to that particular target.

4.5 Forms of Cyber Terrorism

Cyber terrorism as mentioned is a very serious issue and it covers vide range of attacks. Here, the kind indulgence is asked toward the definition of Cyber Crime. "Cyber Crime"' is crime that is enabled by, or that targets computers. Cyber Crime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws. However, cyber crime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data.

Some of the major tools of cyber crime may be- Botnets, Estonia, 2007, Malicious Code Hosted on Websites, Cyber Espionage etc. It is pertinent to mark here that there are other forms which could be covered under the heading of Cyber Crime & simultaneously are also the important tools for terrorist activities.

4.6 Types of cyber Terrorism Attack

There are five main types of cyber terrorism attack which are incursion, destruction , disinformation, denial of service and defacement of web sites. Some of these attacks are more severe than the others and have different objectives. It is important for us to recognize the various methods of attack in order to gain a better understanding on how they can be countered effectively.[49]
Show in the figure as 1.3 :-

48. E. Denning, Dorothy. “Is Cyber Terror Next?” 1 November 2001. URL:http://www.ssrc.org/sept11/essays/denning.htm (6 June 2003)
49. Warren M.J; Furnell S.M. “Cyber-Terrorism – The Political Evolution Of The Computer Hacker.” July 1999.

Types of Cyber Terrorism Attack

Incursion

- These type of attacks are carried out with the purposed of gaining access or penetrating into computer systems and networks to get or modify information This method is very common and widely used with a high success rate.
- There are many loop holes existing in insecure computer systems and networks and terrorists can take advantage to obtain and/or modify vital information which can be used to inflict further damages to the organization or for personal gain.

Destruction

- This method of attack is used to intrude into computer systems and networks with the main purpose of inflicting severe damage or destroying them .
- The consequences of such an attack can be disastrous, whereby organizations might be forced to be out of operations for an undetermined time, depending on the severity of the attacks.
- It can prove to be very costly for the affected organizations to get their operations up and running again and thus it will impact them hard financially and also damage their reputation.

Defacement of web sites

- This type of attack is targeted to deface the websites of the victims. The websites can either be changed totally to include messages from the cyber terrorists for propaganda or publicity purposes which might cause them to be taken down or to re-direct the users to other websites which may contain similar messages.
- The number of cases of such attacks has dwindled in the past few years thanks to a greater awareness on the issue. However, a small number of such cases is still happening and thus proper security measures will need to be taken to try to avoid such embarrassing and financially disastrous situations from happening again.

Denial of Service

- Denial of Service attacks or DOS attacks as they are more widely known are also a common method of attack. The impact of such attacks is felt the most by ecommerce enabled business that sells products or services online. Public websites are also sometimes the target of this type of attack by cyber terrorists.
- The main objective of DOS attacks is to disable or disrupt the online operations by flooding the targeted servers with huge number of packets (requests) which would ultimately lead to the servers being unable to handle normal service requests from legitimate users. The impact from such attacks can be disastrous from both an economic and social perspective where it can cause organizations to suffer from massive losses.

Disinformation

- This method is used to spread rumors or information that can have severe impact to a particular target. Regardless of whether the rumors are true or not, the use of such attacks recklessly can create uncontrollable chaos to the nation or the organization.
- This type of attack is quite difficult to contain since it can be done almost instantly without the need to access the victims computer and network systems..

4.7 Attacks via Internet

4.7 .1 Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized-zed access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking in to a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another person's website called as web hijacking.

4.7 .2 Attack on Infrastructure

Our banks and financial institutions; air, sea, rail and highway transportation systems; telecommunications; electric power grids; oil and natural gas supply lines-all are operated, controlled and facilitated by advanced computers, networks and software. Typically, the control centers and major nodes in these systems are more vulnerable to cyber than physical attack, presenting considerable opportunity for cyber terrorists. There, could be possible consequences of a cyber-terrorism act against an infrastructure or business, with a division of costs into direct and indirect implications:

(i) Direct Cost Implications by cyber terrorism:

- Loss of sales during the disruption
- Staff time, network delays, impenitent access for business users
- Increased insurance costs due to litigation
- Loss of intellectual property - reseaixh, pricing, etc.

- Costs of forensics for recovery and litigation
- Loss of critical communications in time of emergency

4.7 .3 Privacy violation

The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate[50]. The right to privacy as an independent and distinctive concept originated in the field of Tort law. In recent times, however, this right has acquired a constitutional status in **Rajagopal v. State of Tamil Nadu**[51] the violation of which attracts both civil as well as criminal consequences under the respective laws. Modem enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. With the advent of information technology the traditional concept of right to privacy has taken new dimensions, which require a different legal outlook. To meet this challenge recourse of Information Technology Act, 2000 can be taken. The various provisions of the Act protect the online privacy rights of the net users. These rights are available against private individuals as well as against cyber terrorists. Section (2) read with Section 75 of the Act provides for an application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of computer, computer system or computer network located in India, he would be liable under the provisions of the Act. This makes it clear that the long aim jurisdiction is equally available against a cyber terrorist, whose act has resulted in the damage of the property, whether tangible or intangible.

50. Merriam-Webster Online Dictionary, defamation of "privacy"
51. AIR (1994) 6 se c 632,

4.8 International Multilateral Partnership against Cyber Terrorism (IMPACT)

The International Multilateral Partnership Against Cyber Threats (IMPACT), backed by the United Nations (UN) International Telecommunication Union (ITU) and International Criminal Police Organization (Interpol), which is known as the world's first comprehensive global public private partnership between governments, industry leaders and cyber security experts to enlace the global community's capacity to prevent, defend and respond to cyber threats. It has launched its global headquarters in Cyberjaya of Malaysia on 20 March 2009. It will act as a centralized ant cyber-terrorism intelligence centre which allows its 191 member countries to be alerted on cyber-terrorism threats such as attacks against the global financial system, power grids, nuclear plants, air traffic control systems and others. IMPACT seeks to bridge the gap that exists between domestic and international spheres in countering cyber threats. It promotes greater cooperation in combating cyber threats. Impact is supported by International Telecommunication Union and it functions as an operational home for International Telecommunication Union.

4.9 Laws in Various Countries on Cyber Terrorism

4.9.1 Singapore

New laws allowing Singapore to launch pre-emptive strikes against computer hackers, have raised fears that Internet controls are being tightened and privacy is compromised in the name of fighting terrorism. The city-state's parliament has approved tough new legislation aimed at stopping "cyber terrorism," refitting to computer crimes that endanger national security, foreign relations, banking and essential public services. Security agencies can now patrol the Internet and swoop down on hackers suspected of plotting to use computer keyboards as weapons of mass disruption.

4.9.2 Malaysia

Malaysia is to establish an international centre to fight cyber-terrorism, providing an emergency response to high-tech attacks on economies and trading systems around the globe, reports said.

Prime Minister Abdullah Ahmad Badawi, during a visit to the United States said, that the facility, sited at the high-tech hub of Cyber java outside Kuala Lumpur, would be funded and supported by governments and the private sector. The New Straits Times said the centre would be modeled on the Centre for Disease Control in Atlanta, which helps to handle outbreaks of disease around the world.

Abdullah who announced the initiative at the close of the World Congress on Information Technology in Austin, Texas said the threat of cyber-terrorism was too serious for governments to ignore.

The Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism. They are helping all the member countries and training their personnel. The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 members and nonmember countries including Japan, the USA, and Canada. This treaty has a ready enforced after its ratification by Lithuania on 21March 2004.

The Association of South East Asia Nations (ASEAN) has set plans for sharing information on computer security.

4.9.3 The United Kingdom

The United Kingdom adopted Terrorism Act, 2000, which gives the definition of terrorism and also gives various provisions for Cyber terrorism.

4.9.4 Pakistan

Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life," according to the ordinance, which was published by the state-run APP news agency. The Prevention of Electronic Crimes law will be applicable to anyone who commits a crime detrimental to national security through the use of a computer or any other electronic device, the

government said in the ordinance. It listed several definitions of a "terrorist act" including stealing or copying, or attempting to steal or copy, classified information necessary to manufacture any form of chemical, biological or nuclear weapon.

4.9.5 India

Earlier the term "cyber terrorism" was absent from the terminology of the Indian law. Section 69 of the Information Technology Act was a lone strong legislative measure to counter the use of encryption by terrorists. This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource. But after the 26/11 attack on Mumbai the Government of India took strong steps to strengthen the cyber security, including prohibition of terrorist activities though cyber space by way of amending the existing Indian information Technology Act, 2000. The provision that was specifically inserted in this legislature for this purpose was section 66F which defines and describes cyber terrorism. Section 66F mentions that.[52]

(1) Whoever,

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –
(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
(iii) introducing or causing to introduce any Computer Contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of
property or disrupts or knowing that it is likely to cause damage or disruption of supplies or
services essential to the life of the community or adversely affect the critical information infrastructure specified under section70.

52. Information Technology Act 2000 (Bare Act), Universal Law Publishing Co. P\4. Ltd.(2011Xp-36

(a) Constitution of India

Any person who fails to assist the Government agency in decrypting the information sought to be intercepted is liable for imprisonment up to 7 years. Article 300A of Constitution of India states that all persons have a right to hold and enjoy their properties. In a specific case of **Bhavnagar University v. Palitana Sugar Mills Pvt. Ltd**[53] . Supreme Court applied the constitutional clause with the interpretation that anyone can enjoy his or her property rights in any manner preferred. This also includes property rights to information stored on computers or in any electronic format.

Articles 301 to 305 refer to the right for free trade. As long as an individual carries out a business in accordance with law, it cannot be interfered. Besides, free trade and any commercial activities cannot be visualized without technological rights, which mean that any distortion of those is illegal. In India these provisions have been effectively used to protect individual property rights against the actions of cyber criminals.

(b) Penal Code

A big deal of protection is also provided by Indian Penal Code. Section 22 of it gives a definition of a "movable property" stating that it also includes all corporal properties. It means that any Information stored on a computer can be conveniently regarded as a notable property as it can definitely be moved from one place to another and is not attached75. Section 29A of the Code with Section 2(1) (t) of the Information Technology Act provides that "electronic record means data, record, or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche.

53. Information Technology Act 2000 (Bare Act), Universal Law Publishing Co. P\4. Ltd.(2011Xp-36

4.10 Cyber-terrorism and Human Rights

Universal Declaration of Human Rights in its Preamble talks about a "freedom from fear and want". Freedom from fear is mostly a term of psychological nature, however, it is being used very widely nowadays especially in cases of terrorism. Article 3 of the Declaration sets the right to "security of person". As we know, term "person" also includes an environment (s)he exists in, different from the term "individual" which under one of the concepts imagines it as something abstract, apart from any other surrounding conditions. So protecting a personal security would also mean protecting his (her) social, economical and other connections, "threads" established with the environment. As long as in modem reality these are sometimes predominantly based on technology, computers or internet, cyber-terrorism protection also deals with "security of person".

Here I would also add Article 5 with its protection against "degrading treatment". Personal harm is also a part of degradation and treating a person in a current way is something that may be provided by cyber-criminal act as it was proven above.

One important provision that I would like to pay special attention to is Article 12 of the Declaration, It states: "No one shall be subjected to arbitrary interference with his privacy, nor to attacks upon his honor or reputation". "Privacy" is defined as "the quality or state of being apart from company or observation" which in combination with another definition of "freedom from unauthorized intrusion" given by the same source, also includes the privacy of computer-stored data and a right to enjoy its private state of non-interference without personal will of the possessor.

4.11 Cyber terrorism and Modern Terrorist

Cyber terrorism is an attractive option for modem terrorists, who value its anonymity, potential to inflict massive damage, psychological impact, and media appeal. This enables them to carry out acts of terrorism from their own tent, cave, bunker, or palace. Other considerations are as under[54]

1. Large variety of targets.
2. Low risk to terrorists.
3. Greater media coverage

Cyber terrorism is an attractive option for modem terrorists for several reasons.[55]

First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.

Second, cyber terrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

Over a period of time, the level of sophistication required to hack into an information system has decreased. At the same time, the quality, quantity, and availability of hacking tools has increased. Cyber warrior tools are often readily available for downloading from the Internet. A comparatively low technology adversary with minimal funding, training, maiming, and defense resort to cyber terrorism at short notice from anywhere in the world. This creates a very dangerous target-rich and low-risk combination.

54. Gabriel Weizmann. "Cyber terrorism How Real Is the Threat?", United states Institute of Peace. Special report 119, www.usip.org/pubs'specialreports/srl 19.html; (Visited on .luly22,2011).
55. Ibid.

4.12 Some incidents of cyber terrorism:

The following are notable incidents of cyber terrorism[56]:

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

One of the worst incidents of cyber terrorists at work was when crackers in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. More recently, in May 2007 Estonia was subjected to a mass cyber attack by hackers inside the Russian Federation which some evidence suggests was coordinated by the Russian government, though Russian officials deny any knowledge of this. This attack was apparently in response to the removal of a Russian World War II war memorial from downtown Estonia.

4.13 Technological Protection from Cyber Terrorism

Information Technology is the lifeline of most organizations today, and as such a disrupted information system can cause your company to lose market share and eventually bring it to its knees. 94% of companies without a tested crisis plan go out of business after a severe loss of service for two weeks or more. We are so bound as a global community that a disaster in a single major city results in significant ripple effects around the world. Cyber terrorism, weather direct or indirect, is an issue all businesses should anticipate and arrange for backup plans. Depending on the size of the company, backups of the backup plan may need to be considered.

Politically charged events frequently unleash a nest of vim's', worms and Trojan horses on the Internet, and with increasing intensity. In one day, the current Nimda vim's generated one hundred times the traffic that the code red vim's took three days to do. A group setup by the federal government to counter Cyber terrorism released a report stating that "A personal computer and a simple telephone connection

56 http://www.legalservicemadia.convarticle/ll 69-Cyber-Terrorism.html (visited on March 11,2008).

to an Internet service provider anywhere in the world are enough to cause a great deal of them. The right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend."
To protect your business in the event of a disaster you need to identify the mission critical information streams that need to be protected. This may include both print material and computer hardware and software.

4.14 Legal Protection from Cyber Terrorism

If the three sovereign organs[57] of the Constitution work collectively and in harmony with each other, the menace of cyber terrorism can be effectively curbed, if not completely eliminated.
Further, a vigilant citizenry can supplement the commitment of elimination of cyber terrorism.

4.15 Harm principle

Regarding the harm principle, cyber-terrorism does not directly attack individual interests, that is, those that belong to or serve a specific person or a set group of people. On the contrary, cyber-terrorism directly affects a collective interest, an interest that is owned by or serves the general public. As in terrorism, the collective interest directly attacked by cyber-terrorism is the democratic constitutional order. Hence, it can be affirmed that cyber-terrorism constitutes an attack against institutional, state, or national interests.

Said characteristics distinguish cyber-terrorism from common crimes like homicide or assault, but also distinguish cyber-terrorism from cybercrimes such as computer fraud, all of which directly affect individual rather than collective interests. In other words, even if cyber-terrorism harms or threatens individual interests like the life or health of others, this indirect impact is not its ultimate goal, instead the goal is a direct attack on the democratic constitutional order.

Considering the harm principle described, a wide range of situations can be established, ranging from minor to severe.

57. These are the "Legislature", ""Executives" and "Judiciary"',

First, that only the collective interest of "democratic constitutional order" is threatened. This can happen if an individual joins or forms part of a cyber-terrorist organization with a criminal agenda. In this case, for these interests to be at risk, indications that threatening actions against the democratic constitutional order have been taken are necessary.

Second, that the collective interest of "democratic constitutional order" is violated and additionally one or more individual interests are threatened. Such a situation may occur when propaganda is used in cyberspace to destabilize a political regime, in which, for example, the life or health of others is put at risk. As was said with respect to terrorism, the threat in question should be plausible or credible, as cyber-terrorist groups utilizing propaganda in cyberspace to make laughable or absurd threats towards others should not be considered cyber-terrorism.

Third, that the collective interest of "democratic constitutional order" is violated as much as one or more individual interests. This can happen if a cyber-terrorist group, in order to execute a set political agenda, remotely takes control, through a computer network, of a traffic light located on a railway line, and causes two trains in the opposite direction to share the same route, producing, for example, death or injury to its passengers.

4.16 Elements

In terms of its elements, cyber-terrorism is comprised of a teleological element and instrumental element.

Regarding the teleological element, cyber-terrorism should be committed with the aim of altering the constitutional order or to topple the legitimately elected government. By extension, the cyber-terrorist group will always have a political agenda (Warren, 2008). However, although demonstrating these facets of cyber-terrorism can be complicated in practice, it is possible to infer the presence of certain clues, among them, the remaining requirements of the notion of cyber-terrorism structure, harm principle and instrumental element. Thus, it avoids falling into a "psychologization" of the concept of cyber-terrorism which would likely be produced by defining cyber-terrorism exclusively or fundamentally based on the aims of those committing cyber-terrorist acts.

In terms of the instrumental element, cyber-terrorist acts must be executed in a manner appropriate to instil terror in people's minds (Denning, 2000), establishing a belief that anyone anywhere could be a victim of cyber-terrorism.

As can be seen, the presence of the instrumental element is very complex in the case of cyber-terrorism. In that sense, if one thinks of a terrorist attack perpetrated in the "real world", it becomes relatively easy to form the belief that anyone anywhere could be a victim of an attack. Thus, for example, if a terrorist organization carries out an explosive attack in a beach resort with tourists, it is expected that survivors will feel terror and imagine that they –or anyone who visits it– may be the next ones attacked.

Faced with the above, the question arises: When is a cyber-attack capable of generating terror in people's minds? This question has an empirical and a theoretical answer. The empirical answer exceeds the aims of this article. The theoretical answer, on the other hand, must be present considering the kind of interests that are violated or threatened with the cyber-terrorist act, beyond the attack on the collective interest of "democratic constitutional order."

To cause terror in people's minds cyber-terrorism must involve the realization of an indiscriminate attack "in" or "through" the cyberspace, with consequences in the outside world that are identified with deaths, serious injuries or other similar outcomes.

Regarding the effects of the attack, it is insufficient for cyber-terrorist attacks to merely impact inanimate objects or private property if it does not imply harm or at least danger to other interests, mainly the life or health of people.

Therefore, cyber-terrorism is not just the manipulation of data or software that causes a large number of people to lose considerable sums of money through the internet, unless such loss entails economic ruin and a consequent impact on the life or health of its victims. The destruction of data that generates the loss of relevant scientific or academic information is also not a case of cyber-terrorism, unless it implies danger to the life or health of others, for example, if the formula of a medicine is changed through the internet to make it harmful or even lethal (Hua and Bapna, 2013). Meanwhile, the mere attack of web pages by a cyber-terrorist group, for example, DOS (Denial of Services) or DDOS (Distributed Denial of Services) attacks against sites supposedly contrary to the values of Islam (Denning, 2011) or belonging to

state agencies (Hardy and Williams, 2014) do not constitute cyber-terrorism. All these cases may involve the perpetration of computer crimes, cybercrimes or common crimes, but not cyber-terrorism.

In terms of the means of the attack and, especially, the indiscriminate use of violence, cyber-terrorism cannot target objectives that have already been publicly identified. For the same reason, if a (cyber)terrorist organization threatens to assassinate a specific political leader and carries out such threat to kill them using computer networks, this would not constitute (cyber)terrorism as it lacks the very uncertainty previously outlined. A case such as the one mentioned may involve the perpetration of a computer crime, cybercrime or common crime, but not cyber-terrorism.

Instead, attacks against critical infrastructure using computer networks can constitute cyber-terrorism (Denning, 2011; Lewis, 2002), insofar as it endangers actual people. Thus, for example, if a cyber-terrorist group, through a computer network, modifies the information that is issued and received at the monitoring station of a port and thereby puts the life or health of people travelling on the monitored boats at risk, there would be cyber-terrorism, so long as all the requirements of cyber-terrorism already outlined (structure, harm principle, elements) are present.

In relation to critical infrastructure, perhaps one of the most spectacular cases on record was the 2010 attack on Iranian nuclear infrastructure through the malware "Stuxnet" (Meier, 2015). Its diffusion would have operated by means of an infected USB stick (Kochheim, 2015) that, when inserted into a computer connected to the network, would have entered the computer system and focused on the software that controlled the uranium centrifuge machines. While in principle this kind of attack can be described as cyber-terrorism, some doubts arise regarding the accreditation of the teleological element that must be present in any (cyber)terrorist attack, since to date there is no certainty of knowing who would have perpetrated this attack and, therefore, what would have been their purpose or motivation to commit it.

4.17 The challenges that cyber-terrorism creates

Like terrorism, cyber-terrorism involves a series of complex challenges in a global and technologically interconnected world, especially for those who seek to prevent and repress its perpetration. Despite this, unlike terrorism, these are challenges that are more forward looking. So far, terrorist groups "still prefer

bombs to bytes" (Denning, 2011: 3). In that sense, although cybernetic attacks can be cheaper (Weimann, 2005) and easier to execute than a physical attack (Jones, 2005), they are less dramatic and effective than attacks carried out in the "real world" (Lewis, 2002). However, cyber-terrorism constitutes a threat against which certain precautions must be taken, especially if it is considered that it can operate as a complement or suitable support for traditional terrorism (Denning, 2000). From this point of view, it is very likely that terrorism tends to combine attacks in the real world and attacks "in" or "through" the virtual world (Jones, 2005Hua and Bapna, 2013).

Because a terrorist group can use cyberspace for various purposes (Ariely, 2014), it is necessary to clearly distinguish between two situations. First, it is possible that a terrorist attack is carried out through cyberspace, which constitutes, given its structure, harm principle, and elements, a genuine case of cyber-terrorism. Second, it is possible for a terrorist group to use information and communication technologies and, particularly, the internet to carry out a series of actions linked to the objectives it pursues. Such use of the internet will not necessarily constitute cyber-terrorism but may lead to the existence of preparatory acts or facilitation of future cyber-terrorist behaviours.

The benefits that the internet implies in this area are fundamentally related to the favourable conditions it offers for the elaboration of different plans and the execution of diverse behaviours (Cohen, 2002; PovedaCriado and Torrente Barredo, 2016). First, the increasingly reduced costs of connection to the network (Meier, 2015; Neubacher, 2014) allows anyone to access the internet at any time. Second, thanks to the relatively lower costs of state-of-the-art technologies, many subjects can profit from them, including for the commission of illicit actions (Grabosky, 2009) and, certainly, (cyber)terrorist attacks (Denning, 2000).

Linked to the above, the internet is a breeding ground to coordinate (cyber)terrorist attacks (Berner, 2003; Cohen, 2002). In that sense, this network allows communication between several people without requiring that they meet physically in the same place (PovedaCriado and Torrente Barredo, 2016), since it is always possible to connect remotely (Hua and Bapna, 2013). The members of a (cyber)terrorist group can resort to communication systems that use instant messaging mobile phone applications to exchange information. They can also use software for sending text, voice, and video messages (Gillespie, 2016) or even console videogame chats (Podhradsky, D'Ovidio and Casey, 2012), which lets its users, while playing, to communicate with each other. The internet also allows for planning and implementation of an attack to be preceded by

valuable information, since (cyber)terrorist organizations can use the network as a tool for surveillance and espionage of potential targets and victims (Gillespie, 2016; Wilson, 2003).

The internet provides favourable conditions for recruiting new followers (Cano Paños, 2008; MiróLlinares, 2012), from different causes. Moreover, since it is an area in which there is no direct contact between its various actors (Gordon and Ford, 2002), it is possible that not only subjects with a strong personality or character would be interested in being part of a cyber-terrorist group, but also timid or introverted individuals and even people with psychiatric problems. From this point of view, cyberspace is a place that allows the incorporation and participation by everyone in all kinds of initiatives, including criminal or actual cyber-terrorist groups.

In addition, cyberspace is an ideal environment to indoctrinate and train the different members of a cyber-terrorist organization (MiróLlinares, 2012; PovedaCriado and Torrente Barredo, 2016). In that sense, it is possible that the members of the cyber-terrorist group exchange ideas (or ideologies) and strategies of action, including technical knowledge (for example, the manufacture of an explosive or the development of software) to carry out attacks in the future. Moreover, cyberspace facilitates alliances between people and groups with similar objectives and interests, also allowing them to mutually empower each other (Gordon and Ford, 2002) in the sphere of cyber-terrorism.

In cyberspace, it is possible to spread propaganda (Cohen, 2002) easily and automatically. The technical costs to transmit a certain message, while maintaining the anonymity of its sender (Weimann, 2005), are quite low and the communication in question can be disseminated and replicated without prior censorship, innumerable times and at full speed (PovedaCriado and Torrente Barredo, 2016). This allows for many people to know the message of a (cyber)terrorist group, even people who are not direct recipients of that kind of communication. With this, the (cyber)terrorist organization gains publicity (Goodman, Kirk and Kirk, 2007), notoriety, and eventual new sympathizers. In the same way, the internet allows a (cyber)terrorist group to announce the future execution of a (cyber)terrorist attack or to claim responsibility for and, if necessary, justify the previous execution of a (cyber)terrorist attack (PovedaCriado and Torrente Barredo, 2016).

Likewise, and this is particularly important, the internet provides adequate conditions to articulate financing strategies for (cyber)terrorist groups (Cohen, 2002; Gillespie, 2016). Financing mechanisms linked to cyberspace can be distinguished into two situations. In the first situation, members of a (cyber)terrorist

group may commit cybercrimes to finance their various activities, for example, cyberspace fraud (Lewis, 2002). In the second situation, bank transfers may be made for sums of money (Goodman, Kirk and Kirk, 2007) obtained lawfully or unlawfully, while payments may be made for the sale of goods or services online (PovedaCriado and Torrente Barredo, 2016). In any case, such sources of financing can be used to financially maintain the members of the cyber-terrorist group, to recruit and train new members, and to prepare and execute attacks, amongst other things.

In the future, there are many areas that could become possible targets of cyber-terrorist attacks. Consider, for example, the development of intelligent vehicles, whose driving could be controlled (Denning, 2011) by groups of cyber-terrorists through computer networks; or the possibility that such organizations intervene, through the internet, in the navigation of ships and aircraft. To this can be added the remote alteration of sensitive databases, for example, those that establish the pharmaceutical industry's medication formulas (Weimann, 2005). The same can be said of a possible increase, even at a mass scale, in attacks against critical infrastructure. In this context, the more devices and infrastructure (linked to the life and health of people) depend on the existence and operation of computer networks, the more vulnerable these devices and infrastructure will be in the face of possible cyber-terrorist attacks (Lewis, 2002). And the more likely those cyber-terrorist groups will effectively exploit such vulnerabilities.

However, perhaps one of the biggest challenges involved in cyber-terrorism has to do with the lack of certainty about its real dimensions and potential. In that sense, it is not clear to what extent the threat of cyber-terrorism is exaggerated, even for economic reasons. Think, for example, of the complex industry that has in fact developed around cyber-security, including conducting research and publishing documents, hiring experts, creating software, etc. (Weimann, 2005). Therefore, it is crucial that there is reliable information on the specific scope of the phenomenon of cyber-terrorism, so that the various reactions that it generates are rational, proportionate and adequate.

4.18 Means by which the Internet is utilized for terrorist purposes

The means by which the Internet is often utilized to promote and support acts of terrorism. This approach has resulted in the identification of six sometimes overlapping categories: propaganda

(including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber-attacks. Each of these categories is addressed in greater detail below.

1. Propaganda

One of the primary uses of the Internet by terrorists is for the dissemination of propaganda. Propaganda generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers. Nevertheless, what constitutes terrorist propaganda, as opposed to legitimate advocacy of a viewpoint, is often a subjective assessment. Further, the dissemination of propaganda is generally not, in and of itself, a prohibited activity. One of the basic tenets of international law is the protection of fundamental human rights, which include the right to freedom of expression (see discussion in section I.D below). This guarantees an individual the right to share an opinion or distribute content which may be considered objectionable by others, subject to certain limited exceptions. One commonly accepted exclusion with respect to that right is the prohibition against the distribution of certain categories of sexually explicit content, the prohibition of which is deemed to be in the public interest in order to protect certain vulnerable groups. Other exclusions, all of which must be provided for by law and shown to be necessary, may include communications that are clearly detrimental to the protection of national security and communications that are both intended and likely to incite acts of violence against individuals or specific groups of individuals.

The promotion of violence is a common theme in terrorism-related propaganda. The broad reach of content distributed via the Internet exponentially increases the audience that may be affected. Further, the ability to directly distribute content via the Internet diminishes the reliance on traditional channels of communication, such as news services, which may take steps to independently evaluate the credibility of the information provided or to edit or omit aspects deemed to be unduly provocative. Internet propaganda may also include content such as video footage of violent acts of terrorism or video games

developed by terrorist organizations that simulate acts of terrorism and encourage the user to engage in role-play, by acting the part of a virtual terrorist.

The promotion of extremist rhetoric encouraging violent acts is also a common trend across the growing range of Internet-based platforms that host user-generated content. Content that might formerly have been distributed to a relatively limited audience, in person or via physical media such as compact discs (CDs) and digital video discs (DVDs), has increasingly migrated to the Internet. Such content may be distributed using a broad range of tools, such as dedicated websites, targeted virtual chat rooms and forums, online magazines, social networking platforms such as Twitter and Facebook, and popular video and file-sharing websites, such as YouTube and Rapid share, respectively. The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content.

The fundamental threat posed by terrorist propaganda relates to the manner in which it is used and the intent with which it is disseminated. Terrorist propaganda distributed via the Internet covers a range of objectives and audiences. It may be tailored, inter alia, to potential or actual supporters or opponents of an organization or shared extremist belief, to direct or indirect victims of acts of terrorism or to the international community or a subset thereof. Propaganda aimed at potential or actual supporters may be focused on recruitment, radicalization and incitement to terrorism, through messages conveying pride, accomplishment and dedication to an extremist goal. It may also be used to demonstrate the effective execution of terrorist attacks to those who have provided financial support. Other objectives of terrorist propaganda may include the use of psychological manipulation to undermine an individual's belief in certain collective social values, or to propagate a sense of heightened anxiety, fear or panic in a population or subset of the population. This may be achieved through the dissemination of disinformation, rumors, threats of violence or images relating to provocative acts of violence. The intended audience may include direct viewers of content, as well as those affected by potential publicity generated by such material. With respect to the wider international community, the goal is often to convey a desire to achieve noble political ends.

(a) Recruitment

The Internet may be used not only as a means to publish extremist rhetoric and videos, but also a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda. Terrorist organizations increasingly use propaganda distributed via platforms such as password-protected websites and restrict teaches Internet chat groups as a means of clandestine recruitment. The reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits. Restricted access cyber forums offer a venue for recruits to learn about, and provide support to, terrorist organizations and to engage in direct actions in the furtherance of terrorist objectives.

The use of technological barriers to entry to recruitment platforms also increases the complexity of tracking terrorism-related activity by intelligence and law enforcement personnel.

Propaganda may be adapted to account for demographic factors, such as age or gender, as well as social or economic circumstances.

Terrorist propaganda is often tailored to appeal to vulnerable and marginalized groups in society. The process of recruitment and radicalization commonly capitalizes on an individual's sentiments of injustice, exclusion or humiliation

The Internet may be a particularly effective medium for the recruitment of minors, who comprise a high proportion of users. Propaganda disseminated via the Internet with the aim of recruiting minors may take the form of cartoons, popular music videos or computer games. Tactics employed by websites maintained by terrorist organizations or their affiliates to target minors have included mixing cartoons and children's stories with messages promoting and glorifying acts of terrorism, such as suicide attacks. Similarly, some terrorist organizations have designed online video games intended to be used as recruitment and training tools. Such games may promote the use of violence against a State or prominent political figure, rewarding virtual successes, and may be offered in multiple languages to appeal to a broad audience.

(b) Incitement

While propaganda per se is not generally prohibited, the use of propaganda by terrorists to incite acts of terrorism is considered unlawful by many Member States. The Internet provides an abundance of material and opportunities to download, edit and distribute content that may be considered unlawful glorification of, or provocation to, acts of terrorism. It should be noted, however, that some intergovernmental and human rights mechanisms have expressed doubt that the concept of "glorification" of terrorism is sufficiently narrow and precise to serve as a basis for criminal sanctions compliant with the requirements of the principle of legality and the permissible limitations of the right to freedom of expression, as enshrined in articles 15 and 19 of the International Covenant on Civil and Political Rights.

It is important to emphasize the distinction between mere propaganda and material intended to incite acts of terrorism. In several Member States, in order to be held liable for incitement to terrorism, a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required. For example, in a contribution to the expert group meetings, a French expert indicated that the dissemination of instructive materials on explosives would not be considered a violation of French law unless the communication contained information specifying that the material was shared in furtherance of a terrorist purpose.

Preventing and deterring incitement to terrorism in the interest of protecting national security and public order are legitimate grounds for limiting freedom of expression, as provided under article 19, paragraph 3, of the International Covenant on Civil and Political Rights. These grounds are also consistent with article 20, paragraph 2, of that Covenant, which requires States to prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

In the light of the fundamental nature of the right to freedom of expression, however, any restrictions on the exercise of this right must be both necessary and proportional to the threat posed. The right to freedom of expression is also linked to other important rights, including the rights to freedom of thought, conscience and religion, belief and opinion.

(c) Radicalization

Recruitment, radicalization and incitement to terrorism may be viewed as points along a continuum. Radicalization refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies. The process of radicalization often involves the use of propaganda, whether communicated in person or via the Internet, over time. The length of time and the effectiveness of the propaganda and other persuasive means employed vary depending on individual circumstances and relationships.

1. Financing

Terrorist organizations and supporters may also use the Internet to finance acts of terrorism. The manner in which terrorists use the Internet to raise and collect funds and resources may be classified into four general categories: direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations.

Direct solicitation refers to the use of websites, chat groups, mass mailings and targeted communications to request donations from supporters. Websites may also be used as online stores, offering books, audio and video recordings and other items to supporters. Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties.

Funds transfers are often made by electronic wire transfer, credit card or alternate payment facilities available via services such as PayPal or Skype.

Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. An example of the use of illicit gains to finance acts of terrorism can be seen in the United Kingdom case against Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Tousle of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several

countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity.[58]

Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes. Some terrorist organizations have been known to establish shell corporations, disguised as philanthropic undertakings, to solicit online donations. These organizations may claim to support humanitarian goals while in fact donations are used to fund acts of terrorism. Examples of overtly charitable organizations used for terrorist ends include the innocuously named Benevolence International Foundation, Global Relief Foundation and the Holy Land Foundation for Relief and Development, all of which used fraudulent means to finance terrorist organizations in the Middle East. Terrorists may also infiltrate branches of charitable organizations, which they use as a cover to promote the ideologies of terrorist organizations or to provide material support to militant groups.

3. Training

In recent years, terrorist organizations have increasingly turned to the Internet as an alternative training ground for terrorists. There is a growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice. These Internet platforms also provide detailed instructions, often in easily accessible multimedia format and multiple languages, on topics such as how to join terrorist organizations; how to construct explosives, firearms or other weapons or hazardous materials; and how to plan and execute terrorist attacks. The platforms act as a virtual training camp. They are also used to share, inter alia, specific methods, techniques or operational knowledge for the purpose of committing an act of terrorism.

For example, *Inspire* is an online magazine allegedly published by Al-Qaida in the Arabian Peninsula with the stated objective of enabling Muslims to train for jihad at home. It contains a large amount of ideological material aimed at encouraging terrorism, including statements attributed to Osama Bin

58. Net Press. "What is Cyber Warfare?" 2001. URL: http://www.netxpress.com.pk/archives/articles/cwfa1.shtml (10 April 2003).

Laden, Sheikh Ayman al-Zawahiri and other well-known Al-Qaida figures. The fall 2010 edition included practical instructional material on how to adapt a four-wheel-drive vehicle to carry out an attack on members of the public and how a lone individual could launch an indiscriminate attack by shooting a gun from a tower. The publication even suggested a target city for such an attack, in order to increase the chances of killing a member of the Government.

Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications and online activity through the use of available encryption tools and anonym zing techniques. The interactive nature of Internet platforms helps build a sense of community among individuals from different geographical locations and backgrounds, encouraging the creation of networks for the exchange of instructional and tactical material.

4. Planning

Many criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology. In particular, planning an act of terrorism typically involves remote communication among several parties. A recent case from France, *Public Prosecutor v. Hicheur*,15 illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications within and between organizations promoting violent extremism, as well as across borders.

Public Prosecutor v. Hicheur

In May 2012, a French court sentenced Adlène Hicheur, an Algerian-born French national, to five years of imprisonment for participation in a criminal conspiracy for the preparation of a terrorist act (under Article 421-1 et. seq. of the French Criminal Code), relating to acts that took place in France in 2008 and 2009.

The investigation implicating Hicheur, a nuclear physicist, was launched in early 2008 in connection with an e-mail communication containing jihadist content, which was sent to the website of the

President of the French Republic and traced back to a member of Al-Qaida in the Islamic Maghreb (AQIM).

A preservation order issued in January 2009 enabled the authorities to identify e-mail exchanges between the AQIM member and, inter alia, the Global Islamic Media Front (GIMF) and the Rafidayin Center, a website with the stated goal of hosting and disseminating Al- Qaida documents, audio and video recordings, statements from warlords and suicide attackers and the materials of other extremist Islamic groups. The e-mail exchanges were encrypted using the dedicated software "Asrar el Mojahedeen" or "Mujahedeen Secrets", which includes 256-bit encryption, variable stealth cipher encryption keys, RSA 2,048-bit encryption keys and encrypted chat-forum-supported instant messaging.

Dozens of decrypted e-mail communications were presented at trial. The prosecution claimed that the content of those e-mails indicated that Hicheur actively performed, inter alia, the following acts in support of the jihadist network, notably on behalf of the Rafidayin Center: Translated, encrypted, compressed and password-protected pro-jihadist materials, including documents and videos, which he then uploaded and circulated via the Internet. Distributed the encryption software "Mujahedeen Secrets" to facilitate covert Internet communications Conspired with an AQIM member to organize and coordinate pro-jihadist activities, including but not limited to providing financial support to the jihadist cause, disseminating pro-jihadist information and supporting the creation of an operational unit in Europe, and in particular in France, to potentially prepare terrorist attacks Acted as moderator on the pro-jihadist Ribaat website Took concrete steps to provide financial support to AQIM, including through the attempted use of PayPal and other virtual payment systems.

At trial, the prosecution claimed that those communications proved Hicheur had been fully aware that he was engaging with a member of AQIM, and that he had acted knowingly and willingly as an intermediary between jihadist fighters and GIMF. At the conclusion of the trial, the Court held that; "Hicheur became … a logistical and media support for this terrorist structure for which the 'media jihad' is crucial".

The Court further held that "Adlène Hicheur, by giving his agreement to the establishment of an operational unit linked to AQIM in Europe, or even in France, and determining targets or categories of

targets to be struck, participated in a group [AQIM] specifically created to prepare acts of terrorism." The court therefore found sufficient evidence to demonstrate, as required under the French Criminal Code, that Hicheur had provided not merely intellectual support but also direct logistical support to a clearly identified terrorist plan. The decision of the court is appealable.

Steps may also be taken via the Internet to identify a potential target of an attack and the most effective means of achieving the terrorist purpose. These preparatory steps may range from obtaining instructions on recommended methods of attack to collecting open-source and other information regarding a proposed target. The ability of the Internet to bridge distances and borders, and the vast amount of information publicly available in cyberspace, make the Internet a key tool in the planning of terrorist acts.

(a) Preparatory secret communication

The most basic function of the Internet is to facilitate communication. Terrorists have become increasingly sophisticated at exploiting communications technologies for anonymous communication related to the planning of terrorist acts. A simple online e-mail account may be used by terrorists for electronic, or virtual, "dead dropping" of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves minimal electronic traces, but which may be accessed from any Internet terminal worldwide by multiple individuals with the relevant password.

There is also an abundance of more sophisticated technologies that increase the difficulty of identifying the originator, recipient or content of Internet communications. Encryption tools and anonym zing software are readily available online for download. These tools may, inter alia, mask the unique Internet Protocol (IP) address that identifies each device used to access the Internet and its location, reroute Internet communications via one or more servers to jurisdictions with lower levels of enforcement against terrorist activity and/or encrypt traffic data relating to websites accessed. Steganography, the hiding of messages in images, may also be used.

(b) Publicly available information

Organizations and individuals often publish extensive amounts of information on the Internet. In the case of organizations, this may be a result in part of a desire to promote their activities and streamline their interaction with the public. Some sensitive information that may be used by terrorists for illicit purposes is also made available through Internet search engines, which may catalogue and retrieve inadequately protected information from millions of websites. Further, online access to detailed logistical information, such as real-time closed-circuit television footage, and applications such as Google Earth, which is intended for and primarily used by individuals for legitimate ends, may be misused by those intent on benefiting from the free access to high-resolution satellite imagery, maps and information on terrain and buildings for the reconnaissance of potential targets from a remote computer terminal.

Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flicker and blogging platforms, individuals also publish, voluntarily or inadvertently, an unprecedented amount of sensitive information on the Internet. While the intent of those distributing the information may be to provide news or other updates to their audience for informational or social purposes, some of this information may be misappropriated and used for the benefit of criminal activity.

5. Execution

Elements of the categories described above may be employed in the use of the Internet for the execution of terrorist acts. For example, explicit threats of violence, including in relation to the use of weapons, may be disseminated via the Internet to induce anxiety, fear or panic in a population or subset of the population. In many Member States, the act of issuing such threats, even if unfulfilled, may be deemed an offence. For example, in China, the fabrication of a threat and/or the circulation of a threat that is known to be fabricated in relation to the use of bombs or biological, chemical, or radioactive materials or other weapons, when committed with the intent “to seriously disrupt public order”, is criminalized

under domestic legislation.16 Internet communications may also be used as a means to communicate with potential victims or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the attacks of 11 September 2001 in the United States.

The use of the Internet in furtherance of the execution of acts of terrorism may, inter alia, offer logistical advantages, reduce the likelihood of detection or obscure the identity of responsible parties. Internet activity may also facilitate the acquisition of items necessary for the execution of the attack. Terrorists may purchase individual components or services required to perpetrate violent acts of terrorism by means of electronic commerce. Misappropriated credit cards or other forms of compromised electronic payment may be used to finance such purchases.

4. Cyber-attacks

A cyber-attack generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware,phlooding or other means of unauthorized or malicious access. Cyber-attacks may bear the characteristics of an act of terrorism, including the fundamental desire to instill fear in furtherance of political or social objectives. An example of a cyber-attack was seen in Israel in January 2012, involving the targeting of multiple symbolic Israeli websites, such as the websites of the Tel Aviv Stock Exchange and the national airline, and the unauthorized disclosure of the credit card and account details of thousands of Israeli nationals.19 While a considerable amount of attention has focused in recent years on the threat of cyberattacks by terrorists, that topic is beyond the scope of the present publication and, as such, will not be a subject of analysis.

4.19. Uses of the Internet for countering terrorist activity

While terrorists have developed many ways to use the Internet in furtherance of illicit purposes, their use of the Internet also provides opportunities for the gathering of intelligence and other activities to prevent and counter acts of terrorism, as well as for the gathering of evidence for the prosecution of such acts. A significant amount of knowledge about the functioning, activities and sometimes the targets of terrorist organizations is derived from website, chat room and other Internet communications. Further, increased Internet use for terrorist purposes provides a corresponding increase in the availability of electronic data which may be compiled and analyzed for counter-terrorism purposes. Law enforcement, intelligence and other authorities are developing increasingly sophisticated tools to proactively prevent, detect and deter terrorist activity involving use of the Internet. The use of traditional investigative means, such as dedicated translation resources for the timely identification of potential terrorist threats, is also expanding.

Online discussions provide an opportunity to present opposing viewpoints or to engage in constructive debate, which may have the effect of discouraging potential supporters. Counter-narratives with a strong factual foundation may be conveyed through online discussion forums, images and videos. Successful messages may also demonstrate empathy with the underlying issues that contribute to radicalization, such as political and social conditions, and highlight alternatives to violent means of achieving the desired outcomes.20 Strategic communications that provide counter-narratives to terrorist propaganda may also be disseminated via the Internet, in multiple languages, to reach a broad, geographically diverse audience.

The Center for Strategic Counterterrorism Communications, based in the United States, offers an example of a recently launched inter-agency initiative which is aimed at reducing radicalization and extremist violence by identifying in a timely manner extremist propaganda, inter alia, on the Internet and responding swiftly with targeted counter-narratives via a wide range of communications technologies, including digital tools. For instance, in May 2012, the Center was cited as having responded, within 48 hours, to banner advertisements promoting extremist violence posted on various websites by Al-Qaida in the Arabian Peninsula, with counter-advertisements on the same websites featuring an altered

version of that same message that was intended to convey that the victims of the terrorist organization's activities were Yemeni nationals.

The counter-narrative campaign involved cooperation among the United States Department of State, the intelligence community and the military. The Center also uses media platforms such as Facebook and YouTube for counter-narrative communications.

4.20. Rule-of-law considerations

Respect for human rights and the rule of law is an integral part of the fight against terrorism. Due care must be taken to respect international human rights standards in all phases of counter-terrorism initiatives, from preventive intelligence gathering to ensuring due process in the prosecution of suspects. This requires the development of national counter-terrorism legislation and practices that promote and protect fundamental human rights and the rule of law.

States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights, in particular the rights to life, liberty and physical integrity of individuals and the territorial integrity and security of States.

Effective counter-terrorism measures and the protection of human rights are complementary and mutually reinforcing objectives which must be pursued together. Counterterrorism initiatives relating to Internet use may have an impact on the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and a fair trial. While a comprehensive analysis of human rights issues is beyond the scope of the present publication, it is important to highlight key areas for consideration.

4.20 Statistics of Cyber Terrorism

Cybercrimes in India almost doubled in 2017, according to statistics released by the National Crime Record Bureau (NCRB) on October 22. Cybercrime accounted for less than a percentage (0.43%) or 21,796 cases of a total of 50 lakh cognizable crimes in India. Karnataka had the highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttar Pradesh. India recorded over 9,500, 11,500 and 12,000 cases of cybercrime in 2014, 2015 and 2016 respectively. The data for 2017 comes after a two-year delay, with the Centre blaming states in providing statistics for compilation.[59]

As per the report, "During 2017, 56% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7% (1,460 cases) and causing disrepute with 4.6% (1,002 cases)."

Publishing/transmitting of material containing sexually explicit under the IT Act: NCRB has divided this section into three parts. The first two, Section 67A, Section 67B of the IT Act, deal with publishing/transmitting sexually explicit content and depiction of children in a sexually explicit way respectively, in electronic form. The exact offence for the third section was not clearly specified in the report.

Publishing material containing sexually explicit act on the internet (Sec67A)		**Publishing material depicting children in a sexually explicit act (Sec67B)**		**Publication of obscene sexually explicit act in electronic form (not specified in the report)**	
Assam	92	Uttar Pradesh	16	Uttar Pradesh	517
Karnataka	42	Assam	8	Assam	288
Telangana	35	Madhya Pradesh	7	Karnataka	157
Maharashtra	27	Himachal Pradesh	4	West Bengal	90
Odisha	24	Rajasthan/Tamil Nadu	2	Haryana	83
Total India	401	Total India	46	Total India	1768

59. www.medianama.com

The total number of offenses under the IT Act was the highest in Uttar Pradesh, followed by Karnataka (3,152), Rajasthan (950), Assam (941) and Maharashtra (586). However, the total number of offenses under the IT Act across the country stood at 13,635.

Cyber-stalking or bullying of women/children (Sec 354D IPC)

State	No. of Cases
Maharashtra	301
Andhra Pradesh	48
Haryana	27
Telangana	26
Madhya Pradesh	25
Total India	542

North-eastern states such as Arunachal Pradesh, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim, and Tripura did not have any registered cases related to cyber stalking or cyberbullying.

Cases related to violation of privacy in cyberspace under the IT Act:

In 2017, Assam had the highest number of cases (60) registered for violation of privacy. On the other hand, Uttar Pradesh had 47 such cases, Karnataka had 38, Kerala had 35 and Maharashtra had 22 registered cases. States such as Bihar, Jharkhand, Goa, Chhattisgarh, Jammu & Kashmir (now union territories), Meghalaya, Manipur, Nagaland, Odessa, Tripura, and Punjab did not have any case registered related to violation of privacy on the internet. The total number of such cases registered was 245.

Cyber terrorism (Section 66F) under the IT Act:

There were 13 registered cases related to cyber terrorism across the country. Himachal Pradesh had 5 registered cases related to cyber terrorism, which was the highest in the country. While Assam had 4, other states such as Kerala, Tamil Nadu, West Bengal had 1 each.

Frauds related to ATM, online banking, One Time Password (OTP) under section 465, 468-471 IPC

ATM		Online Banking Frauds		OTP Frauds	
Maharashtra	598	Maharashtra	345	Madhya Pradesh	122
Bihar	324	Odisha	116	Andhra Pradesh	62
Odisha	168	Telangana	111	Telangana	61
Uttar Pradesh	120	Uttar Pradesh	69	Uttar Pradesh	18
Telangana	56	Gujarat	42	Rajasthan	16
India total	1543	India total	804	India total	334

Fake news on social media (Sec. 505) under the IT Act:

Section 505 of the IPC is for statements conducing to public mischief. As per the report, a total of 170 cases were registered for cases related to fake news on social media platforms. List for the top five states has been given below:

State	No. of Cases
Assam	56
Uttar Pradesh	21
Madhya Pradesh	1
Odisha	13
Kerala	12
Total India	170

Online gambling under the IT Act cases:

States such as Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Himachal Pradesh, Tamil Nadu, Rajasthan, West Bengal, and Tripura did account for any registered case for online gambling. Details for the top five states have been given in the table below:

States	No. of cases
Jharkhand	16
Madhya Pradesh	10
Uttar Pradesh	3
Maharashtra/ Punjab	2
Karnataka	1
Total India	45

In 2017, a total 11,601 persons were arrested for cyber crime cases, 8,306 were charge sheeted, and only 162 were convicted. It is worth noting that the central government had set-up the National Informatics Centre – Computer Emergency Response Team (CERT-In) and the Home Ministry had set up the Indian Cyber Crime Coordination Centre (14C) to combat cybercrime in the country.

CHAPTER V

SUGGESTION

&

COUNCLUSION

5.0 CONCLUSIONS

Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. There are various interpretations of the term cyber terrorism. It is often difficult to make a clear distinction between cybercrime and cyber terrorism.

Nevertheless, cyber terrorism differs from other criminal forms of action in cyberspace primarily in its goals, which are those common to political terrorism in general. The cyber terrorist differs substantially from the hacker, computer hooligan, or computer thief, whose action sure motivated by greed or hooliganism. The main tactics of cyber terrorism include ensuring that this form of cybercrime has dangerous consequences, is well known by the population, has broad public resonance, and creates an atmosphere that threatens repetition of the act without identifying a particular target. Cyber terrorism is oriented toward using various forms and methods of knocking out the information infrastructure of a state or using the information infrastructure to create a situation producing catastrophic consequences for society and the state. Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided. The truth is that the criminals have changed their methods and have started relying on the advanced technology, and in order to deal with them the society, the legal, and the law enforcement authorities, the private corporations and organizations will also have to change their mechanism to combat it. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardwire and software's so that they can efficiently fight the cyber criminals. Thus, necessary facilities must be established in various parts of the country so that crime in the virtual world can be controlled'. Another aspect which needs to be highlighted is that a culture of continuous cyber education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is very dynamic as the knowledge of today becomes obsolete in a very short time. Lastly the preamble of the Information Technology Act, 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the Act. Has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act, 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the Act is not to suppress the criminal

activity, but this act has defined certain offences and penalties to overpower such omissions, which is understood to come within the characterization of cyber crimes. From this, it can be inferred that the law cannot afford to be static, it has to be change with the changing times and viz. cyber space. This is all the more required, that many applications of the technology can be used for the battement of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy-cam case. The bottom-line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

In the information age the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of trans-national crimes known as "cyber crimes". Cyber crimes have virtually no boundaries and may affect every country in the world. Cyber crimes are "any crime which is committed with tile help of computer and telecommunication technology", with the purpose of influencing the functioning of computer or computer systems. To understand cyber crime as a significantly new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently affecting countries worldwide. Free flow of uncensored information on electronic networks and websites is as attractive to insurgents and extremists groups as it is to dissidents proclaiming their human rights just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crimes. Since users of computer system and internet day by day are increasing worldwide. It has become easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by citizens while using the internet which will assist in challenging this major threat of Cyber Crime.

The problem of cyber terrorism is multilateral having varied facets and dimensions. Its solution requires rigorous application of energy and resources. It must be noted that law is always seven steps behind the technology. This is so because we have a tendency to make laws when the problem reaches at its zenith. We do not appreciate the need of the hour till the problem takes a precarious dimension. At that stage, it is always very difficult, if not impossible, to deal with that problem. This is more so in case of offences and violations involving information technology. One of the arguments, which are always advanced to justify this stand of non-enactment, is that "the measures suggested are not adequate to deal with the problem". It must be appreciated that "something is better than nothing". The ultimate solution to any problem is not to enact a plethora of statutes but their rigorous and dedicated enforcement. The courts may apply the existing laws in a progressive, updating and purposive manner. It must be appreciated that it is not the "enactment" of a law but the desire, will and efforts to accept and enforce it in its true letter and spirit, which can confer the most strongest, secure and safes! protection for any purpose. The enforcement of these rights requires a "qualitative effort" and joint a 'quantitative effort". Thus, till a law

dealing expressly with cyber terrorism is enacted, we must not feel shy and hesitant to use the existing provisions.

In summing up, as the contemporary world is basking in the achievements in the field of communications and information technology, it has become highly imperative to check the emergence and growing menace of Cyber Crime.

Cyber terrorism is distinguished from terrorism by the "place" in which it is perpetrated or by the "medium" through which it is perpetrated, that is, cyberspace. From this point of view, cyber terrorism is not an autonomous crime, but implies a kind of terrorism characterized by a unique method of execution.

Cyber terrorism must comply with the structure, harm principle and elements that define terrorism. Consequently, if these are not verified, we may be in the presence of a cybercrime and not cyber terrorism (for example a computer sabotage.) In terms of its structure, cyber terrorism requires the existence of an organization destined to perpetrate (cyber)terrorist attacks. Regarding its harm principle, cyber terrorism must directly violate a collective interest identified with the democratic constitutional order. In terms of its elements, cyber terrorism must be executed with the specific purpose of altering constitutional order or to topple the legitimately elected government; and must be carried out in a manner appropriate to instil terror in people's minds, establishing a belief that anyone anywhere could be a victim of an attack.

Finally, cyber terrorism creates several challenges in a global and technologically interconnected world. Committing cyber terrorism involves the use of the internet, which offers a series of advantages for those participating in the act. In addition, because the real dimensions and potential of cyber terrorism are not yet clear, reacting with preparation becomes difficult.

5.1 SUGGESTIONS:-

Although it's very big challenge before government to fight with hidden war in form of cyber terrorism because some time these activities may be organized and planned by enemy country/s rather than an individual or any small group but by using following precautions we can minimize the possibilities to commit these crime-

- There is a need of specific provision with a clear definition of 'cyber terrorism'. We may say that 'cyber terrorism is the use of computer as tool or target to cause unpredictable violence and threat in the mind of general people about safety, security and in the mind of Government about national security, safety and interest etc'
- There is need to evolve international standard of security measures.
- Necessary steps must be taken to enable concerning bodies.
- Computer security and awareness training
- Continuing awareness and education regarding terrorist trends and methodologies
- Future readiness to defend against attacks
- Establishment of special court, e-court, in which complain can register on-line and on the date of hearing video conferencing should be used to avoid physical presence.
- Sensitive information should not be stored in the computer systems which are connected to the internet.
- Background of outsourcing agencies should be check prior to outsource any assignment, task to maintain information security inform of authenticity, confidentiality and authenticity of data.
- Special training programmer for judicial officers to deal with cases related to cybercrimes.
- Effective use of intelligence gathered from all sources
- Ministries and departments have been advised to update IT systems and carry out regular audits to ensure an error-free system.
- There must be a specific police force to deal with cybercrimes in the country.
- Separate laws for each of the classification of cybercrime instead of amending the Information Technology Act.
- Creation of special enforcement agencies to deal exclusively with cyber laws.
- Government should impose a ban on websites that exclusively display pornography and hate speeches
- Continued enhancement of resources which are essential to make Network mush secure and robust
- Public/Private interaction to get mixes approach of advanced technology and expert implementation mechanism
- Cyber ethics should be including as a subject in various curriculum at school and college level.

- Establishment of e-cops in those city which contains economic importance
- Promotion of Research and Development in the field of information security
- A techno-legal panel for provide training to various concerning departments.
- Last but not the least creation of awareness among each and every part of administration and society.

5.2 POLICIES RECOMMENDED FOR CYBER CRIME PREVENTION

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bringing into practical part so that the practices are easier to implement. Policies recommended are:

- **(i)** Integrated policies are required to ensure the effective benefits from the Information system. The basic challenge and issue in the development of a cyber society, is the lack of financial and trained human resources.
- **(ii)** A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secure and free from cyber crime and in reach to a common man.
- **(iii)** Promotion of Research & Development in ICTs area and also in Human Resource Development as a core part of the system.
- **(iv)** Up to date, common, and mutually supporting cyber laws should be there to fight with cyber crime and protection of intellectual property rights towards the creation of cyber crime free information society
- **(v)** Adoption of ICTs standards, regulation, and quality assurance to foster high quality and secure services and productions that keep competition in place for the benefits of the communities with in each country.
- **(vi)** High levels of awareness among the each part of the society should be there with regard to information security and cyber crime.
- **(vii)** Effective mechanisms should be there for detection and prevention of cyber crime and improving protection against, detection of, and responses to, cyber crime, at the lower level itself.

- **(viii)** Conduct national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and the private sector, using different media.
- **(ix)** Educate and involve the media professionals, citizen and then encourage them to increase public awareness. Engage large private sector corporations
- **(x)** Emphasis should be laid on less developed countries on effective systems, for protection against, detection of and responses to cyber crime.
- **(xi)** Promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.
- **(xii)** Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- **(xiii)** Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- **(xiv)** Prevention is better than cure. Awareness regarding education and technical support to prevent e-crime is essential, but without discouraging the development of e-commerce.

Adoption of these measures will go a long way in preventing and controlling cyber terrorism and cyber crime which has not only reached menacing proportion but is also likely to increase in foreseeable future. To conclude this study, it may be said on the basis of the discussion in the foregoing chapters that cyber world is a recent origin. Various preventive measures have been taken law & mechanism evolved to check the crime in the cyber world. But these mechanisms are not sufficient to check or control the cyber crime, although the law and enforcement agency has been evolved to check this particular crime. There is however need to undertake research work on the protection of the cyber crime from different angle and so as to find out how it can be minimize it and with the use of internet.

BIBLIOGRAPHY

BOOKS

1. Astt Narayan - LK Thakur, 'Internet Marketing E-Commerce and Cyber Laws' Authors Press, Delhi, 2000.

2. Bama, Yogesh, 'Criminal Activities In Cyberworld.' Dominent Pubhshers and Distributei-s, New Delhi, 2005.

3. Barua, Yogesh and P. Dayal Denzyl, 'Cyber Crimes - Notorious Aspects of the Humans and the Net.' Dominent Publishers and Distributers, New Delhi, 2001.

4. Chopra Deepti and Keith Merill, 'Cyber Cops, Cyber Criminals and the Internet: I.K. International Vwt. Ltd., New Delhi, 2002.

5. Chris Reed & John Angel, 'Computer Crime & Computer Law.' ed.-S , Oxford University Press, Delhi, 2005.

6. Dr Gandhi; K.P.C, 'Introduction to computer related crimes.' CBI Bulletin, Delhi. 7. Dr. Ahmad Farroq, 'Cyber Law in India (Law on Internet).' New Era Law Publications, Delhi, 2011.

8. Dr. Choubey, R.K, 'An Introduction to cyber crime & cyber law.' ed2008, Kama! Law House, Kolkata, 2009.

9. Dr. Lakshamanan A.R., 'The Judges Speaks.' ed.-f *, Universal Law Publishing Pvt. Ltd., New Delhi, 2009.

10. Dr. Rao Joga S.V., 'Law of Cyber Crimes & Information Technology Law.' ed.-T', Wadhwa, Nagpur 2004.

11. Dr. Singh Y.K., 'Cyber Crime and Law.' Shree Publishers & Distributors, New Delhi.

12. Dr. Tewari R.K., Sastry P.K. & Ravikumar K.V., 'Computer Crime and Computer Forensics.' Jain Book Agency, Delhi, 2002.

13. Dudeja V.D., 'Cyber Crime and Law enforcement.' Commonwealth publishers. New Delhi 2003.

14. Fatima, Talat, 'Cyber Crimes' ed.-l^', Eastern Book Company, Lucknow, 2011.

15. Fumell, Steven, 'Hackers, viruses and malicious software: Handbook of Internet Crime.' ed.-l^', Willan Publishing, Cullompton, 2010.

16. Gaur K.D, 'A Textbook On The Indian Penal Code.' Universal Law Publishing Co. Pvt. Ltd., New Delhi, 1992.

17. Gupta Sandeep, 'Hacking in the Computer World.' Mittal Publications, New Delhi.

18. Jain, N.C., 'Cyber Crime.' ed.-T', Allahabad Law Agency, Faridabad, 2008.

19. Jain, N.C., 'Cyber Law.' ed.-T, Allahabad Law Agency, Faridabad, 2008.

20. Jain, N.C., 'The War Against Cyber Crime.' ed.-T', Allahabad Law Agency, Faridabad, 2008.

21. Dr. Farooq Ahmad ,Cyber law in India (law on internet) New Era law Publication, 4th edition: 2011.

NEWSPAPERS & MAGAZINES

Competition Wizard

Frontline

Hindustan Times

The Hindu

The Indian Express

The Nation

The Statesman