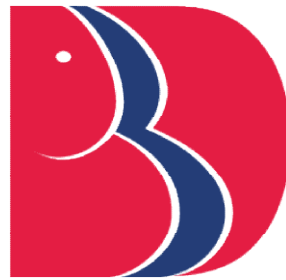


**“CHALLENGES IN CYBER TERRORISM
AND CYBER CRIME IN INDIA”**

DISSERTATION

**Submitted in the partial fulfillment for the
Degree of
Master of Law’s (LLM)
Session: 2019-2020**



BBD UNIVERSITY

Under Supervision of:

Ms.Sonal Yadav

Assistant Professor

Department of School Legal Study

Babu Banarsidas

University Lucknow

U.P. (India)

Submitted By:

Pooja Shrivastava

Roll No.1190997035

LLM (IVth)

Babu Banarsidas

University Lucknow

U.P. (India)

DECLARATION

Title of Project Report "**CHALLENGES IN CYBER TERRORISM AND CYBER CRIME IN INDIA**". I understand what plagiarism is and am aware of the University's policy in this regard **Pooja Shrivastava**. I declare that

- (a) The work submitted by me in partial fulfilment 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.

Date :

Pooja Shrivastava
Roll No.1190997035
LLM (IVth)

CERTIFICATE

This is to certify that dissertation entitled “**CHALLENGES IN CYBER TERRORISM AND CYBER CRIME IN INDIA**” which is being submitted by **Pooja Shrivastava** for the award of the degree of Master of Laws is an independent and original research work carried out by her. The dissertation is worthy of consideration for the award of LL.M. Degree of **Babu Banarsidas University Lucknow U.P. (India)** **Pooja Shrivastava** has worked under my guidance and supervision to fulfill all requirements for the submission of this dissertation.

The conduct of research scholar remained excellent during the period of research.

(Under Supervision of)

Ms.Sonal Yadav

Assistant Professor
Department of School
Legal Study
Babu Banarsidas
University Lucknow
U.P. (India)

Date -----

Place– Lucknow

Acknowledgement

I feel proud to acknowledge the able guidance of our esteemed (supervisor to be acknowledged)

I express my heartiest gratitude and deep sense of respect to my supervisor of **Ms.Sonal Yadav Assistant Professor** Department of School Legal Study **Babu Banarsidas University Lucknow U.P. (India)** for her valuable guidance, generous help and constant inspiration all through the work.

I acknowledge with pleasure unparalleled infrastructural support that I have received from **Babu Banarsidas University Lucknow U.P. (India)**

I find this opportunity to thank the library staff of the **Babu Banarsidas University Lucknow U.P. (India)**

This research work bears testimony to the active encouragement and guidance of a host of friends and well-wishers. In particular mention must be made of (optional)

It would never have been possible to complete this study without an untiring support from my family (optional)

I am greatly indebted to the various writers, jurists and all others from whose writings and work I have taken help to complete this dissertation.

Date.....

Place: Lucknow (U.P.)

Pooja Shrivastava

Roll No.1190997035

LLM (IVth)

ABBREVIATIONS AND ACRONYMS

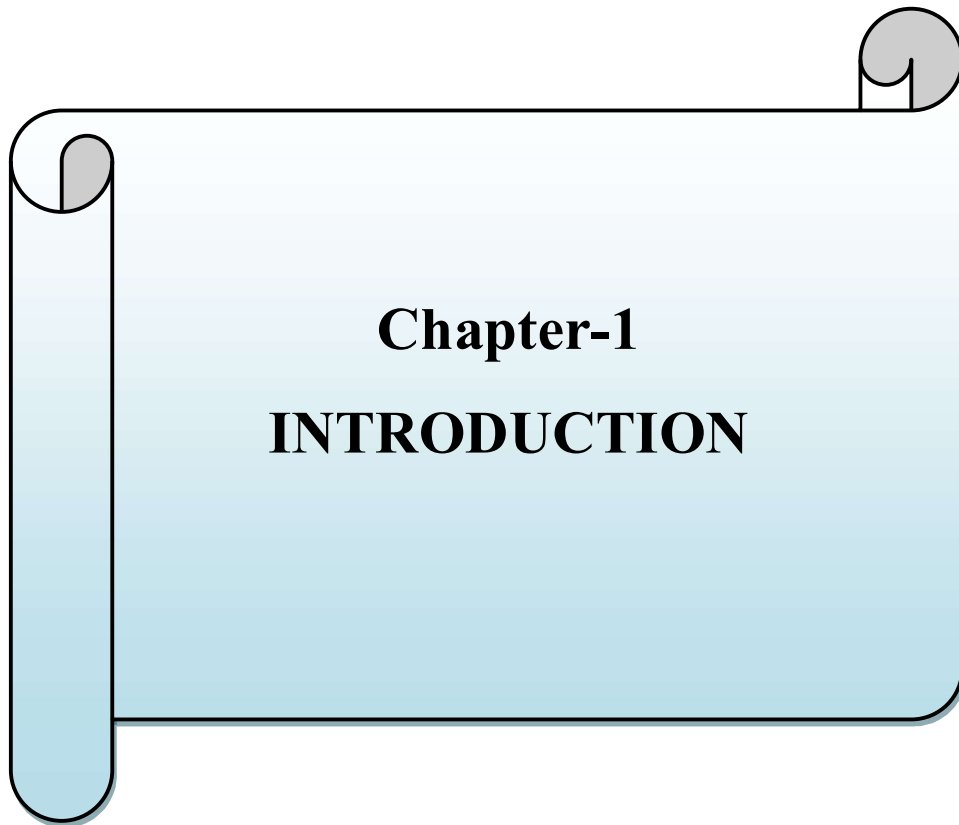
1	3GPP	3rd Generation Partnership Project
2	AIR	All India Reporter
3	ARPANET	Advanced Research Project Agency Network
4	ARPANET	Advanced Research Project Agency Network
5	AVI	Audio Video Interleave
6	BARC	Bhabha Atomic Research Centre
7	BBBO	Better Business Bureau Online
8	CD	Compact Disk
9	CDA	Communication Decency Act
10	CDA	Communication Decency Act
11	CEO	Chief Executive Officer
12	CERN	European Council for Nuclear Research
13	CERT-In	Computer Emergency Response Team- India
14	CII	Critical Information Infrastructure
15	CID	Crime Investigation Department
16	CIPA	Children Internet Protection Act
17	CIW	Cyber and Information War
18	CJI	Chief Justice of India
19	CMA	Communications Management Associations
20	Co.	Company
21	CODEXTER	Committee of Expert against Terrorism
22	COPA	Child Online Protection Act
23	Cr. PC	Code of Criminal Procedure
24	DoD	Department of Defence
25	DG	Director General
26	EDT	Electronic Disturbance Theatre
27	EMC	Electromagnetic Capacity
28	ERNET	Education and Research Network
29	ERRI	Emergency Response & Research Institute
30	FARC	Revolutionary Armed Forces of Columbia

31	FBI	Federal Bureau of Investigation
32	FLV	Flash Live Video
33	GGE	Group of Governmental Experts
34	GIF	Graphic Interchange Format
35	HC	High Court
36	ICANN	Internet Corporation for Assigned Names and Numbers
37	ICCIS	International Code of Conduct for Information Security
38	ICT	Information Communication Technology
39	IGC	Institute for Global Communications
40	IGNOU	Indra Gandhi National Open University
41	IP	Internet Protocol
42	IPC	Indian Panel Code
43	IRC	Internet Relay Chat
44	ISP	Internet Service Provider
45	IT	Information Technology
46	IV	Information Warfare
47	JANET	Joint Academic Network
48	JPEG	Joint Photographic Experts Group
49	LAN	Local Area Network
50	LOAC	Laws of Armed Conflict
51	LTTE	Liberation Tigers of Tamil Elam
52	MCOCA	Maharashtra Control of Organized Crime Act
53	MIT	Massachusetts Institute of Technology
54	MMS	Multimedia Messaging Services
55	MPS	MPEG Audio Layer 3
56	MPEG	Moving Picture Expert Groups
57	NASA	National Aeronautics and Space Administration
58	NASSCOM	National Association of Software and Service Companies
59	NATO	North Atlantic Treaty Organisation
60	NeGP	National e-Governance Program
61	NCRB	National Crime Records Beareu
62	NDMC	New Delhi Municipal Corporation

63	NFNC	National Federal Networking Council
64	NIB	National Information Board
65	NIC	National Informatics Centre
66	NSFNET	National Science Foundation Network
67	NW	Network
68	OAM&P	Operation, administration, maintenance, and provisioning
69	PCT	Patent Cooperation Treaty
70	PLC	Programmable Logic Control
71	PPP	Public Private Partnership
72	R&D	Research and Department
73	ROI	Return on Investment
74	SCADA	Supervisory Control and Data Acquisition
75	SC	Supreme Court
76	SEC	Supreme Court Cases Section
77	TCP	Transmission Control Protocol
78	TV	Television
79	UCS	Universal Communication System
80	UK	United Kingdom
81	UN	United Nation
82	UNCRC	United Nation Convention on Rights of Child
83	UNGA	United Nation General Assembly
84	US	United State
85	USA	United States of America
86	USA	United States of America
87	VCD	Video Cassette Disk
88	VCR	Video Cassette Recorder
89	VSAT	Very Small Aperture Terminal
90	WMV	Window Media Video
91	WPA	Western Provident Association
92	WTC	World Trade Centre
93	WTO	World Trade Organization
94	WWW	World Wide Web

TABLE OF CONTENTS

Chapter No.	Title	Page No.
Chapter - 1	Introduction 1.1 Research Problem 1.2 Research Objective 1.3 Hypothesis 1.4 Research Tools 1.5 Research Methodology 1.6 Literature Review	1-17
Chapter -2	Definition and scope of cyber terrorism & cyber crime in India	18-21
Chapter -3	History	22-25
Chapter -4	Cyber terrorism and Indian law	26-42
Chapter -5	Impact of cyber terrorism and crime	43-49
Chapter -6	Convictions	50-51
Chapter -7	Cyber protection and security system	52-59
Chapter -8	Motivation for cyber attacks	60-68
Chapter -9	Hacking wi-fi and various attack	69-72
Chapter-10	Computer related offence	73-77
Chapter-11	It act 2000 penalties offence with case studies	78-93
Chapter-12	Type Of Cyber Terrorism And cyber Crimes	94-106
Chapter- 13	Approaches and theories of cyber terrorism and crimes	107-112
Chapter -14	Conclusion and suggestion	113-115
	Bibliography	116-121



Chapter-1
INTRODUCTION

1. INTRODUCTION

The founding fathers of Internet barely had any proclivity that Internet could transform itself into an all pervading revolution which could be tainted for criminal activities and which required law. These days, there are many troubling incidents in cyberspace. Due to the mysterious nature of the Internet, it is probable to engage into a variety of criminal activities with impunity and people with intelligence, have been hideously misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. The advancement in this field has been multiplying exponentially but cybercrimes are also thriving rapidly. Although generous progress in technology, uncertainty still prevails and the efforts to trace, identify and bring the criminal to books have not borne much fruit. If cybercrimes are not combated at the early stage, the posterity will suffer from the human values, which will have very damaging effects on the society at large and innocent individuals in particular. The very character of crime itself has undergone complete transformation. There is a conjectural shift in terms of the costs of criminal behaviour and the forms of criminality, which merits state attention.

Globalization and Trade As the global economy grows rapidly, criminal crime has given a new wave, whose current state of violent crime requires a greater focus on the traditional form of law enforcement assets, which handles the bulk. Territorial boundaries are further hampered, as they may appear in cyberspace, where the corporation, which serves computers and telecommunications networks, controls access. The efficiency of criminals has increased due to the advancement of computer and communication technologies to handle serious crime and the risk of danger is much lower. Advanced technology, telecommunications and cyberspace in the process of weak nations violated in order to appear are.

The idea of jurisdiction becomes meaningless when a person has only one address as a computer network. In this century, not only because more and more technological innovation, cyber crime, legal and law enforcement communities memorable for inequality remain, which is becoming uninterrupted. The criminals 'growing financial resources will provide them with an increasingly important player in the global financial market. With the advent of the Internet, cyber law has become an emerging field. Saibarala 's, including electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law and the right to privacy. There have been various computer and internet related offenses. In fact, the rise

of crime on the Internet is directly proportional to the growth of the Internet, and therefore crime or committed attempts.

The basic principle of crime

The core principles of crime are based on the rules of fairness, justice, and fair play, which provide guidance on formulating rational penalties as well as ensuring the settlement of justice for litigation. It is a simple principle of criminal law that no person can be convicted of a crime unless the state party is proven beyond a reasonable doubt:

- He has a specific event or task, which imposes the existence of a particular state for him, which criminal law prohibits ; And
- It was a defined state of mind regarding the state or cause of existence.

So, there is essentially a crime in two elements, namely, *Match Reese* and *Men*.

ACTUS REUS

The word actus means, a physical consequence of human consumption. The definition of the crime of Actus Reus includes all the material except the mental element of the accused. This is not just a law, but may be involved in events that do not involve this law. Actus Reese is defined as "the consequences of human behavior such as the law seeks to prevent."

Rees match is made generally, but not always, conduct, and that sometimes even result in the circumstances, or the formation of the state of affairs, so far as they are relevant. Sometimes a particular state of mind is required for the victim by defining the crime. If so, that state of mind is a part of Actus Reus.

Actus reus in internet crimes

Detecting the Internet of Crime is relatively easy in this component of Actus Reese, but it is very difficult to prove. The presence of this fact can be termed as a crime when a person says:

- Using computer functions ;
- Getting access to any data stored on a computer or a computer, outside access to the data is stored ;

- Gaining access to the Internet or working is trying to pass signals through different computers and computers, which is within the first person's computer. Such a function can be called an actus reus structure.
- The login attempt, though, is worth the effort. For example, an automated system allows hackers to try different passwords, from which practice can often be considered a function.

MENSREA

Mensrea another essential element, which is a crime known as "the structure of *guilty mind* " is called. This continued to change until modern criminal law always considered it necessary to have a guilty mind or some other mental element. Mens were bound to have many different mental attitudes, including motives, irresponsibility, and dishonesty. Deliberately refers to the state of mind of a person who not only expects, but also has potential consequences for his behavior. As long as there is a vision, for example, then there may be a purpose, because it is a person who intends a particular law, such that the consequence of a law should be a proper vision. Although the intention may exist without foresight, it is true that faith is not needed, that is, there can be no vision without intention. A person who does not want to create a detrimental outcome, can take undue risks. If one forgets potential or the potential consequences of their conduct, and yet, they also will, this behavior still is, so it raises the risk of deliberate bring undesirable consequences. Such national behavior can be defined as reckless.

Finally, a person can bring an event with no purpose or foresight. He never considered the possible consequences of his behavior, and the end result may be surprising to him. Under the general law, there is no criminal liability for any unknown or unintentional harm caused by the unexpected conduct.

Mensrea study in Internet crimes

The Internet crime M setting for a vital ingredient definitely, definitely the part of the offender must be aware of the time, which led to the execution of the computer to be protected. Hacker party 's, secure access is required for the purpose, although it is on a computer, and the computer does not indicate any particular purposes. So, HackneyRid doesn't know which computer he attacked. Accordingly, this intention of secure access

does not need to be directed to any specific or specific type of program or data. It is enough that the hacker wants to secure access to the program or data.

So, there are two important components for men studying for hackers or crackers who gain unauthorized access to the system:

- Must have unauthorized access to protect ;
- Hackers need to be time conscious, when they have secure access.

The second element is easy to prove that the alleged hacker is outside the person who has no right to be on the computer or access the data contained in the computer ; However, it is difficult to prove that it has limited capabilities in the case of hackers.

In-depth analysis shows that our old obsolete and primitive civil and criminal laws were somehow created to overcome the end of current Indian society through the innovation and ingenuity of justice. These national rules are in place for a thorough review and replacement. The nature of cyber crime and the capabilities associated with such existing structures cannot be controlled and controlled. In fact, Cyberspace technology, conventional, such as the legal concept of property as evidence, and the evidence of his influence, loco styandi and " Men's rim, the concept expanded as has been observed.

There has been controversy over whether cybercrime requires new laws to deal with them or whether the existing legal system is flexible enough to deal with this new type of crime effectively. Usually countries involved in combating cybercrime, adopted two strategies, namely, dealing with crime as a traditional technology / hi-tech computer and the nature of a new legal framework for crime.

CYBER CRIME: INTRODUCTION

There are many benefits to some new types of technology that have been invented or invented. Likewise, there are some advantages and disadvantages to using the new and intensive technology i.e. Internet services. This violation is known as cybercrime, major harm, illegal activity on the Internet by some individuals due to some loop-holes. Internet, the facilities, the security risks associated with being connected to a large network aware makes. Today's e-mail is a computer misused for illegal activity such

as espionage, credit card fraud, spam, software piracy, which tends to invade our privacy and play our unconscious. Crime activity is on the rise in cyberspace.

Computer crimes are not criminal activities, including the loss of computer information, the deletion or alteration of unauthorized or unauthorized access to a computer system using information technology. Computer crimes include activities such as electronic fraud, device abuse, identity theft and data as well as system interference. Computer crime due to the necessarily physical property damage is not. These include confidential information and a string of important information. Software crime-related activities include software theft, which prevents user privacy. These criminal activities are in violation of human and data privacy, as well as important information theft and unauthorized changes include a variety of computer crime and the use of new and more effective security measures are required.

In recent years, the development and penetration of the Internet in Asia Pacific has been unprecedented. Currently, Internet penetration is increasing in rural areas especially in India and some other countries in the region. The challenges of data protection have also increased manifold. This widespread nature of cyber crime has started to have a negative impact on economic development opportunities in every country.

Companies need to take both preventive and corrective measures if they are protected from any kind of compromise by external contaminants. According to the latest statistics, Asia Pacific produces more than a fifth of malicious activity in the world. Malicious attacks include denial of service, spam and phishing and bot attacks. Overall, spam made in the Asia Pacific region, e-mail can monitor traffic 69% built. According to the National Crime Records Bureau statistics, cybercrime increased by 255% in India alone. And remember, these are just reported cases.

Computer crime is an information technology infrastructure involved in criminal activities, as may be defined, illegal access (unauthorized access), illegal barrier (data from the computer's non-public transmission of the technical means) or included in), data interference (unauthorized destruction, the destruction of data Computer, loss, loot, change or clamp) ; System interruptions (input, transmission,

damage, deletion, loss, alteration or alteration of computer data), abuse of devices, fraud (interference) ID theft, and electronic fraud (Taylor, 1999)

Cyber Terrorism : Introduction

The world is a big place, but it's getting smaller for the advent of computers and information technology. However, as we have made progress in this area, it has a dark side, a new terrorist tactic, commonly referred to as cyber terrorism, has been developed. The killings and the old hostages, the traditional methods, gradually disappear, as the terrorists on the Internet have to pull off their physical exercises. The reason for such an infection stems from the fact that the terrorist has long felt that simply removing another officer should replace another officer ; This is not what the terrorist wants to achieve. Carrying out terrorist networks can be targeted for these reasons, thus affecting a wider class. Disable a closed economy, large Z in the power off, turning on, it's all possible, terrorists with the least risk.

Cyber terrorism is definitely, definitely no such activities, terrorism, information systems or digital (computer or computer network) is used as an instrument or a goal. According to the nature of cyber-normality law, " international", " home-to-home" or "political", but it is always a terrorist and a law involving the computer.

Why is IT so attractive to terrorists ?

Terrorist groups are using computer technology to protect many of their targets. They are exploiting existing technology, to meet this goal, he has worked in the past. However, the main difference between their old tactics and their new methods is that they can easily perform their operations, as well as increasing ignorance অত্ৰন্ত It is extremely difficult to detect such covert operations, and to say that such acts are even more difficult to resist. Terrorist groups use computer technology to create support that strengthens their strategic and strategic plans and goals. These are definitely ' Law:

- Political propaganda
- Recruitment
- Financing
- Inside and inter group communication and coordination

- Collection of information and intelligence
- Used in operations operations, terms of used resources, and has the ability to strike across both worlds.

Common examples for the benefit of terrorism through the use of computer technology illustrate the application of this technology to terrorist groups interested in pursuing their specific agenda. The use of the Internet for propaganda and chaos is particularly popular. Several political opposition groups, such as Iran, Iraq, Mexico, Northern Ireland, and Saudi Arabia, have used the World Wide Web for the purpose.

However, one of the most protesting examples, Lima, captured the 1996 cover by the Peruvian Japanese Ambassador Tupak Amaru housing the revolutionary movement in December. The terrorist group not only used the Internet to spread its revolutionary message to the world through European websites, but also gave their members a video clip of them preparing for their mission.

An additional attraction to terrorists on the Internet is definitely, definitely the key factors in the promotion of the use of violence for a wider audience, not only to remind them, it reminds the audience of the future potential for violence reinforces fears. In addition to supporting terrorist propaganda, computer networks also increase terrorist recruitment and financing. Various US domination groups have used the Internet for financial gain.

The nature of modern computer technology is such that it detests itself in the communications and intelligence activities of terrorist groups. The attractiveness of this facility for expanding group activities can be summed up as follows:

Information technology, which gives individuals and groups on the impact of such a campaign, and organized well arrange and integrated, state-of-funds reserved for the terrorist organization was. Physical distance and national boundaries that once his co-conspirators, their audience and their terrorist goals isolates the, modern telecommunications and the Internet does not exist in the world.

Organizations like the Islamic fundamentalist groups that follow Osama bin Laden rely on computers to coordinate their activities. For example, the Colombian Revolutionary Armed Forces responded to the inquiry via email. Terrorist intelligence

gathering in the computer networks and the World Wide Web to access the equally important equally

Not only has modern computer technology been widely exposed to the above activity, but it is a fashion that terrorist groups use to do so, they can now handle traditional border terrorism beyond the point of view. Terrorist capacities "structured activity" such as recruiting people, communicating and, in particular, being fundamentally powerful and therefore financing the knowledge of state authorities, may be a more lively terrorist group. As a result, the ability of terrorist groups to engage in activities that focus less on threats and more on activities that can be seen and felt. Modern terrorist groups are able to evolve indefinitely, they are stronger than their previous appearance, can be incomplete and deadly.

Moreover, and perhaps more importantly, the advent of computer networks has created a new direction in the terrorist organization. Terrorist groups that use computers to communicate can outperform hierarchical organizational structures and employers.

1.1 RESEARCH PROBLEM

A research problem is a statement about an area of concern, a condition to be improved, a difficulty to be eliminated, or a troubling question that exists in scholarly literature, in theory, or in practice that points to the need for meaningful understanding and deliberate investigation.

Internet and Computer crimes will always involve some type of computer security breach. “computer-security breach” and “computer crime” are not synonymous. They are related concepts, but not identical ones. When computer professionals begin working with computer crime and forensics, they often make the mistake of assuming the two terms mean the same thing.

Of late, cyber space became the major domain of warfare after land, sea, air and space. The younger generations spend more than 80 percent of their time in computers and internet, particularly in Tamil Nadu giving more way for criminal occurrences either unknowingly or knowingly. Cyber crimes not only affect the adult population but also the children, the pornography and the ways in which pedophiles try to lure children on the Internet. This research agenda has a little scope to Review the literature on cyber crimes. The literature indicates that there are many factors to consider cyber crimes. It’s one of the major social problem confronting the society and its impact has significant effect on the socio-cultural and economic development of the country.

1.2 RESEARCH OBJECTIVE

The objectives of the present study are as follows:-

i) 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 operand 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.

ii) 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.

iii) 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 in prosecution and trials.

iv) 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. In view of the above descriptive realities there is a need for having a serious study of the whole scenario to identify the main issues and find out solutions of the problems. There are various laws in Indian scenario keeping in mind the position of cyber crime in India. We can be benefited by looking at American and European experiences that have been battling for the right position till date.

1.3 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 unaffected by it as individuals, business organizations, governments & states all are in the net.

The judicial system in our country is not conducive to effective 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 changed the lives of the people. There is no sphere of human endeavour, 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.

1.4 RESEARCH TOOLS

The research completed for this dissertation was a secondary research data. Secondary research data consisted of research through journals, websites books etc. The findings of secondary research were analysed and combined in order to determine the findings.

The present research work is based on the Doctrinal or Non-empirical research methodology which is concerned with doctrines, legal propositions or propositions by way of analysing the existing statutory provisions and case laws by applying the reasoning power. An attempt has been made to verify the hypothesis through legal reasoning or rational deduction by analysing the primary and secondary sources of law including legislations, case laws, text books on law, commentaries and official websites etc. The present research work also factually relies on academic writings and newspaper reports to access the impact of cyber crimes. The purpose of using this methodology is to ascertain a legal rule for solving the problem of cyber crimes at national and international level and to arrive at certain conclusion and to give suggestions.

1.5 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 deduction.

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.

1.6 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) 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 pennission, alters, damage, deletes and destroys the database available on the computer or network. It also includes the access without pennission to the database or programme 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) 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 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 cyber-crimes, teachers, students, lawyers and judges.

Vakul Sharma (2004) 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

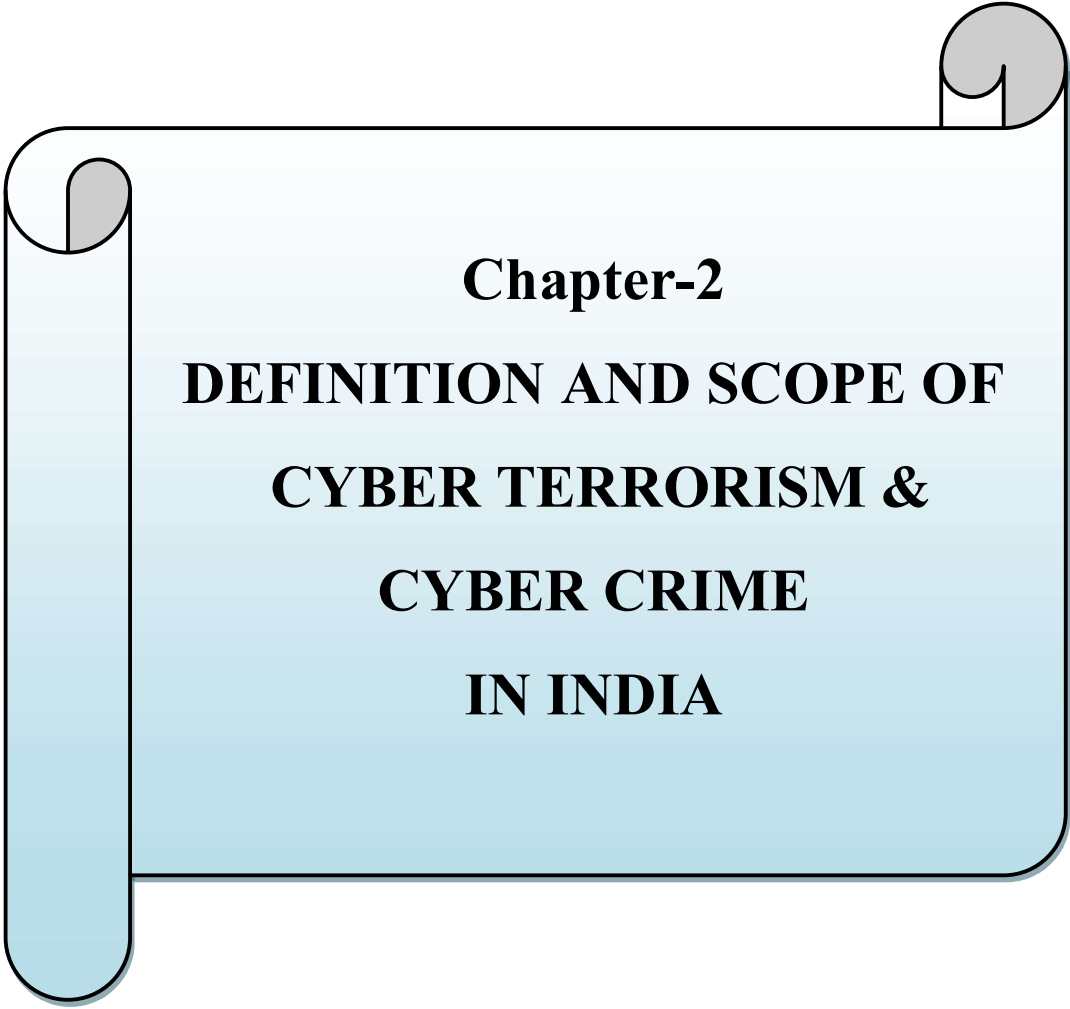
Supreme Court judgments for better assimilation and understanding of its various provisions relating to cyber crime. The author has tried to assimilate the thoughts of Judges, Lawyers, Civil Servants, Police Officers, Technocrats and Students whom he met during his public lectures, discussions, workshops, 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 Infomiation Technology Act has been attempted.

Chris Reed (2000) 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) The 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 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 pom to the regulation of free speech on the Net and the right to privacy.

A new chapter on Cases on Computers, Internet, e-mail etc. have 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. Cyberlaw 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-2
DEFINITION AND SCOPE OF
CYBER TERRORISM &
CYBER CRIME
IN INDIA

2. DEFINITION AND SCOPE OF CYBER TERRORISM & CYBER CRIME IN INDIA

Cybercrime is also called computer crime, used as computer on the edge of illegal up, fraud, child pornography and intellectual property trafficking, identity theft, privacy violation. Cyber crime, especially the Internet through, computer-commerce, such as, entertainment, and has become the central government, the growing importance there.

United States of computers and the Internet as quickly and widely accepted reason, the primary victims of cybercrime and the American villain. The 21st century, however, is rarely Hamlet anywhere in the world who has not been touched by cybercrime or any other kind.

DEFINING CYBERCRIME

New technology creates new criminal opportunities but also creates some new types of crime. What makes cybercrime different from traditional criminal activity? Clearly, a difference definitely, definitely digital computer use, however, any differences that exist between the various criminal activities simply insufficient technology. Criminals fraud in order, child pornography and intellectual property of traffic, a violation of privacy, identity theft, or to the computer is not required. All of these activities existed before the "cyber" symptom became ubiquitous. Cybercrime, especially involving the Internet, represents the prevalence of existing criminal behavior with some fancy illicit activities.

Most definitely Cybercrime ' Law individuals, corporations or government related to attacks on information. Although not a physical body of attack, they have or have a personal corporate virtual body, the group informative feature defines people and organizations on the Internet. In other words, our virtual digital age is an essential element of everyday life to recognize: We are a bundle of numbers and common identities owned by various computer databases owned by government and

corporations. Cyber crime is the centrality of computer networks in our lives, as well as the vulnerability of concrete causes such as personal identification.

DEFINITION OF CYBER CRIMES

Cybercrime has recently become an attractive term for a set of security issues in cyberspace. However, in spite of frequent use, usually there is no acceptable definition. Of course, cybercrime is related to the realm of computers, however, there is no consensus on whether they are connected to the computer itself or not. Some definitions explicitly include computer-related crimes that are not done online, because they view cyber crime in the narrow sense, while others prefer broad definitions, including all computer-related crimes. However, it is clear that most computer crimes are online. Computer prevention and control of various United Nations Manual of crime, cyber crime following provides definitions : computer traditional in nature, which could be involved in such activities is a crime, such as theft, fraud, fraud and mischief, all but everywhere in general, are subject to criminal. Under the ban. Computers have created a host of potential new abuses or abuses, or it should be criminalized (UN 1994, 22).

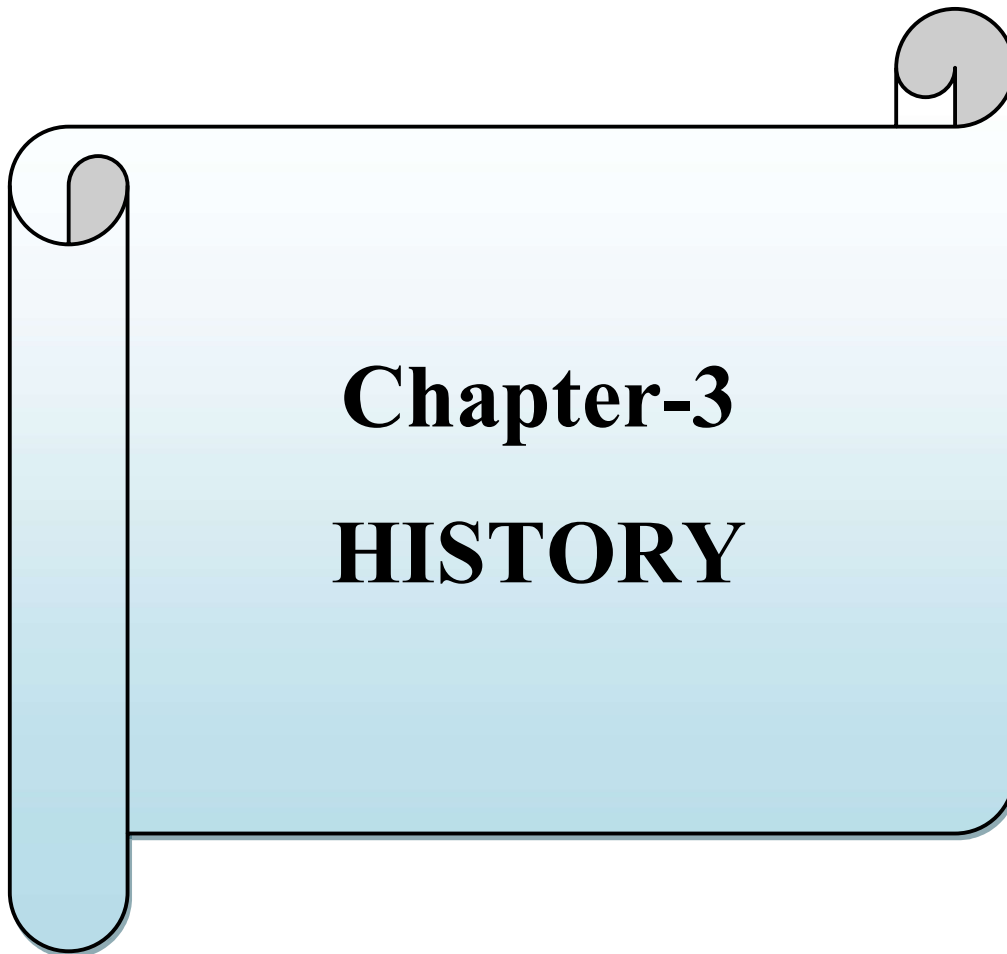
July 1996 in, the UK's National Criminal Intelligence Service began studying a computer crime program called trawlers. Computer crime studies, information technology crime and cyber crime are interchangeable. The Project Trawler defines computer crime as follows: A crime in which a computer network plays a direct and important role in a crime commission Computer interconnection is an essential feature (UNNCIS).

According to UNO experts, the term "cybercrime" is against the use of a computer system or network, in their structures or against covering up any crime. Theoretically, it's a crime that takes place in an electronic environment accept In other words, e-processed data to computers and the Internet can be used in the offenses referred to as cyber crime.

Cyber or computer crimes, definitely, " Law and White Collar Crime and students, non-professional computer programmer, business rivals, engaged the interest of the perpetrators committed by that. These definitions, such as crime, should address these three points:

- When the computer is used to commit this national crime.

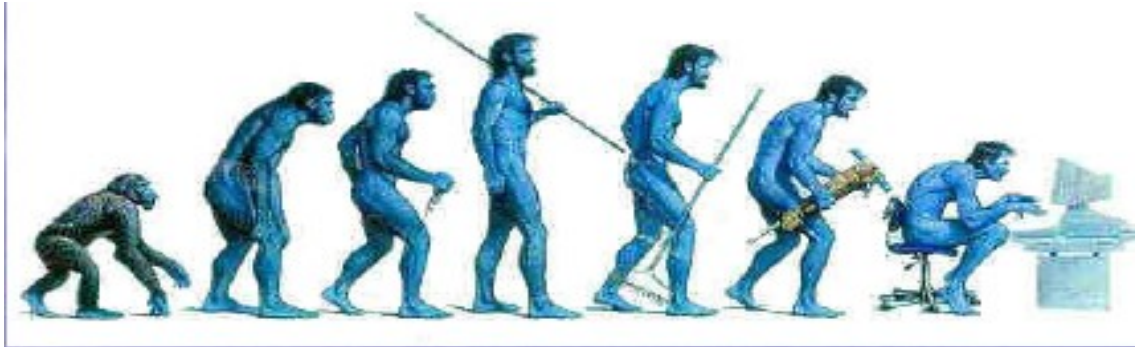
- Computer technology, a single transaction when two " persons of mistakes and errors are responsible for profit.
- When someone does one of the following, he or she is convicted of a computer crime:
 - Can access, damage, destroy, destroy, or transmit any other data, computer database, computer, computer system, knowingly or intentionally without the use of warning or computer network
 - to close or enforce any unlawful scheme
 - cheat, deceive or remove, or do
 - incorrectly controlling or obtaining money, property or data.
 - knowingly or willfully any computer, computer system, data or computer database, computer network, or any work, permission, or copy, or copies, or no supporting documentation, it is internal or external to the computer., Computer systems, or computer networks.
 - intentionally or not intentionally, and access to, data, computer software, can destroy computer programs or computer data, computer, computer system, the existence or ceases to exist internally or externally, or computer network, destroys.
 - intentionally or knowingly causes disruption of service access and computer without permission or a computer, computer system, or cause denial of service or computer networks are an authorized user of the computer.
 - Knowingly or intentionally offer any support to any computer, computer system, offer or support or access through computer network.
 - Knowingly or intentionally attempting to install or compromise any other professional computer services, false representations, false statements, any other unauthorized transactions, any other incoming or receiving AIDS or ABC. Any facilities or equipment or any other means.
 - Knowingly or intentionally causes a computer, computer system, access or computer network.
 - Malicious or computer viruses that knowingly or intentionally launch any computer, computer system, or any other computer into a computer network.



Chapter-3
HISTORY

3. HISTORY

Cyber crime



The Internet is growing very fast in India. It offers new opportunities to grow in every field, entertainment - which we can think of, business, sport or education.

There are two sides to a coin. There are also disadvantages of the Internet. One of the main difficulties is definitely ' Law Cyber crime - illegal activity on the Internet.

Internet, the facilities, the security risks associated with being connected to a large network aware makes.

Today computers are being abused for e-mail spying, credit card fraud, spam, software piracy and these national illegal activities, which invade our privacy and hurt our senses.

Crime activity is on the rise in cyberspace. For the benefit of our netizens, we publish an article in the series Nandini Ramprasad here. Ed.

" The modern thief can steal more with a computer than a gun T tomorrow with the terrorist bomb might be able to do more damage with the help of the keyboard."

- National Research Council, " Risk Computer", 1991

What is this cyber crime ? We read a lot about it in the newspaper. Look up the dictionary definition of cybercrime:

" This is a criminal activity that takes place on the Internet. It is a widespread term that refers to everything from electronic cracking to the denial of a lost service attack to an electronic commerce site."

History

The first recorded cyber crime took place in 1820 ! This fact is not surprising considering the pillars, which are considered to be the closest form of computer, have been around 3,500 BC. In India, Japan and China. The modern computer age, however, began with the analysis of the Charles Babbage engine. The first spam email came in 1978 after being transmitted to ARPNET (Advanced Research Projects Agency Network). The virus 1982 in Apple installed on the computer was the development of a high school student, Rich Skrenta, developed the Elk cloner.

Cybercrime was started by disgruntled employees who physically damaged the computers they worked on to recover their superiors. Such as the ability to house the personal computer has become more accessible and popular, so cyber criminals have begun to focus their efforts on home users. The most common cyber crimes during this period were *phishing scams, cyber-stacking, computer viruses and identity theft*.

As the years passed, more and more households bought home computers with Internet access, cybercrime became bigger and harder to control. *Cyber-bullying and harassment* have become more popular.

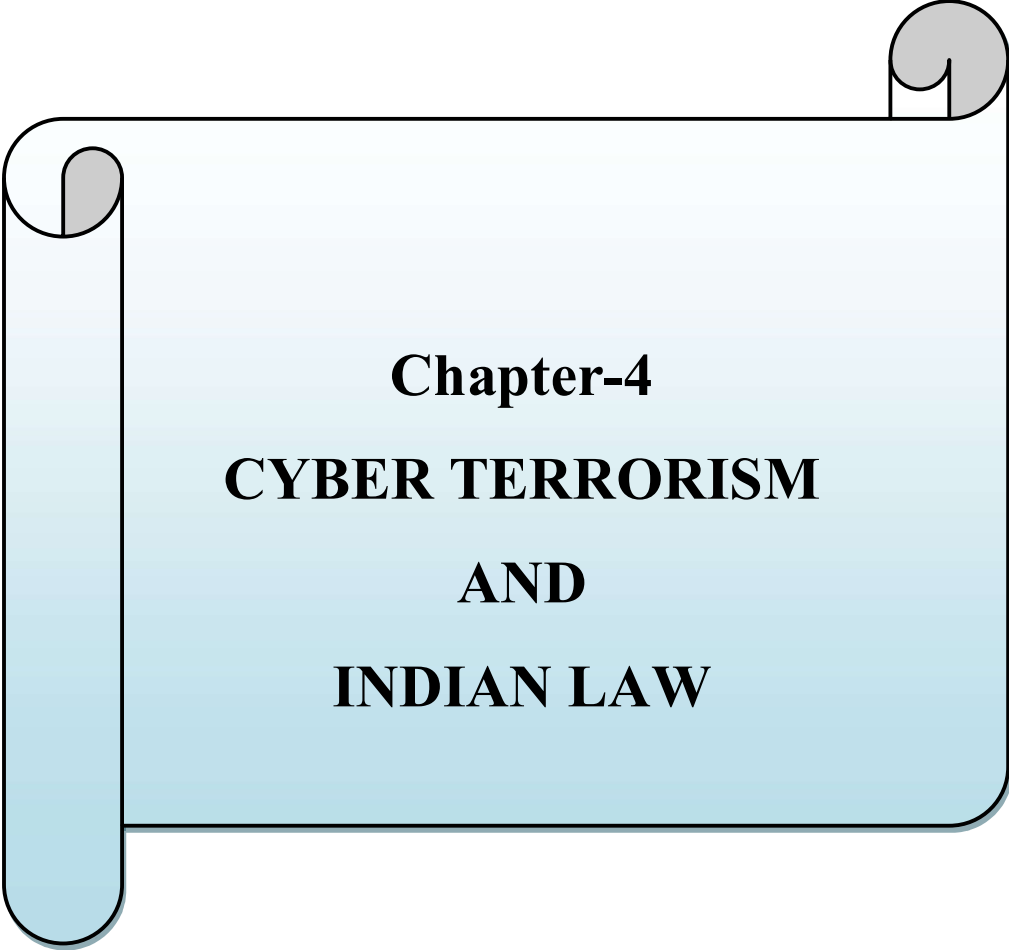
Middle school and high school kids start taking advantage of the Internet to scare their classmates and adults into the real life of employers by intimidating and manipulating them.

Police departments and federal law enforcement have created specialized departments for cyber crime prevention. However, given the history of cyber crime, it is clear that it will be shutting down soon, and it seems that growth will continue until it finds new ways to fight it.

When we are talking about a topic as a case study on cyber crime, it is helpful to have a clear essay. Since this document in the southern regional workshop on cyber law be presented to the representatives of the "Issues and Challenges in Enforcement". insisted. I am more focused on this issue than at the national level, though the topic is observed and considered relevant. I find this topic to be neutral and classified, in good

words, as paper (Class 1) crime, tend to focus on physical networks and hardware (2), fraud and fraud and (3) online crime.

Now I will give you an overview of a few words that are often used in the cyber crime world before starting talking to examples. I am sure many of you will know this and many new conditions are being introduced every day, I am sure this can be a starting point.



Chapter-4
CYBER TERRORISM
AND
INDIAN LAW

4. CYBER TERRORISM AND INDIAN LAW

Although the language, religion, culture and geographical regions are different, the process of birth is the same. No man sees the light of the sun all over the world, regardless of color and color. The birth and death of any human being are controlled by evolutionary processes. Politics, culture, language, religion and geographical regions S. 3 of the item, no changes can bring. The right to life, liberty, freedom of expression, pollution-free air and water, a small shelter over his head, to protect the life of every human being distributed clothes and food minimum. Wherever he speaks or wherever justified, the right to the basic rights of a decent human being, which is a decent life, may be due to the differences in building up the system itself in public but division and rights. Nowadays it is repeatedly affected. The poor people are not getting their share due to being part of it, and this is why some people are angry at the system and resort to violence in their hands to achieve their goals, which is an expression of it. Anger or resentment, and those who are not branded as terrorizing this event.

Terrorism can be defined as a system of conflict - killing, abduction, bombing, air raids and air hostages for the purpose of attaining a specific purpose or desired purpose.

Terrorism as defined by the Federal Bureau of Investigation

"The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political and social objectives".

U s e Title 22, Ch, 38, Sec. 2656 (f) d

Terrorism is defined as predetermined, political motivated violence, also by sub-parties or disguised agents against non-related targets, usually for the purpose of influencing an audience. The United States has applied this definition of terrorism since 1983 for statistical and analytical purposes. US Department of State, 202, Pattern of Global Terrorism, 23.

The various forms of terrorism are as follows ; Individual terrorism, group terrorism, state terrorism, revolutionary terrorism, international terrorism and the last one that has been established by technological development, namely cyber terrorism.

CONCEPTUAL FRAMEWORK

Traditional ideas and methods of terrorism have taken new levels, which are destructive and deadly in nature. In the age of technology weapons and technology expertise, information is acquired to produce lethal combinations of terrorists, safe, if not timely, it must take its own toll. From this the erosion will be almost irreversible and most destructive in nature. In short, we terrorism of the worst forms of face, "cyber terrorism" is known.

Cyber-terrorism differs from ordinary Internet crimes such as identity theft and money fraud, which involves the use of technology to remove or destroy systems and infrastructure, which can lead to injury or death, and may weaken the economy and institutions. To achieve their goals, cyber terrorists target computer systems that control air traffic, electric power

Grid, telecommunication networks, military command systems and financial transactions.

001 On 11 September a suicide mission 19 aircraft run by muggers harmless and innocent loss of lives in the attack had shocked the world. However, it is unfortunate, terrible as it was, only one or two ' persons skilled Internet users who had not entered into the land of their targets, they should be by the dwarf. If the computer system is too shocking to imagine human and economic losses

Given that air traffic, nuclear power plants or major dams have been dropped or misled by cyber terrorists.

In 1997 Barry Colin Cyber terrorism is the term "digital information system, network, such as deliberately abusing or endorsing material terrorist compilation or working feature".

And **the FBI defines cyber terrorism**, "premeditated, attack politically motivated against information, computer Red Hat, sub-national group of computer programs and data d'Or by secret agents of violence against non-combatant targets results." " Security

expert Dorothy Denning defines cyber-terrorism "... as the target of politically motivated hacking operations, causing serious harm and illegal attacks such as attacks against computers, networks, and intimidating the government. Or submit to Or or its people pursuing political or social purposes.

Forms of Cyber Terrorism

Cyber-terrorism is identified as a very serious problem and a wide range of attacks is covered. Here, one is asked about the definition of cyber crime. " Cyber crime", which is a crime targeting computers or enable cyber crime theft of intellectual property, patent infringement, trade secret or copyright laws may include. However, cybercrime involves attacks against computers, which involve intentional processing interruptions, espionage, or unauthorized copying of classified data. " Cyber crime is the key equipment botnet to be, Estonia, in 2007, Malta codes website hosted., Cyber spying on and so on. Here, covered a cyber crime such as the one above this reasonable., As well as for terrorist activities is an important tool in the criminal To discuss activities one by one:

ATTACK VIA THE INTERNET

(i) Unauthorized access and hacking:

This means that access to the computer, computer system or computer network, the logical, arithmetical or memory function resources to be accessed, instruct or make contact. Unauthorized access to the means of a computer, computer system or computer network to the owner or person in charge of a right to access the money will not be.

Hacking every job committed to split into computers and / or networks. Hackers write or use readymade computer programs to attack created computers. They want destruction and they come out of this national destruction. Some hackers hack for personal financial gain, such as stolen credit card details, withdrawal of money after the bank accounts Transfer funds from their account. Controlling another person's website by hacking a web server known as web hijacking.

(ii) Trojan attack:

The program serves as something useful, but does the cool moist things. This national program is called the Trojan. The name Trojan Horse is popular. The Trojan comes in two parts, a client pile and a server part. When the victim (unknowingly) runs the server on their machine, the attacking client will connect to the server and start using Trojan. TCP / IP " " is the most commonly used protocol type for protocol communication, but some functions of Trojan also use the UDP protocol.

(iii) Virus and worm attacks:

A program that has the ability to infect other programs and copy itself and spread it to other programs known as viruses. Programs that are multiplied by viruses but spread from computer to computer are called worms. This attack is definitely the latest " Law" E-Mai virus-rimaindim Michael Jackson Michael Jackson. " When it gets infected on the computer, the worm spreads to other Internet users.

Email and IRC related offenses

(i) Email spoofing:

Email spoofing, which means that other sources of email that was sent from the fact that it was derived from a source appears

(ii) Email Spamming:

Email "spamming" refers to sending emails to thousands and thousands of users - similar to a chain letter.

(iii) Sending malicious code via email ;

Emails are used to transmit viruses, trojans, etc. via attachment emails or to send links to a website on which malicious code is downloaded.

(iv) Email Bombing:

Email definitely, definitely "bombed" feature that sends email messages similar to the specified address repeated misusers. These include:

(v) Sending threatening emails

(vi) Defamatory emails

(vii) Email fraud

(viii) Regarding IRC (Internet Relay Chat)

Demolition of e-governance base

The purpose of e-governance is definitely 'the Law Department official conversations with the citizens of the free and fair and transparent way of sharing information. This information right more meaningful it makes. In *P, UCL. V Uoai* refers to those bases of the Supreme Court, the government that such trade secret can withhold information on various issues. The Supreme Court said: "Every right - legal or moral - has equal objections. It has been subject to many exemptions / exceptions, as it is widely pointed out."

In short, cybercriminals use various tools and methods to counter their terrorism. Some of the main tools is definitely ' Law:

1. Hacking
2. Cryptography
3. Attack the Trojans
4. Computer bugs
5. Computer virus
6. Denial of service to attack
7. E-mail Crime related to E-mail

Motives behind any Attacks are:

1. Intimidate the public or any part of the public; or
2. Adversely affect communal harmony between different religious, caste, language or regional groups or castes or communities; or
3. Oblige or disobey a government established by law; or
4. Endangering the sovereignty and integrity of the nation.

International Effort in Combating Cyber Terrorism

International cooperation in combating cyber terrorism is a different form of relationship between government and law enforcement agencies. Cooperative efforts are divided into three types: international and global efforts, multilateral and multinational efforts, and regional efforts.

A. Efforts from International and Global Organization:

(i) United Nation

The United Nations is a major body that includes coordination and cooperation on the issue of international terrorism. In its proposal, they need to be current and the potential threat to the security of member information is propagated in a multi-dimensional scenario, while good security limits the potential danger. The purpose of these proposals is to improve cybersecurity awareness at both the international and national levels. However, following the September 9 tragedy, the Security Council Resolution 1373 moved forward in the fight against terrorism. The purpose of this resolution is to counter anti-terrorism efforts. This proposal provides a definition of the panic is an internationally recognized, which is an inclusive ban on all forms of violence should be provided, at the international level, targeting civilians, because, as well as countries call for terrorism to sue.

(ii) Interpol

Interpol basement definitely, definitely prevent and to combat international crime, where the countries do not have diplomatic relations, and the legal framework and criminal cases between the working space. In September 2002, Interpol created an anti-terror division in the wake of a dangerous international terrorist attack called the Fusion Task Force.

(FTP) of the main objectives is definitely ' Law: active terrorist groups and subscribe identification, information gathering and sharing intelligence, analytical support provided, terrorism and organized crime humakisamuha to increase the capacity of member states to tackle. Interpol's popularity and priorities do not recognize terrorism as a crime area, and could benefit the country

Interpol's unique position in the international law enforcement community, definitely, definitely make the fight against terrorism,

B. Efforts from Multilateral and Multinational Organization:

(i) The Commonwealth Nations

The main work of the Commonwealth nations, definitely, definitely, including their member countries to adjust their laws. It enforces model law on computers and computer-related offenses and has a great impact on domestic law. It makes extending criminal liability, including any data interference, negligent liability intervention for use of computer systems and illegal equipment. In addition, the double crime across the problem, which has condemned the law, which is the regional nationality of the accused in favor, if he has an offset under the law of the country, where the crime was. Another function of the Commonwealth is to consider legal mutual support between the Commonwealth Member and the Commonwealth Member and a Commonwealth Member. The Minister of Commonwealth Law proposes adopting the Member State on the basis of cyber crime for mutual legal assistance between the Commonwealth Member States and non-Commonwealth States.

(ii) the G- 8 's group

Group G- 8, an informal stage and therefore lacks the administrative structure than an international organization. Group G- 8, the six members of the I- 975 in which, and the G- 6, known as the. Canada joined in 1975 and Russia became a formal member in 1998. The United States, the United Kingdom, France, Germany, Japan, Canada, Italy and Russia, the leader of the 1975 in the annual meeting, a crime which is to discuss the importance of the issue. And terrorism, and information highways.

(iii) Organization for Economic Co-operation and Development (OECD)

The OECD is a unique platform where the 30 countries and the economic, social and environmental challenges of globalization by working together to deal with. The OECD has been working for many years on many ethical issues related to information society. These infrastructure and services, including a wide range of issues around consumer protection, privacy and security, ICT and economic development. " OECD 00 In July of information systems and networks for the protection of adopted guidelines, member governments called for the establishment of high priority. Promoting security culture among all participants for security planning and management and as a means of securing information systems and networks. Guide The goal of this guideline is to build a global culture of security by adopting policies and measures. Internal and external threats, such as cyber-terrorism, computer viruses or hacking, present important social values, such as privacy and personal liberty, in interconnected societies worldwide.

C, Efforts from Regional Organization:

(i) European Union

After the terrorist attacks in Madrid, the EU and member terrorism promise to do everything in all forms of combat power. Thus, the European Union's decision to declare the European Parliament on March 11 as "European Day" reminded one of the victims of terrorism. Disnbr Mar. 2004 on, the EU Member States, the Convention on mutual assistance in criminal matters urged upon approval. Its protocols and the three protocols of the Europol Convention, as well as other aspects of implementing their framework, such as traffic data by service providers, cross-border investigations, exchange of information for terrorist offenses, and the Council for Council control, have been implemented. From

Identify new and applicable functions (SIS) for Schengen Information System. " '

(ii) Council of Europe

In 1949 Since the main function of the Council of Europe, definitely, definitely human rights, the rule of law and pluralistic democracy and the fight against terrorism, which gives consent to these values. Unique terrorist attacks in the United States after 2001 in its efforts to reach out to more and more was. It makes the legal action against terrorism stronger, try to fight cyber-terrorism by addressing basic values security, the causes of terrorism.

The Council of Europe focuses its attention on cyber terrorism and the theme of CODEXTER (Terrorism Against Expert Committee) on cyber terrorism. It is surveying the situation of member states to assess whether existing international tools are sufficient to respond to cyber bullying. "The coder concludes that there are several uses associated with the use of the Internet for terrorist purposes:

- (i) over the Internet, electronic communications and IT infrastructure, not only in those attacks, human and other infrastructure, systems and legal interests of the damage.
- (2) the promotion of illegal material, including the threat of terrorist attacks ; Pride, advertising and glorification of terrorism ; To finance and finance terrorism ; Training in terrorism ; Recruitment for terrorism ; As well
- (3) other logical access to terrorists' IT systems, such as internal communications, information acquisition and target analysis.

(iii) Convention on Cybercrime

The Convention, effective July 2004, dealt with the first Internet or other information network and only international aid law violations. Not only does the Convention ratify all EU member states, but it also does not address cyber-terrorism. The Convention to countries, hacking, copyright infringement, computer access, fraud, child pornography and other illegal activities against cyber criminal laws to update and integrate them to be. " 2 to 6 of the articles of various kinds of crime refers, which do not allow cyber crime and cyber terrorism, the definition of the word Prohibited criminal activity may include cyber-terrorism activity.

(iv) Council of Europe: Convention on the Prevention of Terrorism

The Council of Europe adopted the Convention on Terrorism and increased the effectiveness of existing international texts in the fight against terrorism. Meeting terrorism to prevent member countries attempt to enforce, and the aim to achieve two ways to determine the aim of this conference is definitely " Law : First, a criminal offense been taken, and second, internally it established the (national prevention policies), both to prevent co-operation to strengthen.), And internationally (existing extradition and mutual aid arrangements and additional modifications). In other words, the Convention provides for the protection and compensation of victims of terrorism.

Laws in Various Countries on Cyber Terrorism

Singapore

Singapore's new law allows for the launch of a pre-emptive attack against computer hackers, fearing more tight control of the Internet and privacy compromises in the name of combating terrorism. The national parliament of the city-state should approve laws aimed at preventing computer crimes, including "cyber-terrorism," national security, foreign relations, banking and tough new government services. Security agencies can now patrol the Internet and ban the use of computer keyboards as weapons of mass destruction if hacking is a conspiracy. Violators of computer abuse laws, such as website hackers, can face up to three years in prison or a fine of S \$ 10,000 (\$ 5,800).

Malaysia

The report states that Malaysia is setting up an international hub of cyber terrorism, providing an urgent response to the high-leverage attack on the economy around the world and the business system. Prime Minister Abdullah Ahmad time to visit the United Kingdom Badawi in Kuala Lumpur Cyber Jaya's high-tech hub outside the comfortable seating, the government and funded and supported by the private sector. The New Straits Times says the center will be ready for disease control in Atlanta, which helps combat disease outbreaks around the world. Abdullah, who announced his initiative to bring the world closer Austin, Texas Congress on Information Technology said the government was too serious to reduce the threat of cyber terrorism.

Interpol, your 178 member countries, is doing a great job against cyber terrorism. They are assisting all member countries and training their staff. The European Convention on Cyber Crime, which is the first international treatment of the struggle against computer crime, results in 4 working years by 45 members and non-country experts, including Japan, the United States and Canada. This deal is already 21 And March ' in March 2004 in Lithuania by the authorization has been effective.

The Southeast Asia Nations Association (ASEAN) plans to share information on computer security.

The United Kingdom

UK's Terrorism Act 2000, passed, that the provisions of the definition of terrorism and cyber-terrorism.

Pakistan

According to the ordinance, those who commit the crime of cyber-terrorism and the death of a person, whether sentenced to death or life imprisonment, were released by state-run APP news agency. Which is detrimental to any offense for the use of national security

Computer or any other electronic device, the ordinance said in the ordinance. It defines various definitions of the "terrorist law", including theft or duplication, or theft or copying of classified information required to manufacture a chemical, biological or nuclear weapon of any kind.

India

Earlier, the term "cyber terrorism" was missing from the Dictionary of Indian Law. To oppose the use of encryption by terrorists for the Information Technology Act, Section 9 And the passage of a strong legal system. This section through the agency of any government agencies that any government agency transferred to any computer for any information which can help to direct the public authority (CCA) was approved. Mumbai 26/11 after the attack, the Indian government has taken steps to strengthen cyber security, which put a stop to terrorist activities through cyberspace, the existing Indian Information Technology Act, 2000, the amendments made by. This

provision was included. This purpose of this legislature was Section 7F which defines and Combined with cyber terrorism. Category F 66 in the mentioned,

(1) Whoever,-

(A) India's unity lot of work, integrity, security or interfere with the sovereignty of the people or a class of people in the terror threat to run -

(i) deny or cause access to any person authorized to access the computer resources ; Or

(ii) attempting to enter or access computer resources without authorization or authorized access ; Or

(iii) any computer contamination and such national conduct may be interrupted or cause death or injury or damage or loss of property or property of the person or it is likely to know or occur that it is likely to damage or disrupt the supply. For living or community services or section 70 of the information infrastructure adversely affects or

(B) intentionally or knowingly access or access, without an authorized or authorized access to more computer resources, and the operation is limited to such violations, state security or foreign relations, which have access to data or computer databases ; Or any limited information, data or computer database, as it is believed to be used with such data, data or computer database and integrity can be used to hurt the sovereignty, state or security of India. Friendly relations with foreign states, public order, decency or morality, or contempt of court, or with a host of crimes, or in a foreign country, group person or any other benefit is a crime of cyber terrorism. General chat lounge

(2) Anyone committing a cyber crime or conspiracy must be sentenced to life imprisonment. '

(A) Constitution of India

Anyone who fails to assist government agencies in order to decrypt the information requested went to one of the blocks, the 7-year-old could be awkward. Constitution of India, 300A Article has been stated that all persons of their property rights and enjoy the right to have. *In a specific case of Bhavnagar University. Politana Sugar Mills Ltd. " The Supreme Court has enforced this constitutional clause with the view that anyone can enjoy their property rights in any*

way. It also has the right to property stored on the computer or in any electronic format.

Articles 301 to 305 refer to the right to free trade. When a person gets into a business litigation law, there is no way it can be interrupted. Furthermore, free trade and no commercial activity can be imagined without technical rights, meaning no distortion.

They are illegal. These provisions have been effectively used to protect private property rights against cyber criminals in India.

(B) Penal Code

The Indian Penal Code also provides a great deal of protection. Section 22 defines this as "immovable property" involving all corporation property. This means that any kind of concession stored on any computer can easily be considered as immovable property because it can certainly be moved from one place to another and is not connected. Section 29A (1) (T) of Code 29 of the Technology Law of Information states that "electronic record means providing information, records, or data generated, images or words stored, received or transmitted electronically or Microfilm or computer generated micro fiche".

Cyber-terrorism and Human Rights

Its role in the Universal Declaration of Human Rights discusses "freedom from fear and freedom." Freedom from fear is a psychological nature, but it is used very widely these days, especially in the case of terrorism. Declaration 3 Article "individual rights" has been set. As we know, "person is an environment (S word)" is also included, apart from "personal" terms, except under the conditions under which a person is close to another, some abstract such concepts are imaginary. To say security will protect his (her) social, economic and other connections, "threads" with the environment. Unless modern reality is sometimes primarily based on technology, computers or the Internet, cyber-terrorism protection is also related to "security." Add 5 article here'll also protect individuals against "abusive treatment". Part of reducing personal harm and treating a person in the current manner is something that can be provided by cyber-criminal law. An

important provision that, I have to declare Article 12 of the pay particular attention to me, it says: "No one shall be subjected to arbitrary interference with his privacy, or against attack. N his honor or reputation ".

" A company or the quality or state is defined as, "In addition to monitoring a secret", independence, in combination with the definition of a high Z's unauthorized intrusion "to" have, which is stored computer data, and includes a right of privacy. The personal desire of the officer without interference is to enjoy his personal state. Article 17 the appropriate rights set and the property owner anyone to deprive "no thing or person ownership" is defined as, the two types include: "real property" and "personal property." Private property or "personality" These include "immovable property" which is not real property, money or investment. However, Article 19 plays a different role in the topic and is currently commonly associated with the use of the Internet by terrorists.

Cyber terrorism and modern terrorists

Cyberterrorism modem is an attractive alternative to terrorists, who value its anonymity, greater vulnerability, psychological impact and its ability to influence media appeal. It is in their own tents, caves, bunkers, or to acts of terrorism and from the palace. Among other considerations, definitely, definitely:

- (A) low prices,
- (B) Different types of targets.
- (C) low risk for terrorists.
- (D) Greater media coverage

Cyber terrorism is an attractive alternative to modem terrorists for various reasons.

First, it is cheaper than the conventional terrorist system. The terrorist needs a personal computer and an online connection. Terrorists are not required to buy weapons such as

guns and explosives ; Instead, they can create and distribute computer viruses through a telephone line, a cable or a wireless connection.

Second, cyber terrorism is more anonymous than the traditional terrorist system. Like many Internet surfers, using a terrorist online nickname - log on to a website as anonymous "guest users" - is a "screen name", so making sure the terrorists' real identity is very difficult to track with security agencies and police forces. And no substance is exposed to cross checkpoints in cyberspace, there is no limit to the cross, or any customs agent to Autmart.

Third, the diversity of goals and numbers is encouraging. Cyber-terrorists can target governments, individuals, public utilities, private computers and computer networks

Airlines, and more. The sheer number and complexity of the potential targets guarantees that terrorists can exploit FMD vulnerabilities and weaknesses. Many studies have shown that

Infrastructure and computer systems, which make them extremely complex, make them effectively impossible to overcome all vulnerabilities, because critical Infistrcer, such as electric power grids and emergency services, are prone to cyber-attacks.

Fourthly, cyber terrorism can be managed remotely, such a feature is particularly attractive to terrorists. Cyber-terrorism requires physical training, emotional investment, death risk and travel, rather than the usual forms of terrorism, making it easier to recruit and retain followers of terrorist organizations.

Fifth, as I have loved you, the ability to influence the masses, rather than directly to the cyber-terrorism traditional terrorist methods, maximum media coverage, Wu Z produced is, in the end, the terrorists would the. Over time, hack into the total sophistication level system will be reduced. At the same time, the quality, quantity and availability of hacking tools have increased. Cyber warrior devices are often easily available for Dove / Knowledge from the Internet. With minimal funding, training, weighing and defense

infrastructure, relatively few tech consultants can take cyber bias with less information from anywhere in the world. This is an extremely dangerous target, making rich and low-risk combination.

Some incidents of cyber terrorism:

Following are the significant incidents of cyber terrorism:

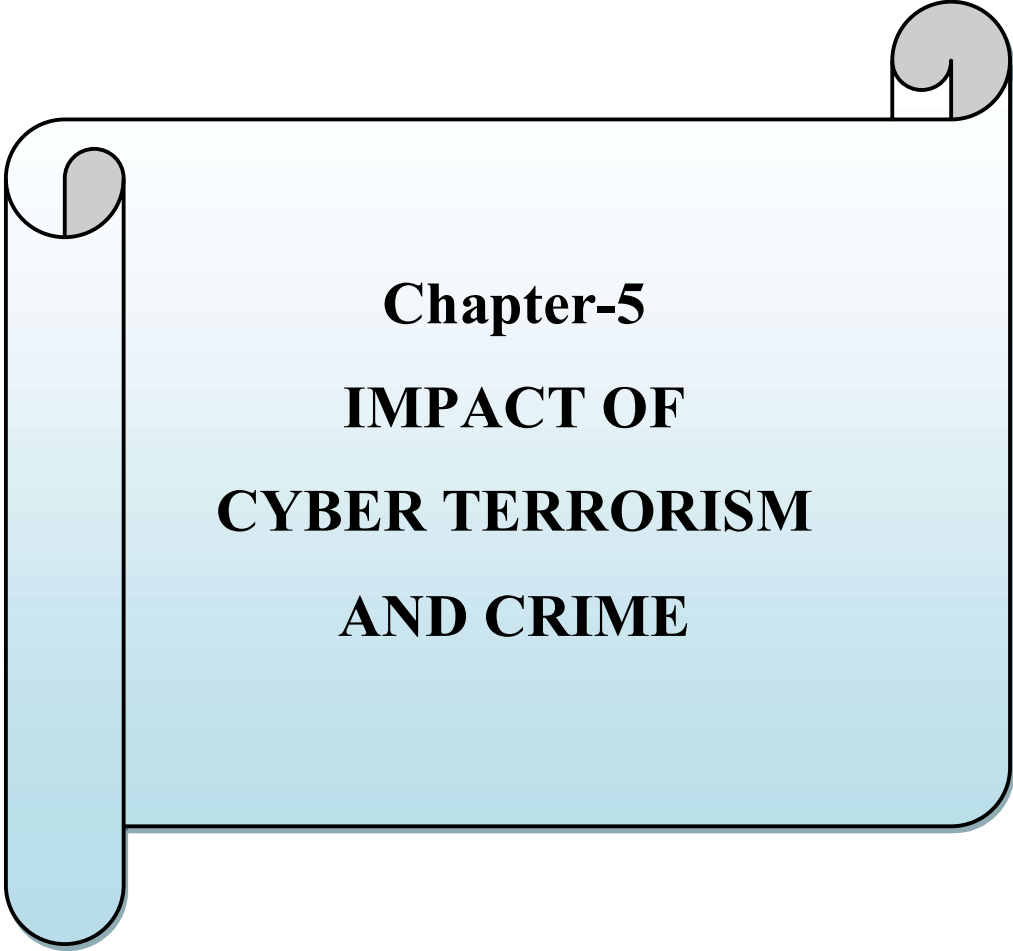
1998 In, the two-week period in the day Attlink Tamil guitar, 800 e-mail with Swaha Sri Lankan embassies. The message " We are the Internet Black Tigers and we are doing this to disrupt your communication" has been sent. Intelligence officials say it is the first computer system with the terrorists first attacked referred to did. 1999 in Kosovo during the conflict, NATO bombs and hacktivists computers powered by e-mail with the denial of service attacks are bombed.

NATO protests bombing According to the report, businesses, public organizations and educational institutions have received highly politically virus-infected e-races from multiple countries in Eastern European countries. Web definition was also common.

- Since December 1997, Electronic Trouble Theater (EDT) has been operating a web sit-in against several sites in support of Mexican zapatistas. At a given point in time, thousands of protesters point to their browsers using a target site that floods the target with a request for faster and repeated downloads. The EDT software is used by animal rights groups against animal abuse organizations. 1999 At the end of a meeting in Seattle during the WTO Hacktivists, group against another Electro Hippies web SAT - In the.

The worst incident was when a cyber terrosists Antarctic research station life support systems for the control of computers in Romania illegally bet was collected, which in the 58 scientists attended. Recently, Mr. 2007, Estonia, the Russian Federation large-scale cyber attacks by hackers aim was to create

The suggestions were coordinated by the Russian government, although Russian officials denied any knowledge of the matter. The attack was apparently shown in response to the removal of the Russian Second World War war memorial in Estonia.



Chapter-5
IMPACT OF
CYBER TERRORISM
AND CRIME

5. IMPACT OF CYBER TERRORISM AND CRIME

The current era is too fast to use the time factor to improve performance. This is possible only because of Internet usage. The term Internet can be defined as the set of millions of computers that provide a network of electronic connections between computers. There are several million computers connected to the Internet. While everyone appreciates the use of the Internet, there is another aspect of currency that is cyber crime using the Internet. Cyber crime can be defined as an act or defined, which is in violation of any law or order or sentence had been left. In other words, direct use of a criminal computer is represented as an activity involved in cyber crime, other illegal access to a computer system or database, manipulation or theft of store or online data, or equipment and data breach. Cyber security is a complex issue that cuts across multiple domains and allows multidimensional, multi-layered initiatives and responsiveness. This has proved to be a challenge for the government as the various domains are generally managed through the respective ministries and departments. The task is made more difficult for all actions and the dispersed nature of the threat and the inability to respond appropriately in the absence of idiot offenders. '

Information Technology (IT), rigidity and relative ease of development of applications that can be commercialized, in its short existence cyberspace has seen a dramatic expansion. From its earliest incarnation to a network (created by the educationist for the use of the armed forces), it has now become a global social, economic and communication platform.

Human telecommunications is understood to increase cyberspace by the recent International Telecommunications Union (ITU) centrality over data and statistics, which according to which the number of Internet users doubled between 2005 and 2010 doubled. Users are connected to a PC through a series of devices from mobile phones (PCs), and are using the Internet for a variety of purposes for storing information from e-commerce to communication. "

As the population growth means that the Internet and threats and vulnerabilities remain more or less cyberspace as before, the potential for a solution has increased at a pace that will increase the number of users. While such disruptions are causing permanent or tragic losses worldwide, they have acted as a wake-up call for their authorities to take

steps to protect their cyberspace and improve their stability. On the one hand, governments are limited by the pressures of political-military national security actors and governments on the other hand by the pressures of economic-civil society actors. '

THE IMPACT OF CYBERCRIME

Lunda Wright, a legal researcher specializing in digital forensic law at the University of Rhodes, posted an interesting research blog in October 2005. This suggests that cyber-criminal prosecution cases have increased. Cyber-piracy related to film and song work has declined. There are fancy cases and strategies for litigation. The corporation and government rely more on the expertise of computer forensic experts. In the end, intergovernmental cooperative efforts have increased. '

Organized crime groups are using the Internet to commit major frauds and thefts. There is a tendency to suggest that white crime is linked to organized crime. As criminals are shifting away from traditional methods, Internet-based crime is becoming more prevalent. The Internet-based stock fraud has affected millions of criminals annually, so crime has become such an attractive area.

Police departments across the country confirm that they are increasing the number of such crimes in recent years. This is consistent with national trends resulting from the increased use of computers, online trading and sophisticated criminals. The year 2004 is more expensive than smuggling cybercrime, and that's because technology is ready to go ahead in developing countries. Scott Borg, the US Cyber Outcomes Unit (a US director of the agency) backed by the Department of Homeland Security, recently stated that denial-of-service services should be a new wave in the future. Insects, viruses, are not considered quite mature compared to the probability of future attacks.

POTENTIAL ECONOMIC IMPACT

011 Norton Cyber Crime has revealed that the 010 in the United States, million 4 And more than a million people in cyber crime was a victim. These criminal acts result in direct financial loss of \$ 32 billion. Online growing problem analysis found

that 69 percent of adults in one day suffer from 1 million cybercrime victims as a result of cybercrime. Many see that C ' at bay crime online business is a true fact '

As today's *consumer* computers, networks, depending on *is* that, because they store information and to protect against cyber crime are used, they are at risk. Some surveys conducted in the past indicate that 3 % of company surveys have caused financial loss due to computer breaches. An estimated number of 450 million dollars, was influenced. Every week we hear about new attacks on the privacy, integrity and availability of computer systems. This can range from theft of personally identifiable information to denial of service attack.

Its dependence on the Internet of Economy has increased, a danger all exposed by cyber criminals. Shares are traded through the Internet, bank transactions are made through the Internet, a purchase is made using a credit card through the Internet. All instances of fraud in this national transaction affect the financial position of the affected company and therefore the economy. The disintegration of international financial markets can be one of the major impacts and is still a serious concern. The modern economy is spread across many countries and time zones. The global financial system due to the disruption in the other regions of the world impact. So any disruption to these systems will send a shock wave out of the market which is the source of the problem.

Productivity is also at risk, Attacks from worm, virus, etc take productive time also from *the* users. The machine is becoming increasingly slow, the server may be accessible, the network may be jammed, and so on. Such attacks affect the overall productivity of users and organizations. This also has an impact on customer service, where external customers see it as a negative aspect of the organization. Also, a significant cross-section of users' concerns about potential fraud prevents online shopping. It is clear that at.

Shopkeepers are losing a portion of their e-commerce income due to hesitation, doubts and concerns. These types of customer trust problems can have serious consequences and are described in detail.

IMPACT OF CYBERCRIME ON MARKET VALUE

The economic impact of security breaches is in the interests of those companies who try to decide where to place their information security budget, as well as where to place insurance companies that provide cyber-risk policies. For instance, physical loss, a ruling in favor of Ingram Micro is not limited to physical destruction or damage to the circuitry of the computer, but also includes the use of functional loss. This new and evolving vision of loss becomes even more important as many companies rely on information systems and the Internet in general to manage their business in particular. This example can force many insurance companies to compensate businesses for hacker attacks and other security breaches. Once the security breach features change, the company continues to assure us the environment is in danger. In the past, the Chief Investigation Officer (CIO) of the FUD Fear, Uncertainty and upper management are security investment promotion was based on suspicion. Recently, some insurance companies have created actuarial tables that they believe provide methods for measuring damage from computer interruptions and hacker attacks. However, in the absence of historical data, this hypothesis is questionable. " Some industry insiders recognize that the rate for this national project has already been determined by estimates." You need a better return on stressed industrial expert safety investment (Arosai) studies, which insurance companies use to scrap insurance, adjustable rates based on safety levels and investing in company security. Prevention strategy.

Depending on the size of the company, comprehensive evaluation of all aspects of the environment can be very expensive and ineffective. IS Risk Assessment provides a way of identifying threats to security and assessing their severity. On the basis of the selection process control to reduce the possibility is definitely, definitely risk assessment. In IS, addressing the question of what the impact of IS security breach in risk assessment will be and how much it will spend on the organization. " However, assessing financial loss from possible IS security breaches is a difficult step in risk assessment the Procedures for the following reasons:

1. Many companies are unable or unwilling to determine their financial losses due to security breaches.
2. Lack of historical information. Many security breaches remain unknown. The embarrassment of the company management, the crime and the fear of the negative

publicity these violations to expose the fear and deterred you. Companies to achieve competitive advantage of the opportunity to attack competitors have warned w

∞. Additionally, firms may fear the negative financial consequences arising from public financial security. Previous research has publicly reported an event that is usually viewed as a negative, it should be a drop in the value of Fimi stock price. "

Risk assessment can be done using traditional accounting based accounting methods like Return on Investment (ROI) method. " However, ROI can easily be applied to security investment. If the security investment is justified, the Chief Investigation Officer (CIO) will be required.

(1) Proof of proof that such potential costs can reduce the security problem to achieve the required capital investment., And

(2) proving that competitive capital investment is invested on equity capital Will equal or exceed the scope of iniyogera

This it is difficult to achieve because of the number of security events is low and there is no measurable return on an accurate assessment of the reasons for the lack of time and resources, araeai ayakauntim-based measures, such as limited also. Instead, companies are dedicating resources to the latest technology and future Z to prevent security TS In addition, this type of elongation Yogeeta facilities, such as the possibility of losing the intangible losses, intangible costs do not include violations as a result of the loss of reputation is not directly measurable.

Thus, a separate approach is needed to assess the risk of a security breach. Such an approach is definitely ' Law Firm to measure the impact of the infringement on the market value. The market price outlook reflects capital market expectations for losses resulting from a security breach. This approach is plausible, because often PR attacks affect more companies, only attacks ^ '. Accordingly, managers aim to maximize the market value of a share by investing in projects that either increase shareholder value or reduce the risk of falling shareholder value.

Impact on customer trust

Cyber-attackers entered as the second argument, and the page and try to break, the pages visited and the hope of an end to the use of the site on the basis of long-term customers Niru Z inspired will. The site under consideration is called fraud, *but the* criminal attack is not recognized as the main cause. This forces the customer to lose faith in the site and the Internet and its power.

Better Business Bureau Online (BBBO), according to the report submitted by the, on the Internet to conduct business, while 80% more online shoppers said the primary concern. About 75 % of online shoppers turn down online transactions when seeking credit card information. Internet access is growing with credit card fraud and security threats. This has become a serious problem for e-commerce.

The allegations, the consumer sentiment of fraud, are actually worse in evaluating the state. A customer's perception can be as powerful or detrimental. Therefore, users are concerned about cheating to prevent many online shoppers from transacting. Concerns about the reliability of an e-business in the context of being unsafe or disorganized have exposed the business to a buyer. Even the slightest idea of security risk or amateur trade puts potential business at risk.



Chapter-6
CONVICTIONS

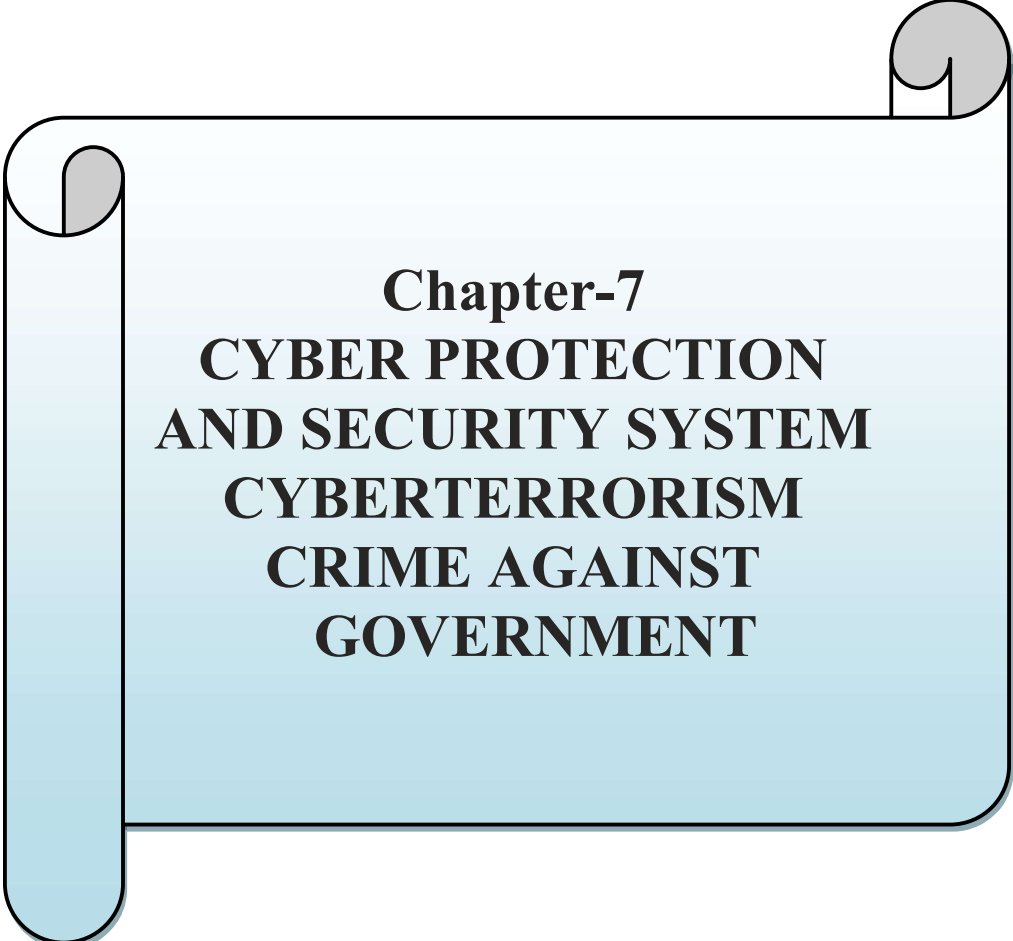
6. CONVICTIONS

Convention on Cybercrime

The Convention, effective July 2004, dealt with the first Internet or other information network and only international aid law violations. Not only does the Convention ratify all EU member states, but it also does not address cyber-terrorism. The Convention to countries, hacking, copyright infringement, computer access, fraud, child pornography and other illegal activities against cyber them to update and consolidate the criminal law to be. " 2 to 6 of the articles of various kinds of crime refers, which do not allow cyber crime and cyber terrorism, the definition of the word. Prohibited criminal activity may include cyber-terrorism activity.

Council of Council: Terrorism Conference

The Council of Europe adopted the Convention on Terrorism and increased the effectiveness of existing international texts in the fight against terrorism. Meeting terrorism to prevent member countries efforts to strengthen and to fulfill the purpose of the two ways to determine the aim of this conference is definitely " Law: First, the criminal offense been taken, and second, internally it established the (national prevention policies), both to prevent co-operation to strengthen.), And internationally (existing extradition and mutual aid arrangements and additional modifications). In other words, the Convention provides for the protection and compensation of victims of terrorism.



Chapter-7
CYBER PROTECTION
AND SECURITY SYSTEM
CYBERTERRORISM
CRIME AGAINST
GOVERNMENT

7. CYBER PROTECTION AND SECURITY SYSTEM CYBER TERRORISM CRIME AGAINST GOVERNMENT

Technological Protection from Cyber Terrorism

Information technology is the lifeline of most organizations today, such as disruptive information systems can cause your company to lose interest in the market and ultimately bring it to its knees and. 5% of companies go out of business for two weeks or more without serious loss of services without a test crisis. As a global community, we are so limited that the unit is a big city in the world, resulting in a significant wave that crashed comes to cyber terrorism, directly or indirectly climate that is a matter for all business forecasting and backup plan can be arranged. Depending on the size of the company, a backup plan can be considered a backup.

In the often-sharp events politically charged on the Internet, horse worms and Trojans become a nest, and with increasing intensity. Within a day, the current Nimda Wimms traffic generated a hundredfold quality, which took three days to code Code Wimms.

The cyber- Tiorijhm set-up was added by a group of federal republics that reported a personal computer and an integrated service provider causing many injuries to a simple telephone connection to the world, " released. Sent in the correct order. Generating a stationary bag such as a power-packed control. Computers can be explosive, and criminals and detectives are hard Will be. "

To protect your business in the event of a disaster, you will need to identify mission critical information streams that need to be protected. These may include print materials and both computer hardware and software.

(i) Backup your Data

Reducing the loss of valuable documents or data can be easily accomplished through regular scheduled backups. It is important to keep backup copies of that off-site. This will assure a fast recovery from disaster.

Various types such as floppy disks, Zip disks, re-write the CD, using removable hard drives can be backed up. The type of media you use depends on the amount of data

stored. Larger companies may also consider installing "mirror" servers, which allow the same location to be deployed in different locations. It should also be noted that reflecting outsourcing applications (application service providers) data centers in ASPs. Paper documents that are considered as important, they should be backed up with the scanner and store offsite. Numerous paper documents were used in New York after the World Trade Center (WTC) disaster. Many other organizations

Companies do not know what they have lost or how to recover lost files. Some irrelevant information and signatures *from the* accompanying.

(ii) Anti-Virus Software

A good anti-VIMS software is essential in your Counter-Ten ' Arism arsenal. It will provide continuous security and alert scans for all file inputs, outputs, downloads, program executables and other system-related activities to help prevent the entry of viruses. If the virus is detected, you will have the option to delete or clear an infected file.

(iii) Firewall / Detection Network

The firewall screens all communications on a system with e-mail messages, which can carry logic bombs. The term " firewall" is a relatively common term for filtering access to a network. They can have a computer, such as a router or other communication device, or come to the network configuration. Services and access are defined by the firewall by each user. One way is definitely, definitely, if they come from user requests to the screen . The old defined domain or Internet Protocol (IP) address. Another method is definitely, definitely system tekit access is restricted. Here are some important things to do to protect yourself from cyber terrorism:

- i. Eye of the account must have a password and passwords should be unusual, to assume strong and where possible, to the alphabet should.
- ii. Change network configuration if errors are known.

iii. Check with vendors for renovations that patch, iv. Audit systems and check logs help identify and identify an entrant.

iv. If you are never sure about the security of a site, or urJoiown accepts one of the suspicious email addresses, do not access it. This can cause problems.

Legal protection from cyber terrorism

I have the constitution of three sovereign organs work together to speak to one another in harmony with that would the, if not completely eliminate the threat of cyber security to effectively be in the kingdom. Also, an alert citizenship saibara terrorism to eradicate the promise fulfilled to that.

Legal commitments

Legislative Cyber Terrorism Niptkr Enforcement of appropriate laws can provide end -to-end help for the detrimental purpose of cyber terrorism. It is noted that the Infokeshn Technology Act provisions effectively created for the IPC 1860, the Indian Evidence Act, 1872, Bankers' Books Evidence Act, 1891 and the Reserve Bank Act 000, appropriate amendments are. 1934, a new chapter in the cyber terrorism work with terrorism bee n information technology links the Acts, 2000 is represent 2008, POTA Act and its amendment a chance for a new ordinance to his likely replacement to make laws for cyber -terrorism agreement with the EF- terrorist law spy create.

Executives concern

The central government and the state government have carried out cyber-terrorism and its phases. One can effectively play its role in dealing with the opinion of its various rules and regulations. - The central government, by the "legislature" is, "officer "and" stray", "Justifier Official Gazette and the electronic Gazette taxonomy, make rules for carrying Infomiation Techjiology provisions of the Act outside. '*' ' Similarly, can the state government, the official gazette notification from, the rules makes it work. the provision for carrying out the self-confidence of the power Te In section a 90 information technology is the law, 2000 was (- Central act 21 contents 2000 ' s), the Government of Karnataka Infomeshn

Teklinoloji (Kamataka) Rules 20047 has " set the rules" cyber cafe "., Where the cyber cafe owner / network service providers Rule 3 (1) of the Internet, services to the public to provide access to the Internet there. Cyber Computer owners have to be careful enough to make the cafe compulsory

The use of computer systems at cyber cafe is not an illegal or criminal activity. Rule 3 (2) that the owner of the cafe / network requires service providers to use any user already has installed the user can not confirm the identity of his / her computer, computer systems and / or computer network to allow access not there. Rules that provide business users of any school or college for any photo ID issued or bank or passport or voter ID card or PAN card, photo ID card or tax identification card or photo ID to the card by continuing identity can install. The cyber cafe owner's satisfaction card is issued to the employer or driver's license. Rule 4 (1) After establishing that available user identification, the following information will be retained and maintained by the cyber cafe owner or manager or guardian or any person authorized cyber management cafe register log. For each user: User (of two), sex and age of the user, (c) contains (i) from, residential address user (iv) the time to log in, and (V out) for the logout out. Rule 4 (2) if a person is available to all cyber cafe owners / Network All of the provider of identification and satisfaction of not establishing any photo ID to be able to, if he is to accept the cyber cafe owner / Network Service Provider by a photograph can be. Using their consent, a 'webcam' cyber cafe user on a computer or computer system explains that verification, photographs and photographs taken by law enforcement officers will be stored on the computer hard disk, whenever necessary to access additional log register entries. The rule also provides that if your user has been disagreeing with the photo shop, then on any computer, the use of the computer system and / or the use of computer networks or Internet cafes will not be allowed. Rule 4 (3) tests should be synchronized with Indian Standard Time (InLST) by providing regular all-time clock in cybercafe. Rule 4 (4) provides that the user's appropriate account is maintained as described by the cybercafe owner / network service provider. Rule 5 (5) It is the user's login is available to register and tally photographs cyber cafe owner / will be retained for one year by the network service providers whenever they need to, law enforcement agencies will be provided. Rule 4 (6) has the provision that cyber police officers may inspect complaints at cyber cafes at appropriate times to ensure compliance with these rules.

If a cybercafe owner / network service provider fails to maintain the log register and is liable for penalties in accordance with the time provided by law or any other law. This provision terrorist activities to the cyber cafe unauthorized use enough to take care of you. In addition, the government can also prevent websites promoting cyber-terrorism. It is to be noted that the Indian Computer Emergency Response Team (CERT-in) is designed as the sole authority for issuing instructions from blocking the web site. " CERT In the dot indicates the complaint is oral submissions to make sure that the web site is blocked it and be satisfied with that website blocking is essential. Websites blocked the IT Act, 2000 on the plain there is no provision. In fact, blakinke censorship as is considered, therefore, if you talk about it and the expression of freedom is limited, but it can be a challenge. but on prom hate, Rna, Bdnami d'Or defamation otting o thers,, promoting racism, gambling, violence and Terr promotion orism, can be blocked because of this kind of pornography and the violence in sex websites free speech and expression is a fundamental right can not be claimed. this blocked the website is " information RM onion balanced flow " and censorship may not be equivalent. if you wanted a website Laka, the Unr Easonable and hashtags based on improper and irrelevant content and external, and because, it would be irrelevant to the unconstitutionality of the attack, in which Article 14 abusers and 19 and 21 and the Constitution of India.

Judicial response

The judiciary can take its stand by taking a tough stand against threat cyber terrorism. However, it is the first jurisdiction issue be wronged as the judicial powers of the court to apply its own to satisfy the needs of the state to deal with the jurisdiction required to possess. Since the Internet "a single entity or a government -owned cooperative enterprise is not, therefore, to regulate the use of any of the rules or the law, there is no absence of the absence of geographical restrictions, the circumstances gave rise to the law, law by law, where the law is the law." What, the law may violate the country. This process further compl created a lack icated uniform and governing law aspects relevant to the jurisdictional dispute the use of the Internet revealed by. It is to be noted that the compulsory, generally, the "follow the policy" of the scholars, a country in which the designated jurisdiction can claim.

(A) the land is no activity "Te on the routine of the" can claim no country has jurisdiction on the basis that,

(B) when an activity is outside the borders of the country, a "subjective jurisdiction" may be attached, but the "primary effect" of the action is within the borders of the country,

(C) a country may claim jurisdiction on the basis of the nationality of the actor or the victim,

(D) In exceptional circumstances, the defense of nation sovereignty from the threat to the right, especially as the international community is seriously recognized.

Nexus, as well as the establishment of a cross, traditional tihyabahi international theory offender and the stage of the "appropriate" sanyogerao calls. Factual on the context hashtag depends, the court, watching the factors on the individual activity of a "significant and shortcuts impact around the" zone, "real link" Download the actors and the stage, between the existing or character, and the controller's action, the debate gave rise to, the extent of regulation is prohibited Is done, and the standards of the international community regulations. To traditional jurisdictional criteria that a payment in the name of the guide in cyberspace is the subject of analysis is derived. '^ * ^ It should be noted that it is based on the mandatory Chapter 1 (2) information then the 75 Advertising Chapter Technology Act, 2000, is that the Indian court has to deal with cyber terrorism jurisdiction over "long".

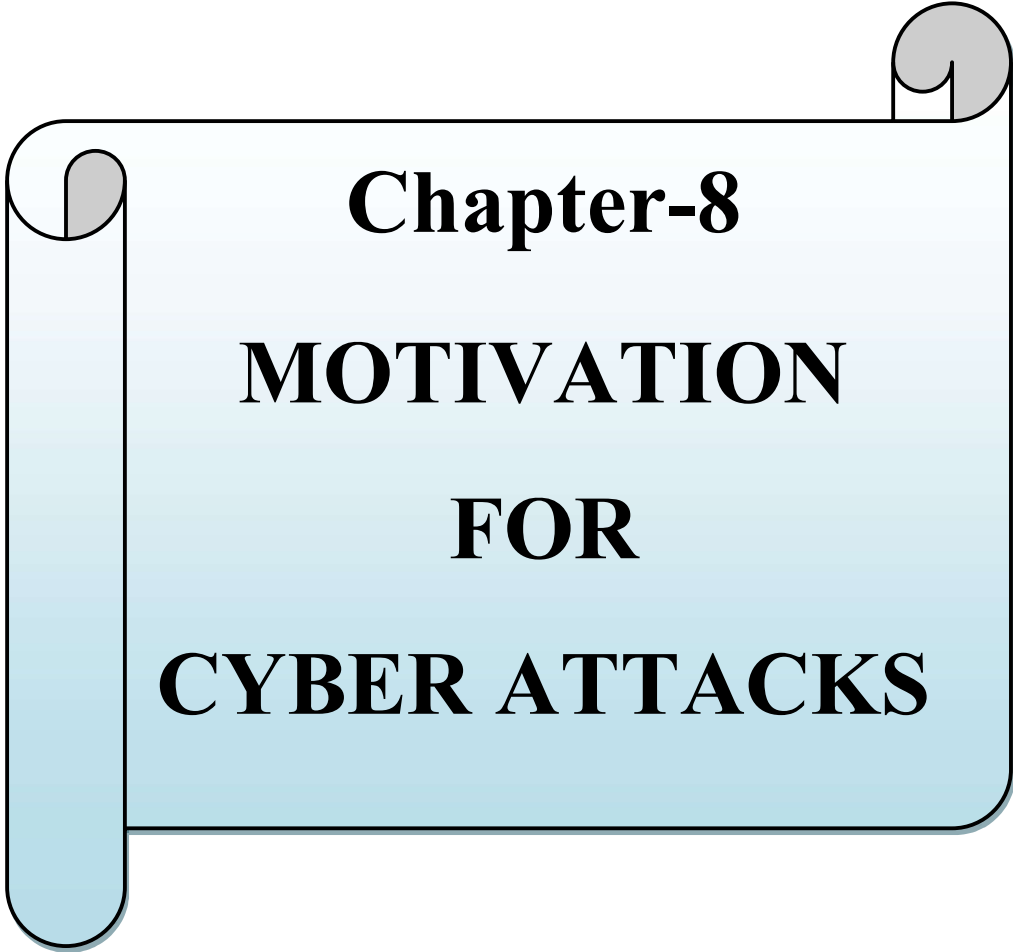
Vigilant citizenry

Cyber evil To communications terrorism state is not the sole responsibility and its Instrumentalities, who, along with the citizens Citizens equally cyber Terijm to fight against a liability under. In fact, these are definitely ” definitely the most important and effective on cyber RR materialism eradication and the eradication process. The only requirement is to encourage them to come forward support cyber Terrorism seats for the fight against terrorism a government of their financial rewards as a Sutbel the incentives could. However, it should be noted that their name discovery and protection must be confirmed before seeking their assistance. If they provide any information and evidence for the fight against cyber terrorism, the court reserves the right to remain anonymous.

Cyber Security Tips - Protect yourself from cyber attacks

How can businesses and individuals defend against cyberbullying? Here are our top cyber security tips:

1. Update Your Software and Operating System: This means you will benefit from the latest security patches.
2. Anti-virus software use : Kaspersky Total Security detects and removes threats, such as security fixes. Update your software for the best level of protection.
3. Strong password usage Please make sure your passwords are not easily predictable.
4. Don't open email attachments from unknown senders: They may be infected with malware.
5. Don't click on links from unknown senders or emails from unfamiliar websites: this is a common method for spreading malware.
6. Don't use vulnerable network vulnerabilities to attack vulnerable Wi-Fi networks in public.



Chapter-8
MOTIVATION
FOR
CYBER ATTACKS

8. MOTIVATION FOR CYBER ATTACKS

We talk about cyber crime.... motivating cyber criminals can be pretty easy. The vast majority of the two, they definitely 'Law and information means. According to a report Verizon Enterprise, Financial and spying by the motivation to attack the whole 93% of the inspiration to create.

Phishing is the root cause of cyber-attacks

Banks: Fake landing pages collect online banking credentials.

Amazon: Counterfeit Receipts Landing Pages give a variety of enhancements, including malware.

Courier: Run fake for distribution, ransom wire, banking Trojan, or links to malware.

Hactivists

In groups of them, including those whose ideologies they consent was not, embarrassing celebrity starting on a corporation to raise their weak highlights, human rights: hactivists

general political, economic reasons - said " social hactivists inspired by the sensitive, proprietary, or, sometimes, free speech, the classified data theft and Panel To four. Other times, they launch a distributed denial-of-service (DDoS) attack intended to deny access to a particular service or website, essentially flooding a website with access to even more traffic., So it is able to take all measures, which may include disaster sites. 10 State Sponsored state sponsored actors are actors in the country to promote the interests of a nation-state from the directions, financial or technical support received.

State-sponsored actors steal and out of intellectual property, personally identify (CII), respectively, identifying information, sensitive or espionage and exploitation and funds. In rare cases, these data appear for sale in underground black markets. Instead, these data are usually kept by actors for their own purposes. While data taken from data breaches may not always be visible in underground markets, they may be tools and guides to take advantage of vulnerabilities that first allow access to vulnerable

systems. For example, the researcher publishes information for published defects that are used to penetrate, and within 24 hours the harassment of the website and the toolkit included harassment.

However, there is no formal authority in handling the Equifax of note penetration.

In some cases, state-sponsored actors are creating cyber-attacks - an official letter selling computing systems is rejected, rejected, disrupted or destroyed. In one example, the 2014 attack on Sony Pictures Entertainment, seeking North Korea's political agenda and parts, sought to prevent the release of movie interviews.



Breaking the law as they are, instead of looking at it, is state-sponsoring actors to maintain that they are acting in accordance with their own laws, and most recognize that cyber-sprej is a legitimate state activity. Identity - diplomatic, financial and economic consequences - is thought to play a role in preventing such attacks from occurring or escalating.

General chat lounge, cyber criminals and cyber criminals motivated by financial gain - they care about making money.

They want our personal, financial, access or health information - so they can be monetized in the underground black market. Particularly in the retail sector, deep wounds were stolen from information displayed on the black market sites throughout the day. These markets are scattered, diversified and dispersed - rapidly growing, constantly changing, and in keeping with buyer trends and regulations to prevent enforcement and security vendors from understanding. They come in various forms. Some are dedicated to a product or a specific service. Tools needed to use a tool - Others offer a variety of products and services for the entire life cycle of attacks, one way for cyber trafficking of stolen goods. These markets are easy for almost everyone - at least at the most basic level. Anonymous cyber criminals, such as (peer-to-peer networks as shops and open markets, respectively) behind the work and their communication and transactions to hide the encryption techniques and digital (such as Bitcoin currency) use.

Cyber attacks are becoming ever more sophisticated, with cyber-hacker threats being shown in new and defined ways, which are harder to detect, and more dangerous than ever. Statistics show that cybercrime is on the rise worldwide. It is estimated that the annual cost of damage from cybercrime to the world in 2021 will be \$ 6 trillion. This is a \$ 3 significant leap trillion in 2015, which is one of the most serious threats to any business now facing cyber-attacks.

Whatever the size of your organization, you are a start-up business or a million dollar company, you should be aware of the risks of cyber attacks. What is the motivation behind all this cyber crime? Cyber hacking related research results indicate that the motivation behind the attack, 90% definitely, definitely about financial gain and espionage. The industries that are most violated are being monitored here, who is hacking and what types of data are being hacked.

Mostly broken industry

All businesses are at risk of cyber-attacks, but there are some industries that are at greater risk than others for hacking. Further weakening of this industry makes the data definitely, definitely financial, health and personal information, including the risk of theft.

Healthcare

All violations of the 24% of health sector occurs, which is 79% of medical and personal information such as social security number, name and home address, income information and contact information are stolen to medical information about specific medical programs unauthorized access to, or for the personal use of prescriptions drugs Can be used to get or sell for profit.

Threats 5 % h ' Law interiors, health care agencies in, 34% of workers fainted other company information leaked to the workers as human error is.

Food Services and Accommodation

Cyber-attacks account for 15% of all violations in the food service and housing industry. These business from your customers because they constantly have a high risk of credit card numbers, name and address, such as contact information is data collection. This stolen data can be used to gain identity theft and access to financial accounts. 99% external risk, data theft 93% with payment information accounting. Of equal concern is that in the food and housing industry, 96% of violations have been detected for months, at which time hackers have already used stolen information.

Public administration

Public administration of food and housing lags behind 14% of cases of administration violations. Personal information accounts for 41% of compromised data. The lack of cyber security funding in 2018 has cut government data with 57% of hacked government agencies. Both personal information and confidential government records are highly searched by cyber criminals so that they can sell this information to foreign entities. If hackers want to make political statements, they are threatening for public sector information.

Retail

The retail industry has always been at risk of cyber-attacks, with at least 50% of retail business in 2018 experiencing security breaches. Of the 3% data provided is compromised by the data, in which % 1% of the data is accepted as an external threat.

The information stolen by Cyber hooker includes both financial and personal data. It can be used to make unauthorized purchases of credit card information as well as identity theft.

Financial

Melt industries 7% to be made definitely, definitely financial sector, where the stolen information, 36% of personal banking and credit card information as well as contact information and made up.

The threat % 9% external, however, these threats do not compromise with the people, for the banking and financial institutions is the cost of a few million dollars. Liability Liability for retail businesses fewer than 015 in the data violating the average amount was a million million dollars.

Business services

Professional services, such as accountants and lawyers, are at risk of cyber-attacks, make up 8% of industry security breaches. The stolen data, 56% definitely, definitely personal information collected from these services to their customers. Information relating to the banking, health care and personal contact records and family data may include.

Who is hacking ?

Threats to data can come from both internal and external sources. Internal hacking comes from within the organization, such as employee defects or fraudulent employees. External threats, definitely, definitely malicious attacks, which come from outside the organization These external threats are often made by threat actors. The lure of the organization and those who disguised as a target of their personal information voluntarily provided information

System Administration (Internal)

26% of internal hackers are based on system administration. These hackers have access to sensitive data and information and usually work in healthcare, financial and public sector companies.

System administrator hackers will take advantage of the data used to provide the stolen confidential information to their own financial gain and sometimes to an external source.

End user (Internal)

22% of internal hackers are end users. These are employees who click on email links or download attachments or software that contains malicious malware.

Malware is definitely, definitely malicious software, cyber devices or computing devices to be affected by the unauthorized access to the code. Usually a website has a link or email embed, hackers just wait for the end user to click on the link or open the email file to run malware.

Other (internal)

Internal hackers are made up of about 22% of "other" hackers. They fall into different categories. For example, only those who want to access computer systems or hackers who access computer networks for any political or social reason prove it

Organized Crime (External)

Organized Crime external hacking 62% is. Ransomware is the biggest threat to organized crime, where cybercriminals and business exploitation organizations, network computing access prevent the use of malicious software, unless paid.

Other threats to hacking include DDos (Distribution Denial of Service) and social engineering. Including access to personal information from phishing in hijack accounts.

Complex (external)

20% of external cyber attacks occur by vulnerable hackers who are not part of organized crime or state-sanctioned hacking. These hackers use sophisticated methods to steal information and make money.

Asymptomatic hackers are difficult to detect. They bypass the cyber-malicious software and bring new malicious software to gain access to the computing system.

State Attached (External)

13% of cyber-attacks are managed by state-linked hackers. These cyber criminals usually have the political or social motivation to hack into computer networks. Frequent attempts are made to compromise the use and access of network traffic.

Is the data hacked ?

Hacked data from businesses and companies is precise and important for cyber criminals. Hackers look for the data so that they can earn money, identity theft can and can not blackmail. Nevertheless, other information is sold to external parties for malicious expression.

Most hacked resources

Hacking resources can originate from information that can be stolen directly from a computer's devices and networks. This information can be used directly by the hacker and contains personal and financial information. Top data assets related to security breaches include:

Database: 18% of the network is connected to a database security breach. One of the reasons for this is that law firms typically use databases to store all information about their companies and customers. Database infrastructure security is constantly under threat. The sophisticated software that hackers constantly create makes them vulnerable.

POS Terminals: POS terminals are at risk, which makes 16% of the breach. Especially malware that can be easily installed, access the system, and steal data such as credit card information.

POS controllers: Security risk by 100% definitely, definitely POS controller who saibarahakim equally at risk of malware attacks. The POS system deals with the processing of business and customer information and business payments.

Most hacked data type

The most common types targeted by cyber criminals include personal, payment information, and medical records.

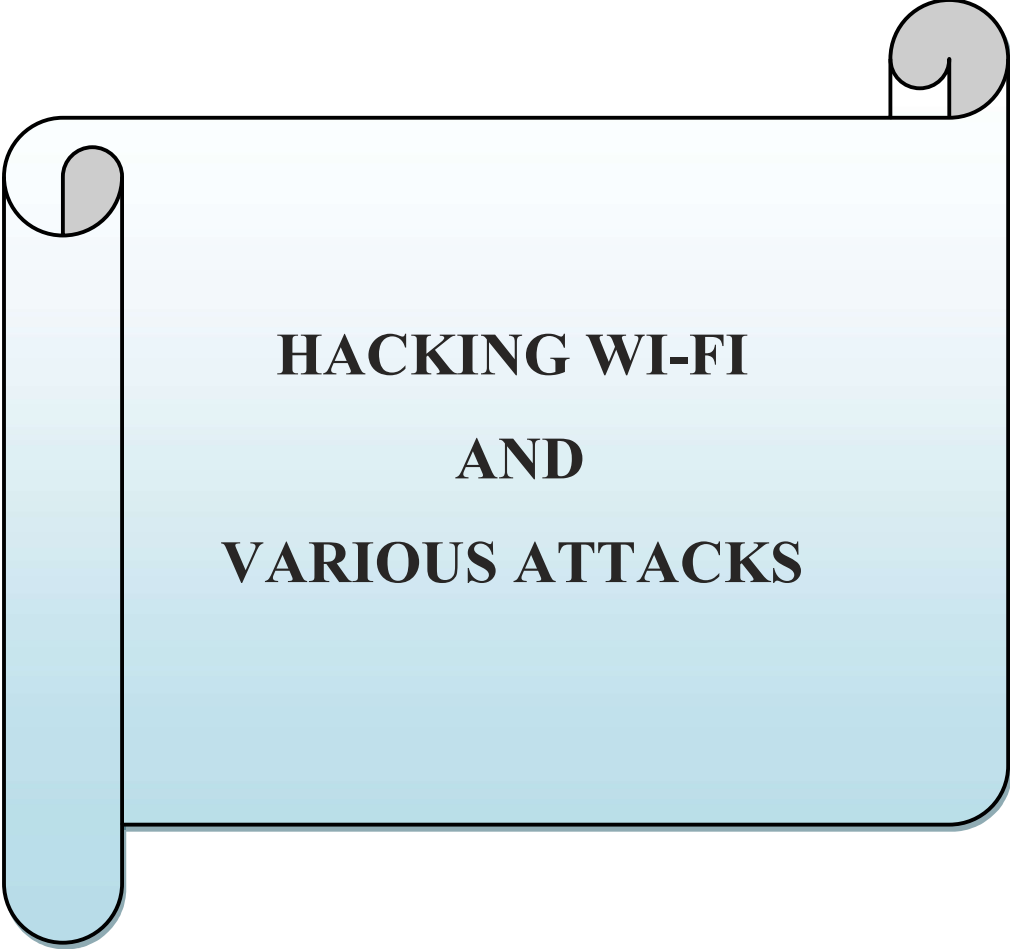
Personal: 36% of the compromised data is personal information. Including name and address, social security number, for example, e-mail and phone, including contact information, such as. This data is often used in identity theft and loans near to apply for and open new credit card can be used.

Payment: Payment information compromises 27% of stolen data in cyber-attacks and may include credit card numbers and other financial information. Once hackers have the credit card information, they are not active in a Z instantaneous can purchase.

Treatment: Personal treatment information hackers can use to buy or treat drugs. Generates 25% of medical data on security breaches.

Hackers are constantly looking for new ways to steal your data. Is your business at risk? You need to know what type of business is most risky and why. Hackers are looking for a sensitive date to use to their advantage, no matter how big or small your company is. Understand the motivations of these cyber criminals, you can use preventative measures to protect your business data.

Learn More About How to Protect Your Business and Customers or Customers Complete Hacker Objectives: The Red Flag and the Resistance Infographic by Verges. You will find out how you motivate hackers and what you can do to protect your confidential information.



**HACKING WI-FI
AND
VARIOUS ATTACKS**

9. HACKING WI-FI AND VARIOUS ATTACK

WiFi Hacking Explained

It has been established that most WIFI networks are extremely vulnerable to security breaches and are easier to hack than ever. If you're technically savvy or not, then, to Wi-Fi is the password for the security that you need to be aware of this. It is important to understand how you can compromise your wireless network and have ways to protect yourself.

Why would anyone hack wifi ?

If you've noticed that your Internet has been slow lately, there may be no compromise on your WiFi security protocol during that time. WiFi essentially gives full access to wireless network hacking crack security protocol, wireless network to view, store, download or abuse hacker. Usually, when hacked into a WiFi, so they can monitor all the data sent through the network. An unauthorized person using your wireless network will be able to see a lot of what you do online. Even if you have a website protected by HTTPS, so a compromised WiFi allows a hacker to see all of these sites processed. Below is a simple list of weak information.

It respects all the web pages you visit and your IP address

Any stored information in your browser (such as stored passwords, keystrokes, and webpage history)

All login information that you visit on any site

Any sensitive financial information is accessed or stored in your browser. In addition, hackers are able to convert any online content they see. With all the information collected from your compromised WiFi, hackers can use their information for their personal needs. They can either sell it, create your impersonation or withdraw money from your bank account. Hacked WiFi on your home network is less likely than public WiFi ; However, both are equally dangerous. Hackers target public and commercial Wi-Fi hotspot, the money banks and hospitals and the national bank stolen from people connected to networks to access to information.

GET ZENMATE NOW

What is a hacked wifi signal ?

Wi-Fi can be accessed on almost every device in the modern day: a smartphone, tablet, PC and laptop. To know if someone is interfering with your personal WiFi, there are some signs that this may prove to be the case. The most common signs and biggest of all was that a hacked WiFi doesn't always have a very slow internet connection, as anyone else can use your WiFi to surf the web. Another sign to watch is definitely, definitely your home Wi-Fi devices that are used to stop the operation of the router is still hanging on. If the light is still peeling your eyes, it means that an unauthorized person is using your Wi-Fi.

Wi-Fi attack

Major Wi-Fi was attacked by setting rogue access points.

Evil Twin attacks:

The attacking company here sets up a fake access point with the same name as Corporate AP near the premises. The access points are connected with worry about an employee inadvertently actual AP's company, he allowed, the access point gives away. Thus, the attacker is able to compromise on the connection.

Few of The Vicious Attacks

Jamming signal:

An attacker can interrupt the network connection by jamming the signal, there is a working device for this purpose known as noise generation.

Misunderstanding attacks:

If the default configuration, weak credentials, weak encryption algorithms are used to set up a router, then the attacker can break into the network.

Honey Spot Attack:

An attacker can set up a duplicate access point / hotspot with the same SSID as a public SS-Fi AP ; So, it can set a trap for users connected to these APs.

UNAUTHORIZED / AD HOC CONNECTION ATTACK:

An attacker Trojans, USER and malware using the system Ad-hoc connection can enable, or a worker before the Internet to share with the ad-hoc connections are being used. The attacker AD-HOC mode, in this mode because the connection can not compromise with the link strongest encryption does not provide.

Methodology:

The attacker will need to detect wireless devices such as war-walking, warlocking, war-driving. There are also tools like NetStamper, Kismet, to detect wireless access points and capture traffic.

Once the connection traffic grabs the, the authentication method is used to analyze traffic protocol analyzer, SSID to be identified and to be able to compromise connected devices and connections.

Depending on the protocol used for encryption, it follows different tools / methods to break the network and gain access to unauthorized networks.

Countermeasures:

Always use WPA/WPA2 encryption.

Do not share your credibility.

Don't open email without email.

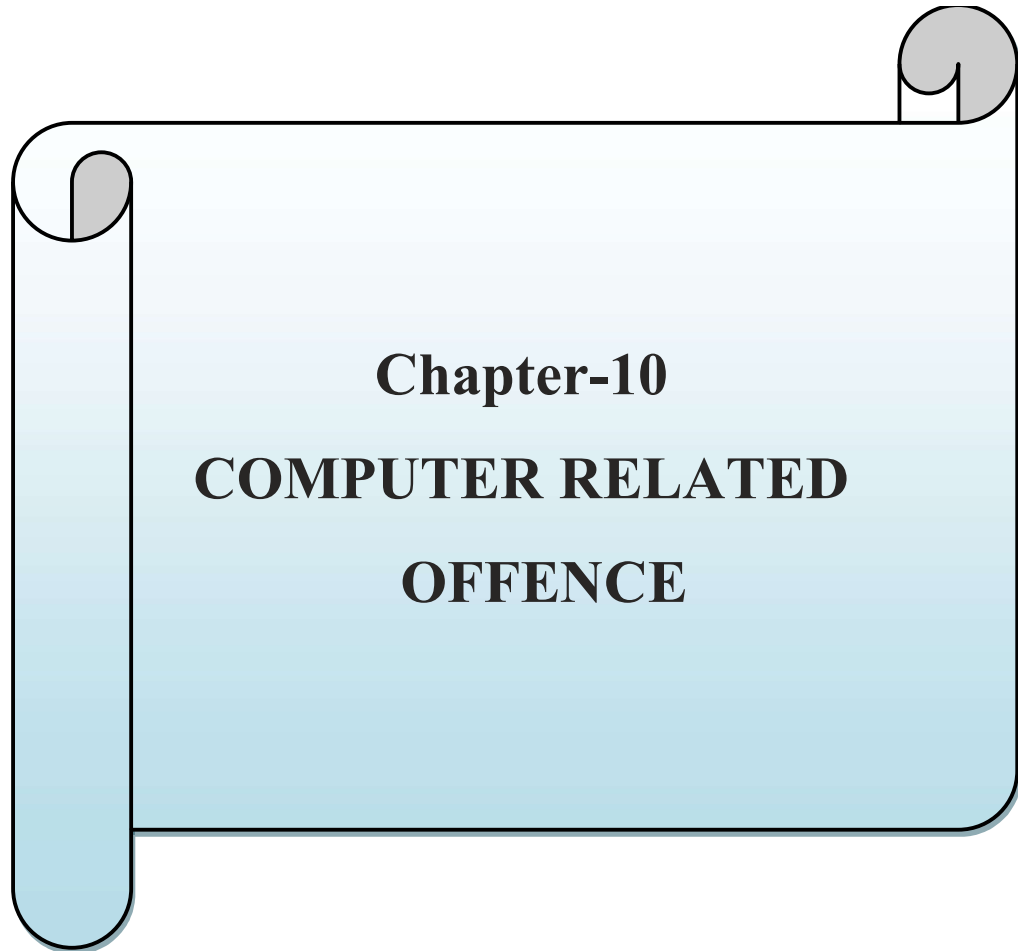
Use IDS / Firewall to filter the connection.

Change the default configuration.

Enable mac-address filtering.

Use a centralized server for authentication.

Do not connect to unreliable / public WiFi hotspots.



Chapter-10
COMPUTER RELATED
OFFENCE

10. COMPUTER RELATED OFFENCE

Computer related crime "for personal or financial gain or loss" organized cyber-crimes that include (UNODC, 2013, p. 16). The cyber category includes this category "Focus on activities... that use a computer system [or digital device] related to the offender's method" (UNODC, 2013, p. 17). 2013 Cyber Crime Detection (page 16 of the UNODC Draft Extensive Study) has identified the following cyber crime.

Computer-related fraud or fraud

Computer-related identity crime

Transmitting or controlling spam

Computer-related copyright or trademark offenses

Computer-related tasks do personal harm

Computer-related requests or "grooming" of children

Computer-related fraud or fraud

Under the Cyber Crime Convention of Europe, the Council on Crimes related to computer fraud and fraud (that is, computer fraud and computer fraud are considered part of). Council of Europe Convention on Cybercrime 7 computer, "... intentionally and without right related to fraud, the input, alteration, deletion, or the suppression of computer data is defined, the result of inappropriate information or is being done. It's such legal for example, pure it was, the data is read directly and sensible or not. " cyber crimes section of the Arab Convention Uena technology crime mixing 10 on the drone is also banned.

Computer fraud, including legal persons, authorities, agencies, impersonation and other institutions for fraudulent acts. Cybercriminals can expose people's personal information to law firms and agencies and provide money, goods and / or services to criminals. Email sent to an active organization or organizations that claim, enables users to content on the numbers and tries to follow the instructions in the email. E-mail is

sent either as an incognito email address (designed to be a genuine email from a company or agency) or to the same domain name (with some minor modifications) of an existing company or agency.

A common tactic used to send users email is to target a website link for users to click, which can be designed to steal user credentials (phishing) by downloading malware on a digital device or sending it to a malicious website. The "spoofed" website (or firm's website) looks like the agency and / or agency's website and prompts the user to input the login credentials. Email to the user as soon as the e-mail (and e-mail are requested tasks) as soon as possible to respond to the user's fear, panic, and / or the spontaneity of the concept of supply (at the bottom of Figure 1, see). For money or other benefits in order to obtain personal information as required, the user's account warning fraudulent activities, and other events and Target need immediate attention.

Computer-related identity crime and spam

In addition to online plans, financial (or financial) fraud, such as bank fraud, mail fraud, and debit and credit card fraud, is waiting online. For example, debit and credit card information has been illegally obtained, sold online, sold and is shared. Sell and share international cybercrime operations, Infracard, stolen credit and debit card information and banking information (DOJ, 2018) by the most famous line at the 2018 Illegal Onion Forum. Was purchased online, sales went and went on to sell personal information with other crimes, identity-related crime, for example, can be used, which is a mistake to identify criminal illegal to accept and / or the victim and / or the use of detection. And / or identity information for illegal purposes (UNODC, ND). Information on the type of identification information, (such as social security number in the United States), such as identification numbers, identification documents (eg, passport, national ID, driver's license and birth certificate), and online credit, including targeted by criminals, he said. (I.e., username and password) (UNODC, 2011, pp. 12-15). Identity offenses may or may not be financially motivated. For example, false identification documents (eg, passports) can be used to travel online (UN-CCPCJ, 2017, p. 4). This type of crime, as well as financial fraud, unwanted e-mails (spam), newspapers, and link sending websites that facilitate, mislead users and do not click on open or designed email

newsletters. Email links, which contain malware or that are designed to send to the Frmd website.

Computer-related copyright or trademark offenses

Council of Europe Convention on Cyber Crime 10 Section " offenses related to infringement of copyright and related rights," " Similarly, information technology crime merger on Arab Convention Article 17... the book" has limited copyright and contiguous rights "in the crime, music, painting and sculpture, such as the creation of films and literary and artistic works related to technology. (Emana computer programs and electronic databases), "" (dabluaipio, 2016, page 4).

Many international agreements deal with copyright protection, including the 1886 Bourne Convention for the Protection of Literary and Artistic Works in the 1994 World Intellectual Property Organization (WIPO) World Intellectual Property Rights and WIPO Copyright Trade-Related aspects. The 1996 agreement. There are also regional laws related to intellectual property. An important example of copyright protection for infringement is ' digital piracy' (for example, unauthorized copying, duplication, or distribution of films protected by copyright law).

Copyrighted works that are considered a form of intellectual property, such as the WIPO " mind creations, such as inventions, literary and artistic works, designs, and symbols, names, images, and defined as used in the trade," he said. 1967 Convention on the article, the World Intellectual Property Organization (the WIPO), founder of the 2 (viii) the

Intellectual property... includes: literary, artistic and scientific works,... artists' performances, phonograms and broadcasts,... innovation in all fields of human endeavor,... scientific discovery,... industrial design,... trademark, Service marks and trade names and titles... protection of unfair competition, and intellectual pursuits in the field of art, scientific, other literal or artistic As a result of the jokes, the session Mr. Okay.

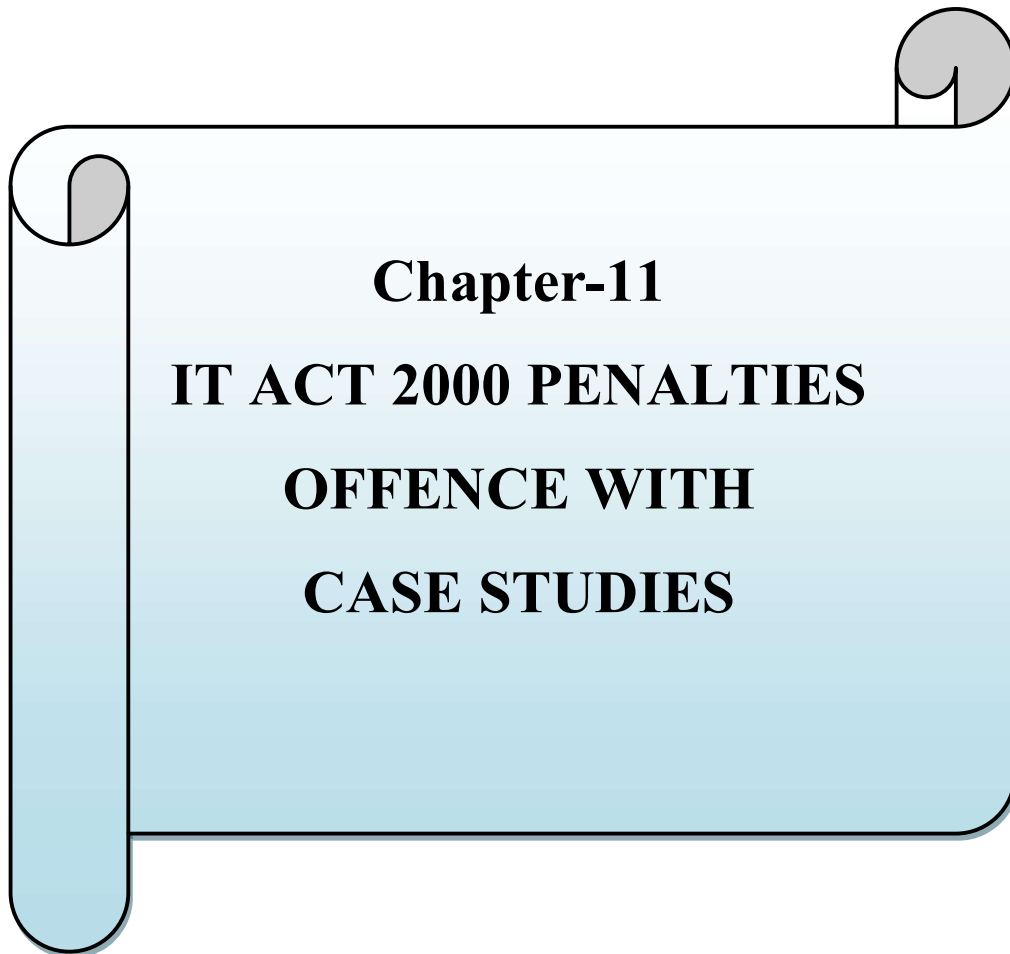
Intellectual property, therefore, not only copyright (eg, books, songs, movies, software, covers, etc.), but trademarks (ie, names, symbols or brands, services, or good deal logos), patent (large) novel unique creations, Innovation and innovation) and trade

secrets (that is, business processes and practices that cover secrets) and valuable information about protecting business competitive advantage. Intellectual Property Cybercrime Intellectual property is explored in more detail in Cybercrime Module 11 on Criminal Property.

Computer-related tasks do personal harm

The UNODC draft by the 2013 Cybercrime Study, " Because computers are at a loss for work " involves " harassing, intimidating, intimidating, or using the computer system to cause intimidation or intimidation" (17). Examples of this type of cyber crime is definitely, definitely Cyber stalakim, saibarahaujim and cyber bullying. These cybercrimes are not included in multilateral and regional cybercrime agreements (eg, the Cybercrime Convention ; the Arab Conference on Cyber Security and the African Union Convention on Cyber Security and Personal Data Protection and Information Technology Crime).

Cyber- stalking, cyberhousing and cyberbullying have been used interchangeably. Some of the children or cyber bullying (eg, Australia and New Zealand), no law or victims in criminal cases referred to it, the United States and against the states by the behavior of young children to use the word cyber bullying. Used to specify. Some countries cyber bullying not use the word, but cyberbullying term in a variety of positions, such as cyber crime or saibarastyakim, or cyberbullying (Austria and Germany) on the Cyber-bullying (European Parliament, civil rights and constitutional issues, 01 2016, 2425) using) To describe, Others do not use any of these words. For example, jamaikarara related, 2015 the Cyber Crime Act 9 (1) paragraph, " malicious and /or offensive communication" has been banned, that "(a) the use by criminals every... other person's computer sent. Any data (messages regardless of whether or otherwise) that is obscene, a threat to the structure, or the nature of the menacing is, and (b) that is intended, or is heedless, Such as transmitting information to the sector, causing discomfort, distress, or anxiety, that person or another person".



Chapter-11
IT ACT 2000 PENALTIES
OFFENCE WITH
CASE STUDIES

11. IT ACT 2000 PENALTIES OFFENCE WITH CASE STUDIES

INDIAN CONTEXT

The Information Technology Act, 20, passed in India, indicates confusion over jurisdiction in the context of the Internet. Information Technology Act, 2000 of the 1 section of the applicability of the new law. Generally under the rule of law, India can be broadly divided into the following major categories:

1. Except in Jammu and Kashmir, laws apply to all states of India.
2. The laws apply only to Jammu and Kashmir.
3. The law applies across the country.

Jammu and Kashmir has been given a special status under the Constitution of India and special laws apply to that state. Considering the universal nature of the impact of computers and the Internet, the Legislature has decided that the Information Technology Act 2000 will come into force across India, including Jammu and Kashmir. Section 1 of the Act, Article 2, begins to extend across India, and applies to any offense or violation committed by an individual outside India, as otherwise preserved. Article 75 clause (2) only stated that "the law is outside the country of a person, computer, out of the computer system or computer network or a crime involving crimes to be completed happening, will be applied in India". The provisions of this nature for several reasons effect is unlikely.

First, it is unfair to suggest that the moment an Indian computer system is used, an action defined by Indian law as a "crime" may be subject to the jurisdiction of the Indian court. For example, let's consider a web site located in a foreign country. This site may host content that is completely legal in its own country, but may be considered offensive or illegal in India. Does anyone want to visit this site on a computer located in the country, that means being charged in court on the site? It seems to violate the principles of justice. As stated earlier, examining the judicial tendency of the amount of activity in a site-specific jurisdiction is a more equitable way to determine jurisdiction. Moreover, although the claim is the jurisdiction of the court and the judgment passed on it on the basis of the export policy of the law, it is unlikely that the foreign court will accept this judge because the rules used by the law will not be accepted

as grants. Jurisdiction of the Indian Court. It would also invalidate the law.

Regarding the jurisdiction of the Internet, Indian jurisprudence is almost non-existent. First, in India as a result of the current government crackdown single model, inter-state conflicts no private international law assumes a level not. As such, there are very few developmental paths to the rules of private international law in India. Moreover, in some cases the courts have surfaced, where the Indian courts have created a revenue earning on a foreign matter from the area where needed. However, this national judicial development will become necessary in the future, as the geographical and regional restrictions on shrinking border jurisdiction and internet sets will be integrated. It is worth considering jurisdiction at two levels. First, as a foreign court exercises jurisdiction over Internet-related matters (as can be clearly seen from the cases discussed above), the outcome of a decree passed by a foreign court against an Indian citizen should be investigated. In other words, under what circumstances can a foreign court be prosecuted against an Indian citizen or a person living in India ? In order to better understand the rights of Indian nationals affected by the work of foreigners, it is necessary to examine the circumstances in which Indian citizens will take jurisdiction over foreign nationals.

OBJECTIVES OF INFORMATION TECHNOLOGY ACT, 2000

The purposes of the Information Technology Act, 20 are defined as:

" Electronic data interchange and electronic communication via other means to complete the transaction for the legal recognition," electronic commerce "as mentioned, communication and data storage, the paper-based method options, including the, government agencies with documents, electronic filing easier and IPC from, the Indian Evidence Act, 1872, meeting Bankers' Books Evidence Act, 1891 in Color RBI Act, 1934 and the factors associated with this case for the correction.

"

In other words, the objectives of the interventions ' Law: -

- To provide legal recognition of transactions conducted through electronic information exchange and other means of electronic communication, often referred to as "electronic commerce" in place of paper-based communication methods ;
- Legal recognition of digital signatures for the authenticity of any information or substance that any law requires under authentication ;
- Facilitate electronic filing in government departments ;
- To store electronic data ;
- Legal approval for transfer of electronic funds between banks and financial institutions ;
- Providing legal recognition to bankers in electronic form for keeping books.

First Act 1 sections each section of the United Nations Commission on International Trade Law relating to the Model Law on Electronic Commerce Information. This is the eleventh chapter is divided into 94 different categories consists of. Its 4-T programs, schedule, I would like to amend the Indian Penal Code ; Schedule II seeks to amend the Indian Evidence Act ; The Third Schedule seeks to amend the Bankers' Book Evidence Act ; And the Fourth Schedule has been amended by the Reserve Bank of India.

The law laid down several provisions for that purpose. Its purpose is to provide a legal framework so as to achieve legal purity for all electronic records and other activities performed electronically.

SALIENT FEATURES OF THE INFORMATION TECHNOLOGY ACT, 2000

The law is for the first time defining cybercrime and hacking harassment, providing for penalties and damages, unauthorized access to computer networks, alterations to databases, launching computer viruses, disrupting services, copying intelligence property (ipr) protected software, electronic documents and electronic fraud. Deception. IT Act 10, 000 provides for a fine of up to Rs provides computer systems to damage 1 fined, and a three- year prison term. 2 lakh for hackers. However, the current police investigating officers, forensic scientists and judiciary are not familiar with the complexity of the Internet, so the punishments are not understood. The law is not fully covered with no

experience, other countries do not have past experience. Accordingly, future changes, based on experience, are not spared.

The main features of IT Act 2000 are as follows:

- E-commerce provides legal recognition, which means contracts can be applied.
- Records can be kept in electronic form. Written records are also electronic records for media law purposes.
- Provides digital signatures for legal recognition. The digital signature certificate must be approved by the authority. Certification Authority confirms the authority's authority to conduct inspections by the controller.
- Cybercrime is defined for the first time.
- Whether or not it is a cyber crime, the officers have to be appointed to decide. Also provide for the Cyber Regulation Advisory Committee.
- Information Technology Rules, 2000 Information Technology (authorized officers) Rules, 2000 and the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 provides.
- Cyber Law Appeal Tribunal to advise hearing appeals against authorized officials
- Indian Penal Code (18 60 0), the Indian Evidence Act (18, 72 b), Bankers Book Evidence Act (1899) and the Reserve Bank Act (193 Act) information technology system has been integrated.
- Information Technology (Certifying Authority) Rules, 2000 also sets forth Information Technology Security Guidelines in Schedule II.
- The certificates also provide security guidelines for the management and management of the Authority (CA) and protect the integrity, confidentiality and availability of their services, data and systems.

The law has led to an exponential growth - trade and other Internet-enabled services like e-trading, e - shopping and e-banking. Sale of immovable property or any interest in any property of the transmission or the provisions of the law interactive materials, power of attorney, a trust, a will and an agreement is not applicable. It is very

important that it applies to any outside India crime or violation, whether it be from a single person (irrespective of nationality), including a computer, computer system or computer network in India. It turns out the information network service provider (ie, its power has given any information) to a third party at its sole discretion or their respective data as intermediaries, if they were not created without evidence to offset their information, and they are careful to prevent the commission. Accepted. However, even better, different computer crimes that have not been defined yet, can be adopted to deal with rapid technological changes in the future.

The Information Technology Act 2000 is the first cyber law in India, which is passed in the Parliament of India. The interesting thing is that not only Jammu and Kashmir plus India applies to all, but any violation or violation of any person under any place anywhere in the world. State governments have also been empowered to make appropriate rules in the field of information technology. In fact, the Department of IT Law 90 clearly states that the State Government may, by notification in the Official Gazette, implement the provisions of the Rules of Information Technology Act. Rules made by the State Government may include electronic, electronic records of the general public, through which the Department of the Government contacted, created or issued and filed any fee or payment to collect any fee: to create or issue an electronic record. The state government has to make appropriate power laws, the legislators are involved in various measures taken by the state powers, which are detailed in the Indian constitution. Of course, it is to note that IT needs the 90 sections under the State Government by the made the rules approved by the state Legislature before each House of the Z ksana Z made a will.

In its rage, the law, therefore, only recognizes the utility of e-commerce and provides the security required for the transaction by a necessary legal framework, but the IPC, the Indian Evidence Act, has any subsequent amendments to the reserve. The Bank of India Act and Banker's Book of Evidence Act, in order to provide legal purity in addition to the advantages of electronic transfer fund account books between guilt-free electronic media and document-based transactions and financial institutions and the equivalent of crime with banks. Electronic forms by banks.

JURISDICTION- THE CONCEPT

The effectiveness of the judicial system depends on the key rules, which define every aspect of the system's functioning ; Primarily, its jurisdiction. The court must have jurisdiction, venue, and appropriate services to hear a case and make an effective decision. The court's power to hear and determine a case. Except, the decision of a court's jurisdiction is void and weak. There are essentially two types of national jurisdiction, namely, content jurisdiction and personal jurisdiction. Subject jurisdiction is defined as the ability of a court to hear and decide a particular category of cases. The case was filed and a court case was filed on behalf of the court to file a case against the person of the ability to determine whether the court had the power. It's done These two courts of the decision to satisfy the lead. This court, which has jurisdictional appearance and ensures enforced power in the absence of such power, the court has decided, uses little or nothing.

CYBER JURISDICTION IN INFORMATION TECHNOLOGY ACT, 2000

However, the law has gone too far. It also applies to anyone in the world violating or violating the provisions of this law. By this provision, the law assumes the jurisdiction of violators of the Information Technology Act, 20, outside the territorial limits of India. This provision is explained by the unique nature of cyberspace, which knows no boundaries. Information Technology Act, 2000 Act is supplied, if not mandatory, the law provides otherwise, according to the AP level violates any Aprad- d'Or is the person regardless of their nationality, Delhi, India is committed outside. It is clear, however, that this law will apply to any offense or violation outside India if any offense or violation is involved with a computer, computer system or computer network located in India. Up to the word "crime-door-door conduct violation, computer-less system- door computer network located in Delhi, India" from a computer is very important in preventing my jurisdiction over IT related work done outside Delhi, India. Assuming the law jurisdiction for the formation of a *fence d'Or* law, which New Delhi, IT-related violations committed under outside India, he said, it has been proven to work on a computer that is mandatory ; Computer network system - Door Delhi, India with computer. For example, the United States, where a website has been created

where pornographic materials are, the site is not built or maintained or computer, computer system or computer network located in sites in India until the jurisdiction of the IT Act gives the right not unless not. The above-mentioned Web site, the door is using a server but no other computer network in diameter, IT law related question Site Act section 67 of the IT department about the authority will receive. Another example Juris to explain the laws related to IT, where America lost a person behind a computer in New Delhi, India, 66 in the system Door Network hack hacking law is not to punish the alleged role of IT in connection with his involvement in India's computer to occur. Similarly, where a computer is a virus anywhere in Delhi, India plants a person, that under Article 43 liability and through it will be net loss compensation related to the ex-compensation law (c) 10 million ordinary chat lounges to hunt for Rs. 1 crore victim.

Act section 75 of 75 seats in the IT-related divisional crime - of or otherwise, such as the Indian Act in other laws such as the Penal Code for violating the ban, such as the Indian cyber-crime against the judgment of the Divisional Law, 18, 60 and 0 at the bottom to get to India, for example, sec Code, 1860, Code of criminal Procedure, 1973, the provision has been determined by the. Preliminary ideas on the jurisdictional IT Act and the Criminal Procedure, the same part for 1973, though said separately. Code of Criminal Procedure, compulsory crime in 1973 in the area of fundamental rights code that legal theory, commonly called over and in a local court with Juries' tried by the way it is. These policies apply to the Criminal Procedure Act of 1973 for the determination of jurisdiction by courts and police. There are multiple places where such a case is on, or clearly in a position to offset in a second position, or where it is continued and continued on the local area, or where the crime is associated with different acts, it can be tried with the court bond by different local areas May ask to be juristic in such areas as political. Where In the event where it is uncertain in which of several areas the offence was committed, again it may be inquired into or tried by a court having jurisdiction over either of such areas of uncertainty.

The case where any cause of action is a crime, whatever has happened and as a result, it may be tried, the crime may be examined or the court has done so by jurisdiction or the result has been effective. For example, in a case of defamation, either of the courts, i.e. of the place from where the defamatory letter was e-mailed and the place at which it

was published or received, if different, shall have jurisdiction to inquire and try the same. To cite another instance; where in pursuance of misrepresentation by A through e-mail from place X, property was delivered at place Y, A can be tried for the offence of cheating either at place X or Y. In a case where a person in Bombay does an act of hacking of a computer system located in Delhi, he may be tried either in Bombay or Delhi.

An act which is offset in this case by reason of another law, which, if a crime or a crime was the subject capable of organizing a crime, can be examined by the first offense or tried by a court whose local jurisdiction was also effective. For example, replacement X low quality fertilizer production, which is marketed via e-commerce at the Y location, can be launched in one of the locations such as the Prosecution Sub - standard fertilizer is a crime. Rhea GD Tee by substandard construction.

In addition, the provisions of the law of any crime, fraud, deception involved in the case were to be followed by the ministerial d'Or telecommunications messages, trying a court has jurisdiction d'Or, this in the letter or mesake can be questioned, the apostle St. - Do ' and the same was received. In addition, any interrogation of the property could be fraudulent or fraudulent in the property or the area could have been tried by the court where the property was betrayed by the person or where the accused person obtained it.

In cases where two more courts or a similar offense is required for trial and the question whether the jurisdiction is questioned or the crime is tried in court, the question will be decided by the High Court, which is the formality of both these national courts. However, if the court subordinate Nate the High Court, the jurisdiction of the High Court in whose jurisdiction the criminal case in question before the appeal was launched will be determined by the. In such circumstances, respect for all other proceedings will cease. Where there is a crime of two or more courts, the choice of the court for the institution of the case depends on the complainant. He will definitely choose the stage, which is the most convenient for him and the most inconvenient for the accused.

Code of Criminal Procedure, 1973 and the IT Act, 2000, Section 75 in the area described in the law, such as going to discuss here, clear, specific and are involved in many different situations that usually occur in cyber crime cases. Its nature and purpose is not to run the Internet conversation run door partying with each other physically towards each

other. Due to the global access to the Internet, cyber crime usually ignores geographical boundaries. These factors imply that in most cases of cyber crime, except where insiders are involved, there would be two or more places, one from where the cyber criminal inflicts the injury—for instance hacks, and the place where the injury is inflicted—for instance at the location of the victim computer, which is hacked. This is in contrast to traditional crimes of rape, murder and kidnapping where the criminal and the victim are at the same place. Moreover, every criminal makes all possible attempts to conceal his identity and place of operation. Alibi is a common defense in criminal matters. Accordingly, every offender makes every effort to conceal his identity and place of operation. Defense Ministers are a common criminal matter in Alibi. These issues, along with the basic instincts of a criminal premise impossible internet anonymity provided by the cyber Criminal makes the nearly invisible. Thus, cyber crime law, the jurisdiction of the practical application of the context, in most cases, Thus, in terms of practical application of the law of jurisdiction over cyber crimes, in most cases, the place of jurisdiction shall be where the victim is inflicted with the injury, whether personally, for instance by fraud, or on his computer, computer system or computer network.

There is a valid point of criticism that this national law cannot be applied in the real world, with the additional authority granted by the Legislature. It is contrary to international law principles to accept the jurisdiction of another country, and therefore, jurisdiction may be contested in different courts in different national jurisdictions. It is also important to note that there are differences between national laws, legal procedures and procedures.

That it is a problem compounded by a specific law within a national jurisdiction and legal not to be prohibited by law, but the same activity is illegal and prohibited by law, is to be practiced in other national jurisdictions. Another basis for criticism is that the national provisions in Article 1 do not meet the criteria for how to apply effectively to boundaries and jurisdiction. Governments may adopt extradition procedures to bring cyber criminals out of their country's jurisdiction, provided that there is a valid extradition agreement between the countries concerned. But the way, as set forth in the Information Technology Act, 2000, Article 1, is a reason for a complex area of problem of actual day-to-day implementation.

The existing international law on the sovereignty of a nation also states that a sovereign assumption can legislate to affect people living within its territorial borders. However, the history of the geography of the Internet is seen and the nature of the network transactions is done, the jurisdiction over which the whole thing is planned. This is even more evident from the emerging policies regarding various decisions on jurisdiction over the Internet. At the beginning of the Internet, the legal issues of the heart and the mind, the continued issue of jurisdiction challenges the strange underlying character of the Internet of Communities and Nations. Section 1 (2) and section 75 of the IT Act, 2000, provide for the extra-territorial jurisdiction of the Indian courts, which, however, seems impossible. There is no uniformity of the courts of India following the tendency to demand jurisdiction based on site activism in the United States. Until now, in cases related to various Internet domain names, the Delhi High Court has taken jurisdiction only on the basis of Internet access.

Famous Yahoo! France's rights in the ***Yahoo! Inc. v. La Ligue Contre Le Racisme et L 'Antisemitisme***, judicial thinking and refined jurisdiction. This decision reached significance and consequence on the whole matter of jurisdiction. From now on, anywhere in the world outside of the court's jurisdiction over Internet transactions and to websites and may take about could

This decision underlines the principle that even if a foreign court passes a decision or an injunction against a country's legal entity, the State has said that this decision or directive will not apply to the country's legal entity or its citizens. Fundamentals and the underlying decision of the foreign court or to the Supreme Court and the country's constitution, the country will have to check the local laws first, before it could be implemented in the country. Country a. It is clear that the court is looking at the totality of the situation when it is determined whether the areas of exercise related to the individual are involved in internet-related activity. However, with the advent of the Zippo case in the United States, the jurisdiction's legal policies have changed. In this case, the US court has decided that there must be something "bigger" than me to enable the court to accept jurisdiction. It can be seen that the IT Act provisions, in particular Article 1 (2) and section 75 (1) of the Indian jurisdiction of the Indian point of view on how the provisions have been revealed, which is totalitarian in

its judicial system. If it is a violation of IT law or computer related crime, influence or affect the computer system or computer network located in India, This extraterritorial jurisdiction all across the world can be exercised if the offence or contravention of the IT Act concerns or impacts or affects a computer, computer system or computer network which is located in India. In practical terms, such an extraterritorial jurisdiction can hardly be enforced given the present growth and context of international Law, Cyber law and cyber space.

As per sub-section (3) of Section 1, the Information Technology Act, 2000 shall come into force on such date as the Central Government may by notification appoint. The Central Government issued a notification on 17th October 2000 bringing into force The Information Technology Act, 2000.

POSITIVE ASPECTS OF THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 20 is a praiseworthy attempt to create the legal infrastructure necessary for the promotion and development of electronic commerce. Before the IT Act, 2000, came into force, the judiciary was reluctant to accept electronic records and communications in India as evidence. Even email has not been accepted as a recognized legal form of law and communication in the law courts under the prevailing law of India. IT Act, 000 in electronic format by the legal recognition of the scene has changed. In fact, the IT Act, 2000 is one step ahead.

From the corporate sector perspective, IT Act 2000 and its provisions include the following positive aspects:

1. These provisions for the corporate sector mean that email is now a legitimate and legal form of communication in our country, which can be properly generated and proven in a court of law. Just as a form of communication with entities outside the company, but inside the company as well as an indispensable tool of communication in, e-mail, corporate thrive today. Corporate should realize that writing an email when they need to be more careful, so as to be out of the company, or email, whatever the language, a legal court documents may be, the company as opposed to sometimes. Even inside-company notes and memos in ordinary chat lounges, so far used for sole government purposes, will be accepted by

the Information Technology Act, 2000, as evidence in court, covered by law. A lot will depend on how these emails are proven in a court of law.

2. Companies will be able to do electronic trading using the legal infrastructure provided by IT Act, 20. Indian Saibrlo under the influence of the, electronic commerce growth is mainly regulated in our country there is no legal framework was, because it was interrupted. Online Commercial Transactions.
3. Corporations now IT Act, 2000 and under the legal validity and authorization of transactions online, they will be able to use the digital signature will be.
4. The IT Act, 20, also opens the door to entry for corporates who have the business of certifying the authority to issue digital signature certificates. There is no difference in the law between the certifying authority being appointed such a legal entity, unless it has been set by the Act, 2000 norms, and has to comply with rules and regulations.
5. List of law in any office, authority, body or agency has no form, the owner or any other documents in electronic form applications or controlled by the government, capable, competent set by the government, which is the cost, time savings. And waste valuable manpower.
6. To keep and maintain corporate valuable and corporate information is mandated by various laws of the country. In the IT Act, 2000, it is possible for companies to retain legal information in electronic form, if any
 - The information contained is not yet accessible to us for later reference ;
 - The electronic record format where it was originally generated is maintained, transmitted or received or formatted, which may appear to have been originally generated, transmitted, or properly received information ;
 - Details, which will help identify the source, destination, date and time of these national electronic records or be available on electronic records.
7. IT Law, 000 Important addressed the issues of security, which is crucial for the success of electronic transactions. The law gave a legal definition of the concept of secure digital signatures, which would have to go through a system of security procedures as agreed by the parties concerned. The coming years, a secure digital signature context, particularly from the corporate sector, the economy will

play an important role, because they will enable online transactions more secure.

GREY AREAS OF THE INFORMATION TECHNOLOGY ACT, 2000

1. IT Act, 20 shall be enforced for any offense or violation committed by any person outside India, not just in India. This provision was not clearly prepared in Section 1 (2). It is unclear how and in particular this law will apply to any offense or violation committed by any person outside India.

2. There is no justification for excluding it from the applicability of IT Act, 20. The net effect of this exclusion by the center is an e-commerce transaction, a negotiable instrument obtained through, are excluded from. The Protection of IT Act, 2000 This refers to the promotion of electronic commerce and begins with the exclusion of real estate from the field of electronic commerce, an argument that defies logic.

3. IT Act, 000 countries have failed to give legitimacy to transfer funds electronically. IT Act, 000 of electronic payment, digital cash, electronic cash, electronic money or other existing electronic payment system does not recognize the idea.

4. Domain names are not defined and the domain name does not find any references to the rights and liability laws of the owners.

5. IT Act, 000 intellectual property rights in any issue related to conservation does not work.

6. IT Act, 2000 and to 40 the number of sections language. 40 paragraph customers to perform the eighth chapter of the pair has the right to. It has been said that where a digital signature certificate, which corresponds to the public key customer private key, that should be listed in the digital signature certificate, adopted by the customer, the customer key pair will be executed by a security mechanism. The entire wording of that section is flawed and shows that the acceptance of a digital signature certificate honors the original generation by the customer.

7. IT Act, 2000, only a limited number of cybercrime crimes such as harassment, computer source code, harassment, publishing pornographic electronic information, violating security measures, digital signature certificates disclosed for some nasty purposes. Except for this crime, other cybercrime is not covered by IT law. IT Act 2000

Cyber-in rows, cyber harassment, cyber defamation, cyber terrorism, spamming, cyber-fraud, cyber gambling, Internet hours, theft, cyber theft, cyber fraud, cyber fraud, credit card fraud, cyber fraud, including cyber crime, including not to have. Identity fraud, e-mail spoofing, credit card fraud, chat room abuse, cyber money laundering, sniffing passwords, spamming, electronic eavesdropping, child pornography, mail bombs, e-mail scams, etc.

8. IT Act, 2008 chat room to deal with crime in all kinds of abuse silent.

9. The IT Act, 2008 states that it is silent about online credit card payments, misuse and misuse of credit card numbers.

10. IT Act, 2008 Chapter XI described the lack of offense, or otherwise completely silent. Section 65 of chapter 78, section 78, at any time, a clear reference to determine whether or not a crime is guaranteed under section.

11. Information Technology Act, 2008, did not address many important issues related to e-commerce, privacy and content control to name a few. Privacy issues have not been touched at all. Article 21 paragraph under the right to privacy is a fundamental right has been recognized as.

CHALLENGES OF CYBER CRIME IN INDIA

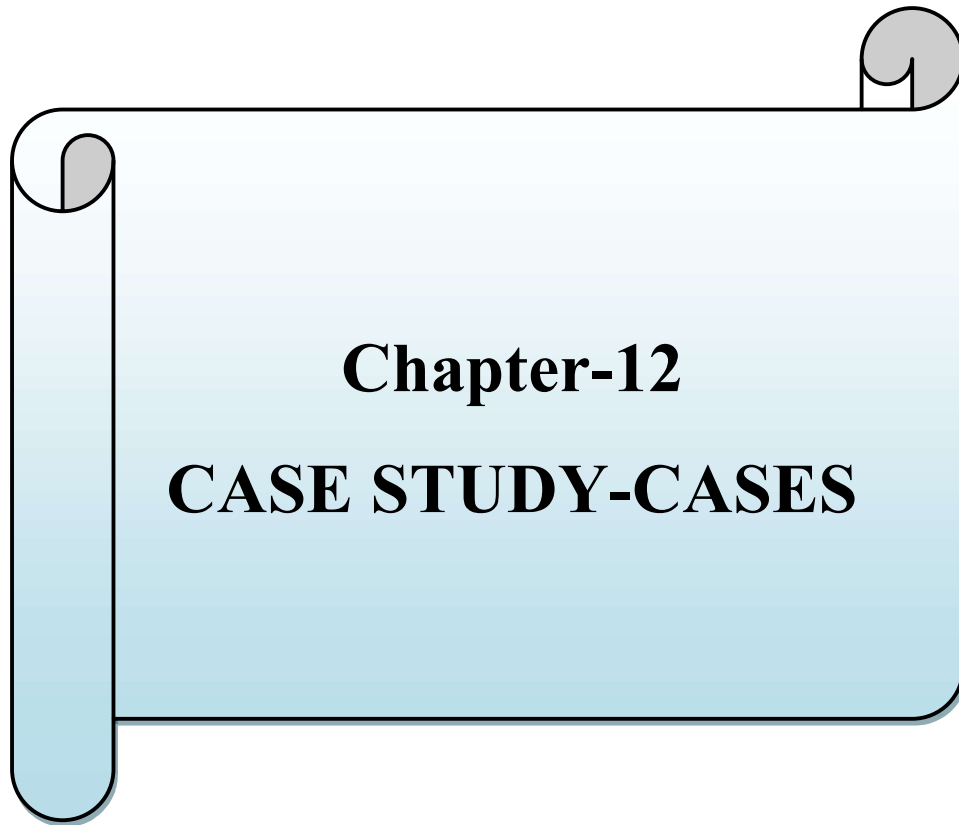
Cybercrime is no longer a maya in India. If computer users, both public and private, are not prepared for this challenge, the situation may be over. The temptation to attack the police, especially the computer system, is as great as a crime. Cybercrime should focus on three aspects. These are definitely ' Law:

- Legal protection available ;
- Availability of training for prosecutors and jurisdictions ; And
- The nature of these links has merged Indian police with foreign law enforcement agencies so that cooperation on investigations and training can be easily arrived at.

Cybercrime does not recognize national borders. To test this danger, more than 30 countries have made different laws in their law book. This law is just to end cyber crime. Legalizing e-commerce is part of the law. This is definitely, definitely documents with government agencies to facilitate electronic filing. The Indian Penal

Code has been drafted so well that the crimes listed in the IT Act cannot be resolved yet, unless we are sure that the details of cyber crime are being discussed in detail. The IT Act needs to be implemented again. We also need to see if we need to apply multiple laws. The extent and nature of cyber crime in our country must demand different laws. In addition to personal digital initiatives, the Central Bureau of Investigation (CBI), ED, Directorate of Revenue Intelligence Directorate and the Income Tax Investigation cart Z -government law enforcement resources, including the valuable input, can provide. Must also draw from international experience. No systematic effort has been made so far as to train prosecutors and judges, although there is evidence of their interest to be knowledgeable. Presumably, the initiative could come from law enforcement agencies that have quality trainers and training institutes. It is not difficult to draft special capsules for this purpose. Being polished in cyberspace was a challenging task.

In short, the Cyberspace is a global event which cannot be dealt with easily, Information Technology Act, 2000 is a great step and the right step at the right time initiative in the national laws of the country, there is no doubt at all that is necessary. Working in media control efforts and accessible, he has such a profound impact on human life that it is beyond contemporary philosophical understanding. It is probably several years later, that the scope and scale effects can be estimated. No system of investigation and without clearly defined rights and obligations, and the forum where it effectively can be applied in the validity of the run with the permission can not be given could, therefore, this law very soon did not come, and it is hoped that legislation at the national level the legal control system paved the way for Will do



Chapter-12
CASE STUDY-CASES

CASE STUDY

INDIA'S FIRST ATM CARD FRAUD

The Chennai City Police have busted an international gang involved in cyber crime, with the arrest of Deepak PremManwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt. The dimensions of the city cops' achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States. At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai.

While investigating Manwani's case During the investigation, police around the world in a cyber crime involving corers the men were attacked. Manwani has an MBA drop-out from Pune College and for some time worked as a marketing executive at a Chennai based firm.

Interestingly, his daring crime career began in an internet café. One day while browsing the net, he was attracted to a site, which offered to help him break the ATM. His contacts, Europe, sitting somewhere, the United States, some of the bank card and \$ 5 dollar credit card number had agreed to. The site also provided magnetic code for those cards, but was charged \$ 200 per code. The site's operators created an interesting idea to get the card user's personal identification number (PIN). He was asked to create a new site that is similar to reputed telecom companies.

That company has several million customers. The main return of \$ 11.75 per fake site visitor, told site promoters, is misplaced. Suppose in many cases this was a real offer by the telecom company

Members login to the site to receive some of that money back, but participate in the process with their PIN.

The team began their systematic robbery with all the data needed to hack the bank's ATMs. Apparently, Manwani and several others had an agreement with the gang behind the site, and could buy any amount of data, or simply snatch - on a shared basis, on certain terms.

Meanwhile, the 30 Success Plastic Cards by Manwani, are essential information that will make a hole in the Attims. He was so entertained that he was able to sell some of these cards to his contacts in Mumbai. Police are also keeping an eye on those people.

After receiving widespread complaints from bill credit card users and banks in the United States, the FBI has launched an investigation into the case and informed the CBI in New Delhi that the international gang had made some connections in India as well.

Manwani has been granted bail after being interrogated by the CBI. But city police believe this is the beginning of a major cyber crime. Number of years. The fourth is mandatory for all electronic merchants to monitor and these are usually kept for a record of the transaction during a specified period. Fifth definitely, definitely law enforcement agencies are trained to deal with the crime of training last but not least, international cyber and international co-operation and harmony with the laws of terrestrial internationally can help to tackle this crime.

Case 1: First Conviction in India

A complaint was filed in by Sony India Private Ltd, a complaint was filed, which Sony - shaped on the website and manage it. The website enables NRIs to ship Sony products to their friends and relatives in India after paying online. The company undertakes to distribute the product to its own recipient. In May 2002 In, Barbara Kanpand identity on the log, a Sony color television sets and ordered a Bangladeshi television. The woman gave a credit card number for payment and requested that the goods be distributed to Arif Azim at Noda. Payment was duly approved by the credit card agency and the transaction was processed. To comply with Didilijens and relevant methods of testing, the company has distributed Arif Azim items. During the delivery, the company took digital photos, showing Thedelvri was producing by Arif Azim. The transaction closes at the same time, but after a month and a half of credit Cardajensi, the company notified it was an unauthorized transaction, because the owner there was rejected. The company filed a complaint with the Central Bureau of Investigation for fraudulent online IPC sections 418, 419 and 420 of the IPC.

Arif Azim was arrested after investigating the case. The investigation found that Arif Azim Noida, a non-US citizen, misused the credit card number while working at the call center.

Company Site

CBI recovers colored television and cordless head phones. The accused has confessed his crime, and Mr. Gulshan Kumar Metropolitan Magistrate, New Delhi Arif Azim Court of the Indian Penal Code 418, 419 and 420 in section convicted - this is the first cyber crime she was convicted.

The court, however, felt that, since the alleged 24 -year-old was a young boy, and he was guilty before, there was the need for a moderate approach. The court sent the accused to probation for one year.

Case 2: The first juvenile accused in a cyber crime case.

2001 April, the New One Person

Delhi complained to the crime branch regarding the website. Amazing.com, he claimed, carried vulgar remarks about his daughter and a few of her classmates. During the inquiry, print-outs of the site were taken and proceedings initiated.

After the investigation, an 11th grade student and a classmate of the student were arrested. In November the Juvenile Board obscene comments about his classmate to create a website allegedly refused to take the child away. Defendant's advice would leave his client in a stable condition that he was not in a stable state. Look for discharge from the Advocate said, for almost two years the case is pending. Charged with applying the rule, Metropolitan Magistrate Sntoshswi value of the said 'mental state in which adolescents comes under the law, it will be considered when the final order. "However, the quality of women's oppression Act (Prohibition) Act in the left. The accused Technology under the law, prosecute, and a woman's modesty to decrease intended it. He said, leading the investigation can not be closed, especially when the allegations were made.

Case 3: The first case to be found guilty under the Information Technology Act of India 2000.

A case related to posting obscene, defamatory and bothersome messages about a tribal woman in the Yahoo Message Group. This email was also sent to the victim for information provided to the accused through a false e-mail account opened in the victim's name. Posting messages shocked the woman with the conviction that he was stubborn. February 2004 On the basis of a complaint I went hunting, the accused sent by the police to Mumbai and arrested him in the next few days. The alleged victim was a friend of a known family and was found unworthy of marriage. Although she is married to another man. The marriage ended after the divorce and the accused resumed contact with her. The unwillingness to marry him, harassed through the Internet.

IT Act, 2000, 469 and 509 IPC sheet to U / S 67 of IT Act 2000, to be filed have been Respected Adv. CMM Egmore 18 other witnesses and 34 other documents and materials has been cited. C.C.NO. 4680/2004 in the same file was taken. The state police have examined 12 witnesses and identified the entire document. The defense argued that the abusive mail must have been given to the ex-husband's accuser or the accuser. Further, defense counsel argued that some authentication proof of the Indian Evidence Act, Act get 5 B section under did not last. However, court expert testimony and testimony presented other evidence, including cyber cafe owners, that proved guilt-ridden.

Court to consider the eye because I went by to check carefully, pornographic messages and destroy U Z establish the law was brought before the criminal courts. In this case, Mr. S. kotharamandana, special public prosecutor, by

Government conducted the case.

Respected Mr.Arulraj, Additional Chief Metropolitan Magistrate, Egmore, gave the following decision on 5-11-04 :

"The accused Section 469, 509 IPC and 67 IIT Act, 2000, any offense found guilty and convicted have been charged 469 IPC Under 2 years for labor is a crime Tendergo was sentenced Theoffence U / s 509 IPC has been one year in jail and 500 / - Rs IT Penalty Act 2000 offense U / 67 s to RIfor 2 years and the Rs.4000 / - at the same time sentenced to a fine of words. We have to. "

Case 4: Father and son convicted in IT Act in Kerala.

Additional District and Sessions Court 00 2006, in the Pentecostal church, the priest and his son filed by the state rigorous imprisonment in the first case, the lower court cyber upheld.

On Wednesday, Priest Ezra Balan and his son, Anishbaln, filed an appeal against the order of the Chief Judicial Magistrate.

Additional District Judge TU Matthewuccutti said it was time for the government to investigate the growing trend of cyber crime in the state. Magistrate Court orders two to three years rigorous imprisonment and a fine of Rs upholds. 25,000 under Information Technology (Article IT) Act 67 ; Six-month rigorous imprisonment under section 120 (b) of the Indian Penal Code ; And sentenced to one year rigorous imprisonment and a fine of five thousand rupees. 10,000 under paragraph code 469. IT law enforcement Section of 66 section of this sentence rejected. Cyber case in January - February 2002, the previous and the priest and his son were guilty of the first cyber crime.

Both were found guilty of pastor Abraham and his family morphing, web-hosting and e- mailing nude pictures.

Balan worked with the priest until he came out with him and was later shown the door. Balan Sharon joins the Pentecost church. Afterwards The prosecutor, both Abraham, his son, Valson Abraham and daughter, Morf Captioned fake e-mail ID Starla Luke and e-mail their photos.

Morfd's photo was posted on the Web and the accused, the editor of the magazine looking at a local defender, wrote about this photo of your publication. Walson got the picture on the Internet and asked his father to file a police complaint. In Perumbavavar, a police team raided the house of Balan and his son and collected evidence. The magistrate's decision came after a four-year hearing, for which the court had to buy a computer with an Internet connection and luggage. Police services were protected. Also a computer analyst for complete proof. Nine witnesses, including Internet Service Provider and Bharat Sanchar Nigam Limited, have been produced in court.

Case 5: Renowned Orthopedist from Chennai.

Dr. L. Prakash was convicted in various ways for molesting his patients, performing sexual acts on camera and posting pictures and videos on the Internet. In December, a fifty-year-old doctor who was trapped by the police while acting in a porn film, a young man filed a police complaint. Apparently the doctor had promised the young man that the picture would only be aired in selected circles overseas and in the aftermath of his life, he opened a box of Pandora watching himself in a porn video posted on a Web suburban police investigation. And his younger brother had settled in the United States published nearly a million shots and video footage, which is something very close to the real and maraphedera was collected

It was alleged that he dug a huge amount of money into the porn business, it was said. Fast Track Court Judge, and Radha, who in February 2008, the four were convicted, light 1.27 a fine of Rs one lakh, the main accused in the case, and 2,500. His three colleagues - Saravanan, Vijayan and Asi Ganesha. Each judge said that the severity of the crime committed by the accused is to be given a life sentence for the light, the maximum punishment should be given under the Immoral Trafficking Act. He should not show any deficiency.

Judge irregularities tryaphikim Act, IPC, Arms Act and unsafe represent the female (Prevention) Act, the publisher, among others pretend said.

Case 6.: The juvenile confessed to sending the threatening email.

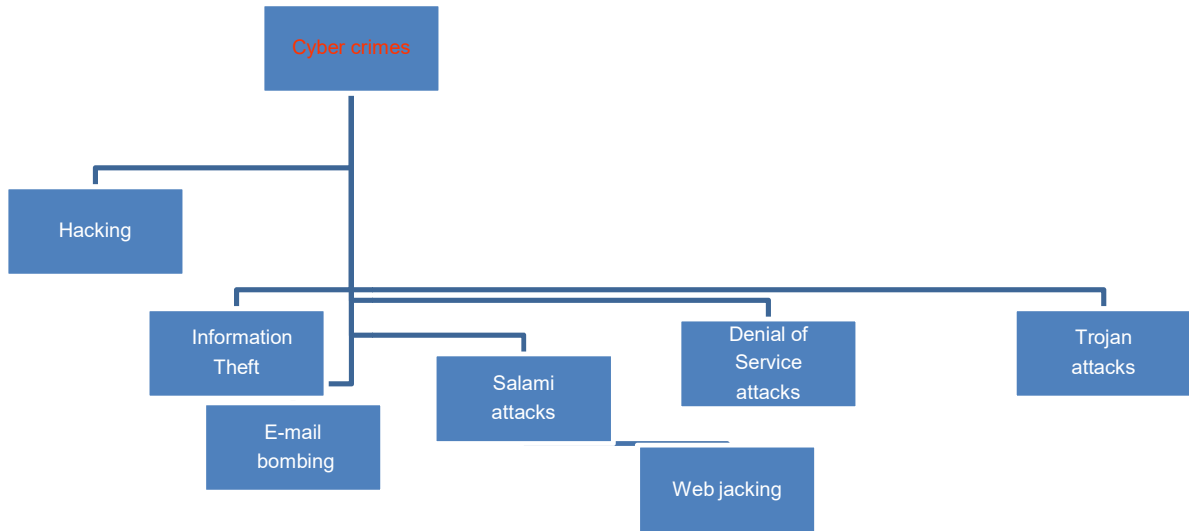
In Ahmedabad a 16-year-old student threatened to blow up, the Corporate Office went to the railway station had got an e-mail message, Mumbai convicted in juvenile court. A private news channel on 18 March 008 in an email that the sender had claimed that Dawood Ibrahim gang, an undefined for a bomb to blow up the train will be removed. A case was registered at Andheri police station under section 6 of the IPC and transferred to the Cyber Crime Investigation Directorate. During the investigation, CCIC discovered the cybercafe from which the email account was created and the threatened email was sent.

The owner of the cafe told police about friends who came that day to run the net. Police called to them and found that the system used for sending EMI was only accessed by one

customer. 22 Mark 08 from, a twelfth-grade science students arrested during the interrogation, said that he mischief, which as "breaking news" on television was fun, we sent you an email.

12. TYPE OF CYBER TERRORISM AND CYBER CRIMES

TYPES OF CYBER CRIMES



CYBER CRIME IS MAINLY AGAINST THREE SECTIONS OF SOCIETY:-



MAJOR CYBER CRIMES

Virus, worm, Trojan or spy-ware infection in the system by phishing Impersonation of companies by email or any other electronic means Spam, unsolicited email messages, rejected services, Companies are trying to overload or overload the website, the network through which it becomes unavailable to the outside world. Unauthorized access to, outside of system resources from unauthorized access,

Destroy / destroy

Organizations destroy or damage systems damage

Extortion

Discount money or other claims based on the threat mand

Fraudulent transactions

Transactions that result in the loss of the Company or its customers

Physical damage

Damage or theft of computer or physical storage media

Unauthorized by Internal

Successful access by insiders to unauthorized data

Internal Miss

Unauthorized use of the interior by conducting infringing security polls

As you can see from the classification, cybercrime can develop from different regions. When we 'Insider' cyber crime considering supporting elements that, The misuse of portable storage, unnecessary software downloads, illegal P- 2, P file sharing, remote access program can be seen as an abuse, Chaotic WiFi access points, rogue modems, download media, personal devices, unauthorized blogging, personal instant messaging accounts, message board posting, private email accounts, non-network web browsing and commercial e-mail abuse.

Although I have covered almost all types of cyber crime examples, I did not include examples of cyber warfare, espionage, and terrorism because I think it is beyond the scope of this paper.

Although if any of your readers are interested, I would be happy to discuss these topics

CLASSIFICATIONS OF CYBERCRIMES: DIFFERENT BASIS

The Internet is gaining momentum and worldwide to make these crimes very easy, efficient, risk-free, cheap and profitable. Incidentally new crimes on the internet or for old crimes or for a crime commission. Broadly stated, '**cyber crime**', **the Commission can be called an act of omission, via the Internet, or associated with, or attached to, directly or indirectly, whether, in any place, which is prohibited by law, financial and / or physical, has been granted**

A) Internet crime: Internet crimes include group crimes that criminalize Internet infrastructure. These are definitely ' Law:

- Hacking
 - (a) Theft of information
 - (b) Theft of passwords
 - (c) Theft of credit cards numbers
 - (d) Launch of malicious programmes
- Espionage
- Spamming

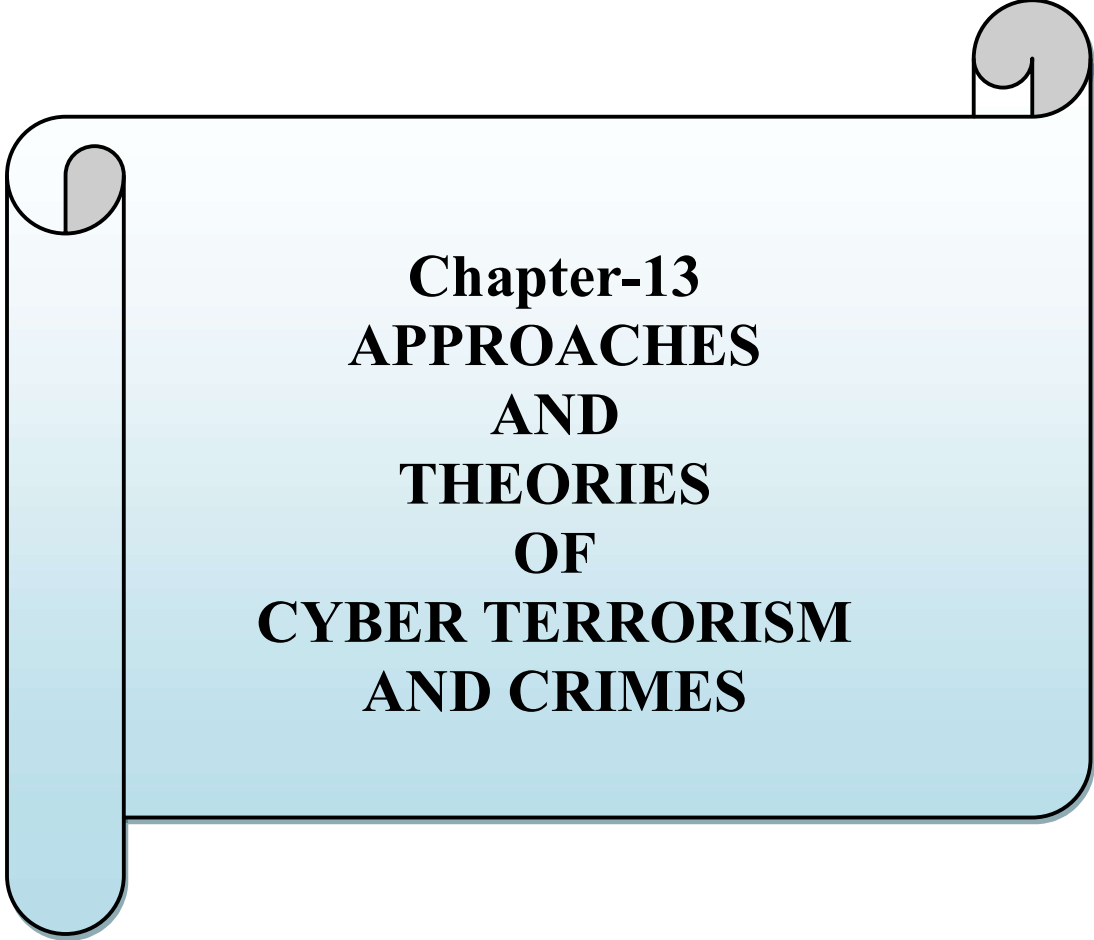
B) Web based crime: Web based crimes have been categorized separately and have been further classified separately and have been further classified into four subcategories.

- (a) Web site related crime
 - Cheating and frauds
 - Insurance frauds
 - Gambling
 - Distribution of pornography
 - Sale of pirated software
- (b) Crimes through e-mail

- Threats
 - Extortion
 - E-mail bombing
 - Defamation
 - Launching of malicious programmes
- (c) Usenet related crime
- Distribution/sale of pornography material
 - Distribution/sale of pirated software
 - Discussion on methods of jacking
 - Sale of stolen credit card numbers
 - Sale of stolen data
- (d) Internet relay chat crime
- Cyber stalking
 - Fraudsters use chat rooms for developing relations with unsuspecting victims
 - Criminals use it for meeting conspirators
 - Hackers use it for discussing their expertise of showing the techniques
 - Pedophiles use chat rooms to allure small children.¹
- Offences against the confidentiality, integrity and availability of computer data and systems
 - (a) Illegal access
 - (b) Illegal interception
 - (c) Data interference
 - (d) System interference
 - (e) Illegal devices
 - Offences related to computer
 - (a) Computer-related forgery
 - (b) Computer-related fraud
 - (c) Computer sabotage
 - (d) Cyber stalking
 - Offences related to contents
 - (a) Offences related to child pornography

¹ Subhas P. Rathore and Bharat B. Das,(2001) “*Cyber Crimes: The emerging trends and Challenges, Souvenir, National Conference on Cyberlaws and Legal Education*”, NALSAR University of Law, at 56-57

- (b) Offences related to infringements of copyright and related rights
- Offences related to crime on web
 - (a) Computer network break-ins
 - (b) Industrial espionage
 - (c) Software piracy
 - (d) Cyber pornography
 - (e) Mail bombings
 - (f) Password sniffers
 - (g) Spoofing



Chapter-13
APPROACHES
AND
THEORIES
OF
CYBER TERRORISM
AND CRIMES

13. APPROACHES AND THEORIES OF CYBER TERRORISM AND CRIMES

Approaches to analyze cyber terrorist communities: Survey and challenges

Cyber-terrorism has become a major threat to world peace and global economic prosperity. Significant increase in cyber-terrorist community ecology of the community's internal confrontation (the internal structure, the executive strategy and management) internal confrontation achieving effective methods, techniques and tools needed to lead to that. Strategy). In the literature, cybercriminals have done much research to identify and analyze terrorist groups. Specifically, social network analytics (SNA) has emerged as an important research area that seeks to analyze cyber terrorist communities. In this study, we study, study, and classify key methods related to cyber-terrorist community analysis. Their properties, strength and discuss. The approach is classified into two main categories, namely, the SNA based approach and the hybrid approach. In addition, we identify areas of interest, more effective ways to help cyber-terrorists develop community analysis and access more research with the purpose of creating functions.

We must be reasonable in discussing the potential dangers, thus this report may occur at any time, without any precautionary measures. The majority of our digital infrastructure is already protected in large quantities, as beggars, and has been expanded by Butler (2004); Current technologies include: firewalls, password protection systems, key encryption (such as 3DES, RSA), stenography, intrusion detection system, secure socket layer (SSL), IPS, access control lists and more. When discussing terrorism activities in general, the responsibility to prevent liability usually depends on governments and national organizations. Cyber-terrorism is led by the goals of US government action, our national security, our intelligence services, the Ministry of Defense, Government Communications Headquarters, Military Intelligence Articles 5 and 6. Addressing this, the British government has categorized cyber-attacks. A threat to national security ("010 of the 015 official policy: Cyber Security", 015). This cyber-terrorism services, Analysis and monitoring of potential threats cover center keeps. Not only is terrorism work, cyber-attacks are not a growing concern, but crime, GCHQ, a

subdivision National Cyber Security Center (Ansis) 2017 is launched. Enasiasasira the sayorana Martin said, the company has already 188 has conducted. NCSC opens three months before high-level cyber-attacks across the country ("Britain to enter a new era of online opportunity", 2017). Organizations like NATO is taking action against the threat of cyber-terrorism, allies on July 01 2016 in a "cyber- defense commitment" ("Cyber Defense", 2017), made was. To provide intelligence information, the active response, the government in 2013 in the cyber security information sharing partnership (Siwaispi), and the introduction, in which the private sector and the public sector ("a high level of communication between security professionals to 2010, from 2015 the government's policy: Cyber Security", 2015). In addition, the National Center for Infrastructure Security also addresses your work with organizations in the UK that have gone through paragraph 3.4 discussing digital infrastructure support. Its mission is to improve communication between both government agencies and non-governmental organizations, thereby strengthening our network against cyber-attacks. Cabinet Office of the UK Cyber Security Strategy Annual Report, details of their actions and their expenditures by the cyber security government against cyber attacks, Figure 2 (See Cyber Security and Information Assurance, 2016 Office).

Preventions and mitigations of future attacks

The vulnerability of software and new technologies has proven in recent years that security is often not a priority during its development. Internet of Things (IOTO) a device that example, which is why this issue has been widely discussed over the years. Correspondent Lucian Constantin (015) cited that: "The Application Protection Agency bherakodera a party in December acquired the six up-to-date devices of this research is carried out, and five have serious problems are expected," MIT Sloan Management Review reported that companies dangerously Not related to the security of these national devices (Olemanu, 2017). Going forward, it is worth noting that a large amount of our cyberspace security is built on security and companies are not fully aware of the risks to the technologies they are using. Thus, cyber will be implemented as an integral part of security software and equipment development, a valuable method of preventing an already advanced terrorist threat. While our government has a variety of barriers to cyber-attacks, often the chances of being caught are criminals in mind, it can be said that this is not a concern for terrorists and terrorist organizations.

Consequently, when discussing cyber-crime prevention against cyber-crime, see the approach because of the attacker's point it should be considered separately. Often, terrorists have no law to follow and are not concerned about the consequences of being identified before or during an attack. Let's assume it is important for a preliminary inspection, to protect the identity of the attacker and the fastest of actions. Identifying access to the most active areas of research in cyber terrorism in the last 20 years (Cyber Institute, 2003) 2003 In our system and physically secure barriers, it is necessary to apply the right approach to detect attacks.

Many of these techniques, as discussed earlier, this week went on, encryption, including the choice. Password, can be viewed as one of the oldest methods of intrusion detection. As these methods are commonly used, as well as weaknesses became common. It is noteworthy that, attacks to mitigation, the attack in order to be effective as far as possible during the ongoing need to develop new penetration detection system. Not only does this improve mitigation, but it also allows a finite system to do potential damage to a limit and thus can cause irreparable damage before protecting valuable property. Additionally, responses to cyber attacks can be improved by focusing more on data protection during attacks. As discussed by many security professionals around the world, data breaches have not been backed up recently, so it's important to always have an updated version of the system or database. Limiting the amount of cyber-attack damage is an essential part of incident management.

It is an early stage of recovering and reacting to an activity of cyber terrorism and enables future security. Going forward, one of the biggest discoveries in publishing this report is that cyber terrorism should always be considered an imminent threat. Until the terrorists take action, they are hiding in our society. When we discuss terrorism, it is responsible for tourists in the physical and digital space. Each of them causing harm by terrorists who want to publish a particular inspiration, section 3, is shown. It is considered to be always in search of potential attacks must, as 3. 4 section discusses the art of the possible threat to the control system. Anti-terrorist methods It is important to use this demonstration to their advantage. Understanding where cyber terrorism can happen and developing an active response to potential threats is important. We have learned that cyber-attacks can be carried out at any time or place, identifying and finding ways to develop terrorism carries an important importance in every justice. The choice of monitor, cyber crime law or hard to develop the technology for the detection system

may include. Cyber-terrorism prevention, while checking Article 4, is one of the biggest concerns for the government, as it is clearly being developed further, we have given the following recommendations to help respond to cyber threats: 1. ' Fire enforcement ' processes, effectively checking security measures, mitigating an attack and responding to an incident. This is especially emphasized for industrial control systems. 2. Understand the importance of developing and developing detection technologies, with a particular focus on collecting preliminary reconnaissance information on cyber threat intelligence. Methods that can be considered or expanded include data mining and machine learning to predict potential attacks. 3. Providing greater education to both private and public sector companies that are developing technologies that may be threatened by cyber terrorism. New system developers must ensure the security sequence is at the forefront during construction to limit the amount of focus.

Cyber terrorism and Security Measures

It "further opportunities to expand our cyber-terrorism A. Z padanasila be", a term widely accepted definition, the following two relevant questions to consider:

What do terrorists want to do in cyberspace ?

How do we try to counter this national activity ?

To address these key questions, we first need to know our basic "who" and "what": who is "terrorist" ? What is " cyberspace" ?

Terrorists people, who as a member of an organization or an option (possibly in collaboration with the national government) is to be played with, which is trying to deliberately increase or mass casualties against the civilian population may look expensive. At a minimum, these laws are intended to intimidate these populations and attract national or international attention.

Cyberspace is definitely, definitely sets the computer-communication networks. It is a leading technology-enabled media critical processes and structures that route, commodity prices and the control and management system that provides a portion.

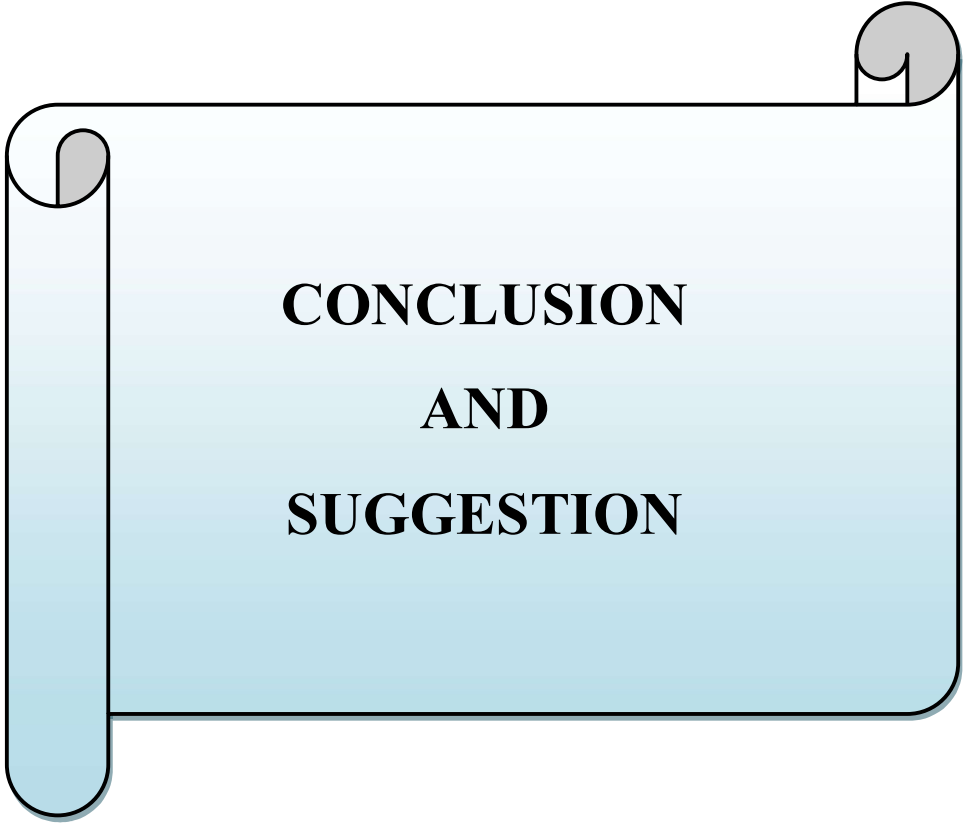
Cyberspace is the single largest component of the Internet, with over 200 billion users in many countries and nearly 1 presence. For the most part, national and

international telecommunications infrastructure is built, including most public phone systems and wireless, landline and satellite communications. Outside the Internet, these telecommunications rely heavily on infrastructure computing technology. So, by our definition, they are part of cyberspace.

Other critical infrastructure in the United States, and increasingly elsewhere in the world, depends on direct control and computer communication. These include removal, banking and financing, energy distribution, emergency preparedness and response, and major public health.

Digital control and monitoring control and data acquisition systems (DC/SCADA) definitely, definitely computer-communication networks, which are used by the various, proposed quote: "**Cyber terrorism and Security Measures.**" National Academy of Sciences. 2007 Science and Technology Counter Terrorism: Proceedings of an Indo-US Workshop. Washington

Manage sensitive processes and physical functions for infrastructure and industry. DC / SCADA systems are commonly used to transmit data and control instructions over the Internet, rather than previously used dedicated networks. They should pay special attention to terrorism.



**CONCLUSION
AND
SUGGESTION**

14. CONCLUSION AND SUGGESTION

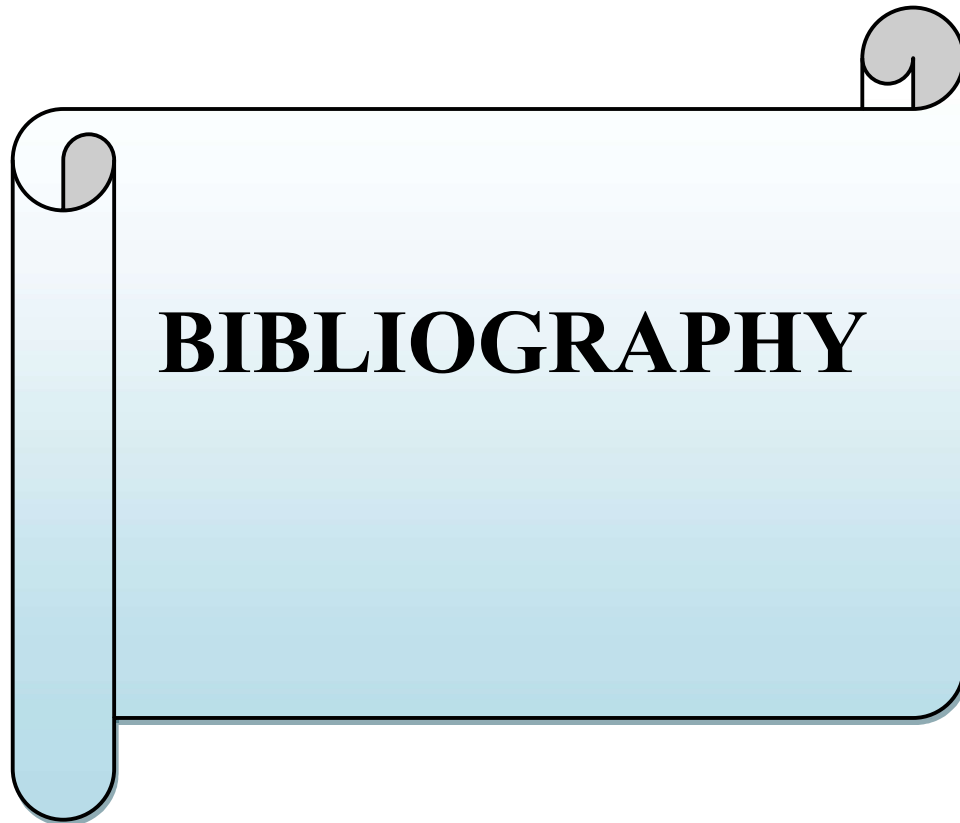
Cybercrime is no longer a illusion in India. If computer users, both public and private, are not prepared for this challenge, the situation may be over. The temptation to attack the police, especially the computer system, is as great as a crime. Cybercrime should focus on three aspects. These are definitely ' Law:

- Legal protection available ;
- Availability of training for prosecutors and jurisdictions ; And
- The nature of these links has merged Indian police with foreign law enforcement agencies so that cooperation on investigations and training can be easily arrived at.

Cybercrime does not recognize national borders. To test this danger, more than 30 countries have made different laws in their law book. This law is just to end cyber crime. Legalizing e-commerce is part of the law. This is definitely, definitely documents with government agencies to facilitate electronic filing. The Indian Penal Code has been drafted so well that the crimes listed in the IT Act cannot be resolved yet, unless we are sure that the details of cyber crime are being discussed in detail. The IT Act needs to be implemented again. We also need to see if we need to apply multiple laws. The extent and nature of cyber crime in our country must demand different laws. In addition to personal digital initiatives, the Central Bureau of Investigation (CBI), ED, Directorate of Revenue Intelligence Directorate and the Income Tax Investigation cart Z -government law enforcement agencies, including the valuable input, can provide. Must also draw from international experience. No systematic effort has been made so far as to train prosecutors and judges, although there is evidence of their interest to be knowledgeable. Presumably, the initiative could come from law enforcement agencies that have quality trainers and training institutes. It is not difficult to draft special capsules for this purpose. Being polished in cyberspace was a challenging task.

In short, the Cyberspace is a global event which can not be dealt with easily, Information Technology Act, 2000 is a great step and the right step at the right time initiative in the national laws of the country, there is no doubt at all that is necessary. Working in media control efforts and accessible, he has such a profound impact on human life that it is beyond contemporary philosophical understanding. It is probably several years later, that the scope and scale effects can be estimated. No system

of investigation and without clearly defined rights and obligations, and the forum where it effectively can be applied in the validity of the run with the permission can not be given could, therefore, this law very soon did not come, and it is hoped that legislation at the national level the legal control system paved the way for Will do



BIBLIOGRAPHY

BIBLIOGRAPHY

BOOKS

- [1.] Astt Narayan - Thakur LK, 'Internet Marketing E-Commerce and Cyber Laws' Authors Press, Delhi, 2000.
- [2.] Bama, Yogesh, 'Criminal Activities In Cyberworld.' Dominant Pubhshers and Distributei-s, New Delhi, 2005.
- [3.] Barua, Yogesh and Dayal Denzyl P., 'Cyber Crimes - Notorious Aspects of the Humans and the Net.' Dominant Publishers and Distributers, New Delhi, 2001.
- [4.] Chopra Deepti and Keith Merrill, 'Cyber Cops, Cyber Criminals and the Internet: I.K. International Vwt. Ltd., New Delhi, 2002.
- [5.] Reed Chris & Angel John, 'Computer Crime & Computer Law.', 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.' ed-2008, Kama! Law House, Kolkata, 2009.
- [9.] Dr. Lakshamanan A.R., 'The Judges Speaks.', 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.] Talat Fatima, 'Cyber Crimes', Eastern Book Company, Lucknow, 2011.
- [15.] Fumell, Steven, 'Hackers, viruses and malicious software: Handbook of Internet Crime.', 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, Allahabad Law Agency, Faridabad, 2008.
- [20.] Jain, N.C., 'The War Against Cyber Crime.' ed.-T', Allahabad Law Agency, Faridabad, 2008.
- [21.] Kamath Nadan, 'Law relating to Computes, Internet and E-commerce.' Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2008.
- [22.] Kumar, Akshay, 'Information Technology and Info Guide.' Authors Press, Delhi, 2000.
- [23.] Kumar, Krishna, 'Cyber Laws-Intellectual Property and E-commerce security.' Dominant Publishers, New Delhi, 2001.
- [24.] Majid-Yar; ' Cybercrime & Society.' ed-1", SAGE India Publication Pvt. Ltd., New Delhi, 2006.
- [25.] Misra S.N., 'Indian Penal Code.' ed.-18' , Central Law Publication, Allahabad, 2012.
- [26.] Nagpal Rohas, 'Cybercrime and corporate liability.' CCH India, 2008 27. Prasad, R.S., 'Cyber Crime: An Introduction.', The ICAI University Press, Hyderabad, 2004.
- [27.] Ratanlal & Dhirajlal, ' The Indian Penal Code.' Wadhwa & Co. (P) Ltd., Nagpur, 1987.
- [28.] Hiller S., Janine, 'Internet law and policy.' Prentice hall, New and Cohen Ronnie, Jersey, 2002.
- [29.] Sharnia S.R., 'Indian Legislation on Cyber Crime.' Anand Publication Pvt. Ltd., New Delhi.
- [30.] Sharma Vakul, 'Information Technology law and Practice: Cyber Law & E. Commerce.' Universal Law Publishing Co. Pvt. Ltd. Delhi, 2004.
- [31.] Sir Stephen James, 'History of the Criminal Law of England.' Vol. II, Macmillan & Co., 1883.
- [32.] Smith I.C, Smith and Hogan, 'Criminal Law.', Oxford University Press, London, 2002.
- [33.] Smith, Graham J.H, 'Internet and Regulation.' Sweet & Maxwell, London, 2002.
- [34.] Srivastava, V.P., 'An Introduction to Cyber Crime Investigation.' Indian Publishers Distributors, Delhi.
- [35.] Suri R.K., Diwan P., Kapoor S., 'Information Technology Laws.' Bharat Publishing House, New Delhi, 2000.

- [36.] Verma, S.K., & Mittal, 'Legal Dimensions of Cyberspace.' ILI Publisher, Delhi, 2004.
- [37.] Vishwanathan, Suresh T, 'The Indian cyber law with cyber glossary.' Bharat Law House, New Delhi, 2000.

ARTICLES

- ❖ Benjamin R. Jones, 'Comment virtual Neighbourhood watch: open source software & community policing against Cyber crime.' The Journal of Criminal Law & Criminology. Vol.97, No. 2, winter 2007.
- ❖ Chinchure Anant D., 'Global Response to Secure Cyberspace: A Comparative Analysis of National Strategy of USA and India.' Karnataka Law Journal. Vol. 5, 2010.
- ❖ Chinchure Anant D., 'Cyber (Computer) Crimes- A Conceptual Analysis.' Criminal Law Journal. Nov. 2010.
- ❖ Gupta Aman Kumar, 'Cyber Crime and Jurisdictional problem.' CBI Bulletin. June-December 2006.
- ❖ Dr Verma Anita, 'Cyber Pornography.' Army Institute of Law Journal Vol.- 1,2007.
- ❖ Dr. G.I.S. Sandhu, 'Cyber Crimes and IT Act- Penology and Jurisdictional Issues.' Army Institute of Law. Vol. I, 2007.
- ❖ Dr. Karkara Gurbax Singh & Dr. Shanna S.K., 'Law of Cyber Crime in India.' Journal of The Legal Studies. Vol. 29, 1998-1999.
- ❖ Dr. Ponnaian M., 'Cyber Crimes, Modem Crimes and Human Rights.' The PRP Journal of Human Rights. July-Sept. 2000.

JOURNAL

- ❖ Aligarh Law Journal.
- ❖ Andhra Law Times.
- ❖ Army Institute of Law Journal.
- ❖ Banglore Law Journal.
- ❖ CBI Bulletin.
- ❖ Civil & Militaiy Law Journal.
- ❖ Cochin University Law Review.
- ❖ Criminal Law Journal.

- ❖ Delhi Judicial Academy Journal.
- ❖ Encyclopedia of Criminology.
- ❖ Gujrat Law Herald.
- ❖ Indian Bar Review.
- ❖ Indian Journal of Public Administration.
- ❖ Indian Police Law Journal.
- ❖ Bibliography
- ❖ Information Technology Law Journal.
- ❖ Journal of Indian Law Institute.
- ❖ Journal of Legal Studies.
- ❖ Karnataka Law Journal.
- ❖ Kerla Law Times.
- ❖ Lawyers Collective.
- ❖ Nyay Deep.
- ❖ The Indian Journal of Criminology and Criminalistics.
- ❖ The Journal of Criminal Law & Criminology.
- ❖ The PRP Journal of Human Rights.
- ❖ Indian Evidence Act, 1872.
- ❖ Indian Penal Code, 1860.
- ❖ Information Technology Act, 2000.

NEWSPAPERS & MAGAZINES

- ❖ Hindustan Times
- ❖ The Hindu
- ❖ The Indian Express
- ❖ The Nation
- ❖ The Statesman
- ❖ The Tribune
- ❖ Times of India

WEBLIOGRAPHY

1. <http://www.cyberlaws.net>
2. <http://www.internet.edu>
3. <http://www.networksolution.com>

4. <http://www.cvbercash.com>
5. <http://www.google.co.in>
6. <http://www.merineews.com>
7. <http://www.mit.gov.in>
8. <http://www.indiacoe.nic.in>
9. <http://www.netsafetv-nic.in>
10. <http://www.apiap.org/opinions/legal>
11. <http://www.navi.org/pati/cvberobscentv.html>
12. <http://www.rtrd.nic.in>
13. <http://www.citchr.com>
14. <http://www.legalser\dceindia.com>
15. <http://www.crime-research.org>
16. <http://www.oscsis.org>
17. <http://www.infowar.com>
18. <http://www.terrorism.com>
19. <http://www.cs.georgetown.edu>
20. <http://www.fmdlaw.com>