DISSERTATION TITLE

EFFECTIVENESS OF CYBER LAWS AND REGULATIONS IN INDIA: A CRITICAL STUDY

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

SUBMITTED BY

KAJAL JAISWAL

UNIVERSITY ROLL NO. 1220997018

SCHOOL OF LEGAL STUDIES

UNDER THE GUIDANCE

OF

PROF. DR. SUDHIR AWASTHI

SCHOOL OF LEGAL STUDIES

BBD UNIVERSITY

SESSION 2020-21

CERTIFICATE

This is to certify that the dissertation titled, "Effectiveness of cybercrime laws and regulations in India: A critical study"is the work done by Kajal Jaiswal undermy guidance and supervision for the partial fulfilment of the requirement for the Degree of **Master of Laws**in School of Legal Studies Babu Banarasi Das University, Lucknow, Uttar Pradesh.

I wish her/his success in life.

Date--------------**NAME OF SUPERVISOR**

Place-Lucknow Prof. Dr. Sudhir Awasthi

DECLARATION

Title of Dissertation Effectiveness of cybercrime laws and regulations in India: A critical study

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

Kajal jaiswal

I declare that

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

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

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

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

Date: ……………… **Kajal Jaiswal**

Place- Lucknow University Roll no 1220997018

LL.M. (CSL) (2023-24)

ACKNOWLEDGEMENT

I express my deep sense of gratitude to "Almighty God" who is guiding me in this world with a previous knowledge and general plan and direction. Without his blessings this work could not have been completed. It is my privilege to acknowledge with deep sense of gratitude and devotion, the keen interest and value guidance rendered to me by **Professor (Dr.) Sudhir Awasthi, Professor of Law Dean of School for Legal Studies**. This is because of her great support, guidance and constant encouragement and inspiration that I have been able to complete this work.

I highly value the support and help of the staff associated with Babu Banarasi Das University, library and Pankaj Kumar sir Lucknow, and all other persons who helped me to materialize this work directly or indirectly.

I would also like to extent my gratitude towards the people who are not my family but became my support system in Lucknow Last, but definitely not the least, it is my pious duty to record my heartiest gratitude to my family, and especially my parents who have nourished and nurtured me from very beginning and taught the first lesson of life and had taken all pains to bring me to this stage of presenting this research paper.

DATE **Kajal jaiswal**

Roll no. 1220997018

PLACE: LUCKNOWLL.M. CCL

ABBREVIATION

AC	Appeal Cases
AIR	All India Reporter
All. ER	All England Reporter
All.	Allahabad
App Cases	Appeal Cases
ATM	AutomatedTailor Machine
AVS	Address verification system
B& Ad	Barnwell. and Adolphus. 1830-1834 K.B
BBM	Black Berry Messenger
BES	Black Berry Enterprise Server
Beav.	Beavens'sReports. 1838-1866
Bing.	Bingham Reports. 1822-34
Bom.	Bombay
CBI	Central Bureau ofInvestigation
CJI	Chief Justice of India
Co.	Company
CVV	Card Verification Value
CPC	Civil ProcedureCode. 1908
Cr. P C	Criminal Procedure Code. 1973
Cr. LJ	Criminal Law Journal
I T	InformationTechnology
Ibid.	Ibedum
ICA	Indian Contract Act. 1872
IPC	Indian Penal Code. 1860
J.	Judge
JJ.	Judge
K B	Kings Bench
LR	Law Reports. Exchequer.1865-75
LT	Law Times Reports 1843-

Ltd.	Limited
NI Act	Negotiable Instruments Act. 1881
Pvt.	Private
RBI	Reserve Bank of India
RECLAB	Reportof the Expert Committeeon Legal Aspects of Bank Frauds
SBI	State Bank of India
SC	Supreme Court
SCC	Supreme Court Cases
UK	United Kingdom
UOI	Unionof India
WWW	World Wide Web

TABLE OF CONTENT

Chapter 1

Introduction

The modern thief can steal more by way of a computer than by way of a gun. Tomorrow'sterrorist may be able todomore damages by way of a keyboard than by way of a bomb[1]. The inventionof the computer has opened new avenue for the fraudsters. It is an evil having its origin in the growing dependence oncomputer in modern life. Though there is great talk about the Cyber Crimes there is nothing called Cybercrime. The crime such as frauds. forgeryistraditional. and are covered by the separate statute such as Indian Penal Codeor alike. However, the abuse ofcomputer. and the related electronic media has given birth to a gamut of new type of crimes which has some peculiar features. A simple yet sturdy definitionof these crimes would be "unlawful acts wherein the equipment transforming the data be it a computerormobile is either a toor a target orboth". In India, the Information Technology Act deals by way of the acts wherein the computer is tofor an unlawful act. The kind of activities usually involves a modificationof a conventional crime by using computer. Same examples are financial crimes. child pornography. sale of illegals articles. online gambling. intellectual properties crimes. email spoofing. forgery. cyber defamation. cyber stalking. unauthorized access tocomputersystems ornetworks. email bombing. theft of data contained in electronicform. data diddling. salami attacks. worms/virus attacks etc. The use of Computer's is increasingly spreading and more. and more users are connectingto the internet. The internet is a sourceforalmostanybodyto access. manipulate. and destroyothersinformation. The rapid developmentof the Internet. and computertechnologyglobally has also led to the growthof new formsoftransnational crimes especially those which are internet related. These criminal activities directly relate to the use ofcomputers. specifically illegal trespass into the computer system or database ofanother. manipulationor theft ofstored data. orsabotageof systems. and data. Characteristic feature of these crimes is that these crimes are considered as illegal. unethical orunauthorizedbehaverofpeople relating to the automaticprocessing. and transmissionof data usingComputer Systems. and Networks. These crimes have virtually noboundaries. and may affect any countryacross the globe within a fractionofsecond. Ways of tackling Cyber Crimes throughlegislation may vary fromonecountry to another. especially when Cyber Crimes

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

occurwithin a specific nationaljurisdiction by way of different definition. and socio-politicalenvironment.[2]

Almost every activity that involves people has been affected by information technology.One of the biggest issues with information technology is how antisocial elements abuse it. Computers, computer networks, and other electronic devices offer new, sophisticated. capabilities tocommit customary offences. Consequently, computers and networks may serve. as both criminals' tools and targets. The growth of the computer, computer network, andinformation technology revolution is tied to the birth of this sort of crime related toinformation and communications. The prevalence of cybercrimes and their effects are risingin lockstep with the exponential growth in our reliance on technology.Since their creation, computers have been used in criminal activity.

Every work has two aspects, a positive aspect, and a bad aspect, according to social norms.When it comes to information technology, this rule also holds true. The abuse of technologyhas led to this dependency on information technology, which has significant drawbacks inaddition to its benefits in making life simpler. This outcome is viewed as cybercrime. Therefore, it is necessary to govern human behaviour in cyberspace. No nation can afford tooverlook its destructive effects. However, no significant platform has beendeveloped by all the world's nations. Cybercrime poses a huge danger to civil society sinceit represents a dark period in the progress of the information revolution.

Cybercrimes with high frequency and broad collateral harm include cyber hacking, cyberpornography, cyber defamation, money laundering, and cyber fraud. While a crime done onthe ground has an impact there, a crime committed online may have a more significantimpact.

“No words can better describe the present scenario of technology than the following stated by Cosmosthe villain in the movie “Sneaker”.

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

[2] Anirudh Rastogi. Cyber Laws. lexi Nexi

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, cybercrime, 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.Cyber Crime is the latest type of crime which affects many people. It refersto the criminal activities taking place in computerorcomputernetworks. intentionally access withoutpermission. alters. damages. deletes. and destroys the database available on the computerornetwork... and also includes access withoutpermissionon a database orprogrammeof a computer in order to devise or execute any unlawful scheme orwrongfullycontrolorobtainmoney. propertiesor data. It poses the biggest challenge for the Police. Prosecutors. and legislators. Crimes of this nature is usually indulged in by young teens. recreationalcomputerprogrammers. and persons having vested interest. Cyber-crime in its most practiced form includes offences such as tampering by way of the sourcecodeof a programme. hacking intocomputer systems. publicationofobsceneinformation. and misuse of licenses. and digital signatures. The problem is multifil as it covers the crime related to economy as well as other crimes such as pornography which has its basis in certain moral standards. and uses parameters like indecency. and obscenity. [3]Enormousamountofmoney is earned by the Cybercriminals. either by causing huge damage to the computer systems or by stealing data which is marketable or by way ofsomefoul play through the network. The question here is what constitutes a computer crime[4]. The study further found that close to half of the of Indian Enterprises saw cyber securities as their top issue. rating it above threats from natural disasters. terrorism. and traditional crime combined. by way of the rate of attacks increasing in several organizations. a sizeable chunk of the companies said that the nature ofcyber-attacksconsistedof external threats as well as internal threats. and negligence.

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

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

DEFINITION OF CYBERCRIME

The Indian assembly does not offer the precise definition of Cybercrime in any statute, even the data Technology Act, 2000; that deals with cybercrime does not outline the term of cybercrime but normally the term cybercrime means that any criminal activity that is carried over or with the assistance of net or computers.

Cybercrime has recently become an attractive term for a set of security issues in cyberspace. However, despite 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 cybercrime in the narrow sense, while others prefer broad definitions, including all computer- related crimes. However, most computer crimes are online. Computer prevention and control of various United Nations Manual of crime, cybercrime 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 L996 in, the UK's National Criminal Intelligence Service began studying a computer crime program called trawlers. Computer crime studies, information technology crime and cybercrime 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 acceptin other words, e-processed data to computers and the Internet can be used in the offenses referred to as cybercrime.

Cyber or computer crimes 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.Dr.**. Debarati Halder and Dr. K. Jaishankar**define cybercrimes as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the[1] reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern

telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”

The term 'cybercrime' has not been defined in any Statute or Act. **The Oxford Reference** Online defines 'cybercrime' as crime committed over the Internet. The Encyclopaedia Britannica defines 'cybercrime' as any crime that is committed by means of special knowledge or expert use of computertechnology. So, what exactly is Cyber Crime. Cyber Crime couldreasonably include a wide varietyof criminal offences. and activities. A generalized definitionof cybercrime may be "unlawful acts wherein the computer is either a tool or target orboth".

CBI Manual defines cybercrime as: ~

- (I) Crimes committed by using computers as a means. including conventional crimes.
- (ii) Crimes in which computers are targets.

The Information Technology Act. 2000. does not define the term 'cybercrime’. Cybercrime can generally define as a criminal activity in which Information Technology systems are the means used for the commissionof the crime.

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

1. Any illegal action in which a computer is the tool or objects of the crime i.e., any crime, the means or purpose of which is to influence the function of a computer,

2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

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

The IT Act provides legal recognitionfor transactions carried out by means ofelectronic data interchange. and other means ofelectronic communication. commonly referred to as "electron ecommerce". involving the use of alternatives to paper-based methods of communication and storage ofinformation. The IT Act facilitates electronic filing of documents by way of the Government agencies.

CYBER CRIME. and ITS CATEGORISATION

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

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

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

CYBERCRIME AGAINST PERSONS: ~

The first category of cyber-crimes committed against person include various like transmission of Child-pornography, sexual harassment of any one wraith the use of a computer, such and e-mail spoofing and cyber stalking. Any unwanted contact between two people that directly or indirectly communicates a heart or place the victim in fear can be considered stalking. The Trafficking, distribution, posing and dissemination of absence material including pornography, indecent exposure and child pornography constitutes one of the most important cybercrimes know today. The potential harm of such a crime to humanity can hardly be over stated[5]

Cybercrimes committed against persons include crimes like transmissionof childpornography. harassment of any one by way of the use of a computer such as e-mail. The trafficking. distribution. posting. and dissemination of obscene material include pornography. and indecent exposure.constitutesoneof the most important Cybercrimes known today. The potential harm of such a crime to humanities can hardly be amplified. This is one Cybercrime

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

which threatens to undermine the growthof the younger generation as also leave irreparable scar. and injury onthe younger generation. if not controlled. Cyber-harassment is the distinct cybercrime. Various kinds of harassment can dooccur in cyberspace. orusing cyberspace. Harassment can be sexual. racial. religious orothers. Person perpetuating such harassment is alsoguiltiestof cybercrime. Cyber-harassment as a crime alsobrings us to another related area of violation of privacy of citizen. Violation of privacy ofonline citizen is a Cybercrime of a grave nature. Noone likes any other person invading the invaluable. and extremely touchy area of his/her privacy which the medium of internet grants to the citizen.

CYBERCRIME AGAINST PROPERTY: ~

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

CYBERCRIMES AGAINST THE GOVERNMENT: ~

The third category of Cybercrime relate to Cybercrime against Government. Cyberterrorism is one distinct kind of crime in this category. The growthof internet has shown that the medium of Cyberspace is being used by individual. and group to threaten the international government as also to terrorise the citizen of a country. This crime manifests' itself into terrorism when an individual "cracks" into a government or military maintained websites. It was said that internet was becoming a boon for the terrorist organisation. Cracking is amongst the gravest Cybercrimes known. It is dreadful feeling to know that a stranger has broken into your computer system without knowledge. and consent. and has tempered by way of precious confidential data. and information. Coupled by way of this the actually is that nocomputer system in the world is cracking proof. It is unanimously agreed that any. and every system in the world can be cracked. The recent denial of service written as DOS attack seen over the popular commercial sites like eBay. flipkart. amazon. Myntra. and others are a new category of Cybercrime which are slowly emerging as being extremely dangerous.

Cyber Crime and Organized Crime

The internet revolution has transformed the society in general and the commercial world in particular. While commercial dealing is rampant on the internet due to its reach worldwide in low cost. So organized crime also found the new opportunities and benefits on internet that are very useful for furthering the criminal activities organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. Some traditional criminal groups are seeking the co-operation of criminals with the necessary technical skills, newer types of criminal networks operating in the area of e-crime have already Emerged[6]

Statement of Problem

With the advancement of this technology, theproblemaroseregardingtherewrongful use. Information technology has made life easier; it has also made crime easierthan in the past. Information technology eliminates the need for actual physical contactto commit a crime. Cybercrime may be committed anywhere from any place throughthe computer and internet. The incident of computer crimes has dramatically increased Cybercrime is different from conventional crime related to person and property,as it requires some virtual medium. It has virtually no boundaries, due to the vastpenetration of the internet across the globe. This feature affects every country;moreover, transnational nature makes it more challenging for law enforcement agencies.

to investigate these cybercrimes. "The most important characteristic of the cyber worldis the lack of distance and borders in it. The major advancement in technology isbringing people together worldwide. In the Information superhighway calledcyberspace, a person in the next room and a person in the farthest country are equal interms of distance and the technology brings together those seeking to engage in illicitactivities and thus assists in the construction of criminal enterprises. For even arelatively minor crime committed in one of the Indian villages through computernetworks, the investigation might extend to the whole world"in the last few years and law enforcement agencies also find it difficult to tackle theproblem. Cybercrime has generated manifold challenges for law enforcing agencies concerning the investigation and law enforcement because they are prepared fortraditional crime, and they

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

are not properly trained and equipped for dealing with such cases.The widespread use of Information Technology has also given scope forcybercrime and other forms of unauthorized access to computers and data. Theprotection of the integrity of all types of data in electronic form, computers, andcomputer systems, is crucial to the protection of the privacy of any person and thesecurity of business concerns, financial institutions, and governmental agencies.

Thelaws governing the physical world are, however, incompetent at governing criminalactivities in cyberspace where the subject matter often is an intangible object such asone's email, social networking sites accounts, website, virtual currency, or personalinformation. The regulation of cyberspace, hence, requires specialized laws.Information technology has also given birth to a new variety of criminalactivities. Criminals use this technology to commit both traditional crimes (cheating. embezzlement, theft, etc.) and new-age crimes, which were not known by traditional laws (cyber hacking, denial of service attacks, and data theft, etc.). For example, a website having limitations of viewers or requests (for information) at a given point of time. Cybercriminal can prevent the website from functioning by overloading it with requests that are known as denial-of-service attack. Such attacks can cause huge losses to an online business, but there would be no clear remedy under ordinary law.

The involvement of the computer is not limited to the basic cybercrimes only, but it is also extensively used in a wide range of other crimes such as drug trafficking, frauds, forgeries,

extortion, gambling, kidnappings, organized crimes, software piracy, white-collar crimes, etc. Nevertheless, another problem for legislation is the vagueness of some of the crimes. Many times, criminals are not even aware that they are committing a crime.

Email spamming, identity theft with no financial implications are examples of such kind ofbehaviour.

Objectives

1. To examine the legal framework for cybercrime India, including relevant law regulations, and guideline
2. To identify the challenges and limitations of the existing legal framework, in addressing cybercrime in India.
3. To evaluate the effectiveness of law enforcement agencies in investigating and prosecuting cybercrime cases.
4. To analyse the impact of cybercrime on Indian society and the economy.
5. To propose recommendations for improving the legal firework and law enforcement efforts to combat cybercrime in India.

Hypothesis

Whether"India's current legal framework for cybercrime is inadequate in addressing the complex and rapidly evolving nature of cybercrime, and requires reforms to ensure effective prevention, investigation, and prosecution of cybercrime".

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

It is easy to commit and difficult to prevent.

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

ii) Cybercrime 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 cybercrime 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.

Research Methodology

The present study mainly doctrinal, descriptive, and analytical study.

a. Primary Source

b. Secondary Source

In the present research, the researcher has used primary as well as secondary sources of data collection. Researcher has collected data through Textbooks, Articles, Reports, ReferenceBooks, and Official websites of various departments such as Department of Information Technology, Central Bureau of Investigation, have also been helpful. The nature of the study required a heavy reliance on internet sources.

Literature Review

Chandra deep Singh Samar in his book "Cybercrimes with special reference to the information technology Act, 2008"

Discussed historical perspective, origin, and growth of cybercrimes, elaborated peculiar feature of cybercrime along with mode and manner of committing various types of cybercrimes. Further, it has also discussed terms of verification and requirement of guilty mind in the cybercrimes, especially offences mentioned in the IT Act, 2000. The book has given outlining of various efforts to combat cybercrime at the international level.

Dr M. Dasgupta has given emphasis to major cybercrime in his book "Cyber Crimein India: A Comparative Study" and discussed the nature and element of cybercrime, criminal liabilities theories of criminal behaviour in cyberspace and cybercrime under the IT Act, 2000. He has also discussed the history and evolution of cybercrime, major cybercrimes witnessed nowadays such as cyber hacking, cyber fraud, cyber pornography, and cyber terrorism etc. Itdeals with the difference between national and international perspectives pertaining to cybercrime.

Cyber- crime orcomputer crime is considered to be any crime that uses a computer. and a computer network (Matthews. 2010). A basic definition describes cybercrime as a crime where computers have the possibilities of playing an important part (Thomas. and Loader. 2000). Themain factor in cyber-crime increase is the Internet. By use of Internet. cybercriminals often appeal to images. codes orelectronic communication in order to run malicious activities. Amongthe most important types ofInternetscrimes, we can mention: ~ identities theft. financial theftespionage. pornography. or copyright infringement. The cyber-crimes can be divided into twocategories: ~ the crimes where a computer network attacks other computersnetworks – e.g., acode or a virus used to disable a system. and. the second category. crimes where a computernetwork attacks a target population – e.g., identities theft. fraud. intrusions (Sveinsson. 2011).Issues revolving around cyber-crime have become more. and more complex. Computer criminal activities have grown in importance. and institutions are more interested than ever in putting amend to these attacks. Progressions have been made in the developmentof new malwaresoftware. which can easily detect criminal behavior (Balkin et al... 2007). Moreover. high qualitative-virus systems are offered for free now in many countries at every purchase of a computer an operating system.

Justice Jatindra Singh (2012)[7] 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.

R. K, Chaubey (2009)[8]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

[7]Cyber Law Jain Book, New Delhi, 2012.
[8] An Introduction to cyber crime & cyber law. ed-2008, Kamal Law House, Kolkata, 2009

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.

Chris Reed (2000)[9] 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 has 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.

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.

Nandan Keinath (2008)[10]. 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 pomp to the regulation of free speech on the Net and the right to privacy. A new chapter on Cases on Computers, Internet, email etc.

[9] Internet Law Text and Materials. Butterworths, London, 2000

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

Chapter 2

2.1. Legal Farmwork for Cyber Crime in India

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 loopholes. Internet, the facilities, the security risks associated with being connected to a large network aware make. 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.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 cybercrime has started to have a negative impact on economic development opportunities in every country.

A general definition of cyber law states that it is a legal framework that governs all legal issues relating to the internet, computer systems, cyberspace, and information technology. A wide range of subjects are covered under cyberspace law, including contract law, privacy legislation, and intellectual property laws. It oversees electronic commerce as well as the distribution of software, information, and data security. Cyberlaw gives e-documents legal validity.Offence committed, ranging from fines to imprisonment. The Computer Fraud and Abuse Act of 1986 was the first cyber law that was ever to be enacted. It prohibits unauthorized access to computers and the illegal use of digital information.

Internet usage has increased, and so has cybercrimes. There are several stories of cybercrimes in the media today ranging from identity theft, crypto jacking, child pornography, cyber terrorism etc. In cybercrimes, the computer is used either as a tool or a target, or both, to commit unlawful conduct. In our fast-moving digital age, there has been a phenomenal surge in electronic commerce (e-commerce) and online stock trading, leading to more cybercrime. 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 [11]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.

2.3. Types of cyber-crimes the following are types of cyber-crimes:cyber-crimesinvolve a modificationof a conventional crime by using computers.Following is a comprehensive list of the various types of Crimes which have been committed in the recent times.

1. Child pornography or child sexually abusive material (CSAM):

In its simplest sense, child sexual abuse materials (CSAMs) include any material containing sexual images in any form, wherein both the child being exploited and abused may be seen. There is a provision in Section 67(B) of the Information Technology Act which states that the publication or transmission of material depicting children in sexually explicit acts in an electronic form is punishable.Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cybercrime. The Internet is being highly used by its abusers to reach and abuse children p35 sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cybercrime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of paedophiles. The podophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start contacting children on their e-mail addresses.

2. Cyberbullying:

A cyberbully is someone who harasses or bullies' others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted using

[11]https://blog.ipleaders.in/cyber-crime-laws-in-india

digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviours that is intended to scare, anger, or shame those being targeted.

3. Cyberstalking:

Cyberstalking is the act of harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through texts, emails, social media posts, and other forms and is often persistent, methodical, and deliberate. Cyber stalking can be defined as the repeated acts harassment or threatening behaviourof the cyber-criminalon the victim by using the internet services. Stalking may be followed by seriousviolent acts such as physical harm to the victim. and the same has to be treated. and viewed seriously. It all depends on the courseofconductof the stalker. Cyber Stalking is a problem which many people especially young teenage girls complainabout.[12]

2.2. What is cybercrime?

Any criminal activity that involves a computer, networked device, or any other related device can be considered a cybercrime. There are some instances when cybercrimes are carried out with the intention of generating profit for the cybercriminals, whereas other times a cybercrime is carried out directly to damage or disable the computer or device. It is also possible that others use computers or networks to spread malware, illegal information, images, or any other kind of material.

As a result of cybercrime, many types of profit-driven criminal activities can be perpetrated, such as ransomware attacks, email and internet fraud, identity theft, and frauds involving financial accounts, credit cards or any other payment card. The theft and resale of personal and corporate data could be the goal of cybercriminals.

In India, cybercrimes are covered by the Information Technology Act, 2000 and the Indian Penal Code, 1860. It is the Information Technology Act, 2000, which deals with issues related to cybercrimes and electronic commerce. However, in the year 2008, the Act was

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

amended and outlined the definition and punishment of cybercrime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

4. Cyber grooming:

The phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act.

5. Online job fraud:

An online job fraud scheme involves misleading people who require a job by promising them a better job with higher wages while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

6. Online sextortion:

The act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten to get a sexual image, sexual favour, or money from such individuals.

7. Phishing:

In computing. phishing is a formofsocial engineering. characterized by attempts to fraudulently acquire sensitive information. such as passwords. and credit cards. by masquerading as a trustworthypersonor business in an apparently officialelectroniccommunication. such as an email or an instant message[13]. The term phishing arises from the use of increasingly sophisticated lures to a Phish forusers’financial

[13] http: ~//www/trai.gov.in

information. and passwords[14]. The act of sending an email to a user falsely claiming to be an established. and legitimate enterprise in aneffort to scam the user into surrendering private data that will be used for identities theft. The email directs the user to visit a website where they are asked to update personalinformation.such as passwords. and credit card. Socialsecurity'sno... and bank accountno. that the legitimateorganization already has. The website. however, is bogus. and is setup only to steal the user'sinformation. By spamming large group large groupofpeople. the „phisher counted on the emailbeing read by a percentage ofpeoplewho actually had listed credit cards numbers withlegitimacy. Phishing also refers to a brand spoofing or carding. is a variationon phishing. the ideabeing that the bait is thrownout by way of the hope that while most will ignore the bait. some will be temptedinto biting it. by way of the growingno. ofreported phishing incidents. additionalmethodsofprotection are needed. Attempts include legislation. user training. and technical measures. M-o-r-erecent phishing attempts have started to target the customersof banks. and online paymentservices[15]. While the first such example are sent indiscriminately in the hopeof finding acustomerof a given bank or service. recent research has shown that phishers may in principle be able to establish what bank a potential victim has a relationwith. and. then sends an appropriatespoofed email to the victim. In general, such targeted versionsof phishing have been termed as spear phishing[16]. Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web.

8.Vishing:

In vishing, victims' confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call. Callers can often pretend that they are from the government, tax department, police department, or victim's bank.

[14] Tan. Koon. Phishing. and spamming via IMInternet StormCentre. December 5th. 2006

[15] Ollmann. Gunter. THE PHISHING GUIDE: ~ UNDERSTA NDING A ND PREVENTING PHISHING ATTA CKS: ~ Technical Info. 2006

[16] What is Spear Phishing?Microsoft Securities atHome. July 10th 2006

9. Smishing:

As the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website, or downloading malicious software that resides on the victim's computer.

10. Credit card fraud or debit card fraud:

In credit card (or debit card) fraud, unauthorized purchases, or withdrawals from another's card are made to gain access to their funds. When unauthorized purchases or withdrawals of cash are made from a customer's account, they are considered credit/debit card fraud. Fraudulent activity occurs when a criminal gains access to the cardholder's debit/credit number, or personal identification number (PIN). Your information can be obtained by unscrupulous employees or hackers.

11. Impersonation and identity theft:

A person is impersonated or exposed to identity theft when they make fraudulent use of an electronic signature, a password, or any other unique identifier on another person's behalf.

12. Hacking

Hacking means unauthorized access to a computer system[17].Hacking requires unauthorized device access and the modification of the device so as to enable continued access, as well as a change of the target machine set-up, purpose, or service, without awareness or consent of the system owners. Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a

[17] Section 66 of data Technology Act. 2000

computer resource or diminishes its value or utility or affects it injuriously by means is said to commit hacking.

Vinod Kaushik and Or's. V/s Madhvika Joshi and Others[18]

The main issue in this case is whether accessing a husband's and father-in-law's email account without their permission amounts to 'unauthorized access'. In this case, the first respondent had accessed the email account of her husband and father-in-law, in order to acquire evidence in a Dowry harassment case. The Adjudicating Officer held that accessing an e-mail account without authorization amounts to a contravention of section 43 of the information Technology Act 2000. There was no compensation awarded to the complainant as the respondent had only submitted the information so obtained to the police and the court. The Adjudicating Officer, however ordered the first respondent to pay a fine of Rs. 100, as she was held to be in contravention of Section 66-C (identity theft and dishonest use of the password of any other person) of the IT Act 2000.

13. Virus dissemination

This illegal activity type requires either direct or non-authorized entry to the operating system by installing new applications that are classified as ss bugs, worms, or logic bombs. The unauthorized removal or deletion of machine data or the Internet function, which prohibits regular device functions, is obviously an illegal offence and is generally referred to as computer sabotage.

14. Email bombing

Sending massive amounts of mail to a victim, which could be an individual, an organisation, or even mail servers, causing the system or network to fail.It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g., if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends. E-mail spamming is a variant

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

ofbombing; it refers to sending email to hundreds orthousandsof users. E- mail spamming can be made worseof the recipients reply to the email. causing all the original addresses to receive the reply. [19]

15. Virus / worms attacks

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

16. Trojan attacks

A Trojan is an unlawful programme that operates from within by pretending to be an approved software and therefore disguising its true intentions.A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

17. Cybersquatting

Cyber-squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different). p38 A trademark owner can prevail in a cyber-squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiffs' distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out of pocket expenses.Obtaining a domain name in order to collect payment from the owner of a trademark (including a business name, trade name, or brand name) is known

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

as cybersquatting, and it can also include typo squatting (where one letter is different). A trademark owner can win a cybersquatting case by proving that the defendant registered a domain name containing the plaintiff's distinctive trademark in bad faith and with the purpose to profit.

18. Cyber Defamation

Cyber defamation is defined as any negativestatement intended to harm a person's company or reputation. Libel or slander Can be used to defame someone. When defamation is carried out via computers and/or the Internet, it is known as cyber defamation.Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

19. Breach of confidentiality and privacy

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

K.L.D Nagasree v, Government of India, represented by its Secretary, Ministry of Home Affairs and Or’s[20]

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

The respondent gave the order to intercept messages from the mobile phone of the petitioner. The Court examined the procedural safeguards that are in place in case with respect to an

[20] AIR2007AP102, (Aiidhra Pradesh High Court).

order of interception of communication. These safeguards are enshrined in Rule 419-A of the Indian Telegraph Rules 1951 pursuant to the guidelines laid down by the Supreme Court in the case

20. HACKING

Hacking means unauthorized access to a computer system[21]. It is the mostcommon type of Cyber Crime being committedacross the world. The word “hacking” has been defined in section 66 of the Information Technology Act. 2000 as follows. “Whoever by way of the intent to cause orknowingly that he is likely to cause wrongfullessor damage to the public or any person. destroysor deletes or alters any data residing in a computerresourceor diminishes its value or utilities or affects it injuriously by any means commits hacking” Punishment for hacking under the above-mentionedsection is imprisonmentfor three years or fine which may extend up to two lakh rupees orboth.

21. SALAMI ATTACKS

A salami attack is a series ofminor data-securities attack that together result in a larger attack. For example. a fraud activity in a bank. where an employee steals a small amountof funds from several accounts. can be considered a Salami Attack[22]. Crimes involving salami attacks are typically difficult to detect. and trace. These attacks are used forcommissionof financial crimes. The key here is to make the alterationso insignificant that in a single case it wouldtocompletelyunnoticed e g a bank employee inserts a programinto the bank servers that deducts a small amountofmoney (say Rs. 5 a month) from the accountof every customeraccountholder will probablynotice this unauthorized debit. but the bank employee will make a sizable amount each month[23].

22. SALE OF ILLEGAL ARTICLES: ~

This would include sale ofnarcotics. weapons. and wildlife etc. by posting data on websites. bulletin boardsor simply by using e-mail communications.

[21] Section 66 of data Technology Act. 2000

[22] Aderucci. Scott. Salami Fraud. www.all.net/CID/attack/papers/Salami .html

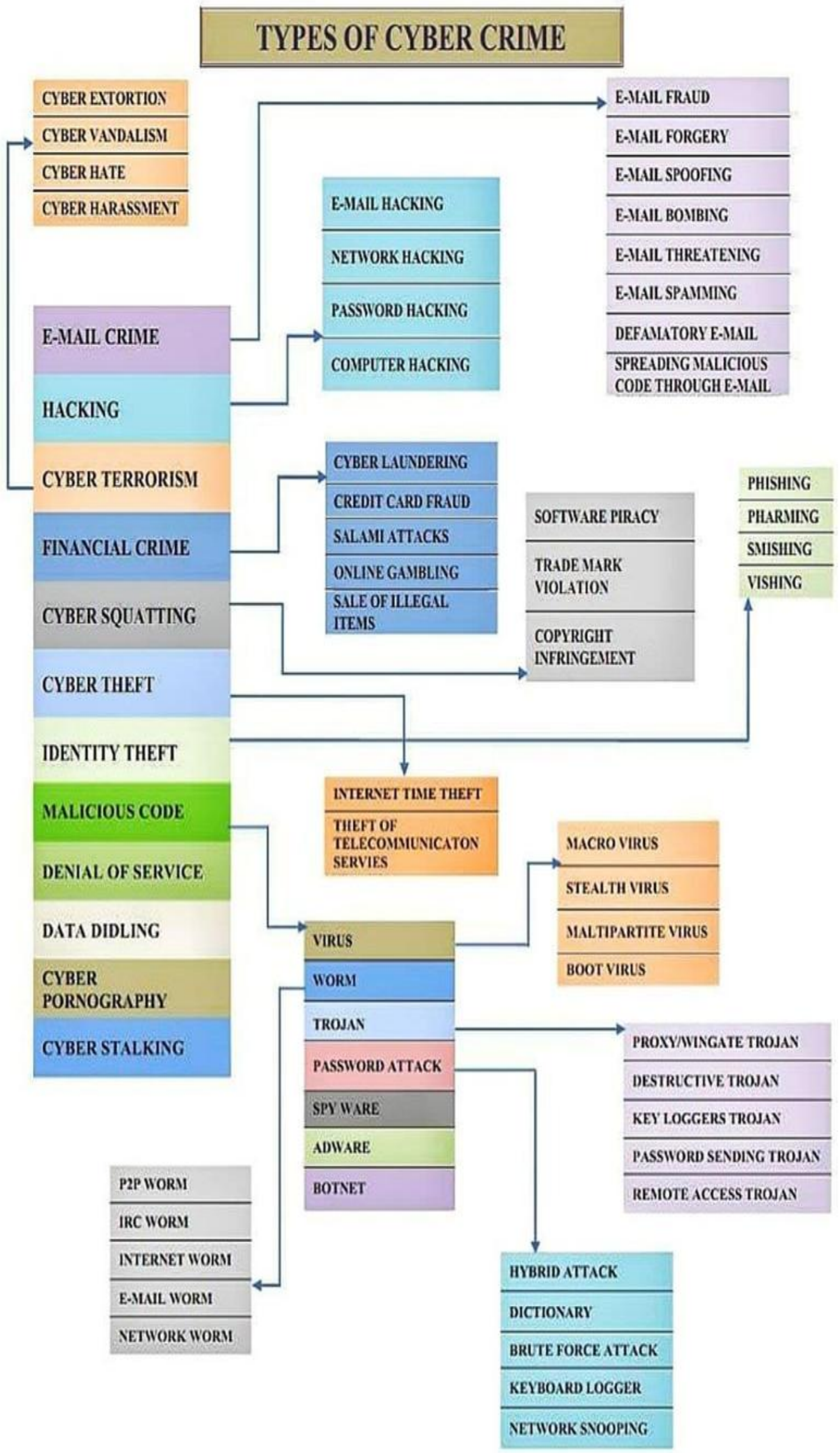
[23] Kabab. M E Salami fraud. www.nwfusion.com/newsletters/sec/2002/01467137.ht ml.

INTERNET TIME THEFT

Theft of Internet hours refers to using someone else internet hours. Section 43 (h) of the IT Act. 2000 lays down civil liabilities for this offence. It reads as.whosoeverwithout the permissionof the owneror any otherpersonwho is in charge a computer system orcomputernetwork. charges the service availed of by a person to the accountofanotherperson bytampering by way ofor manipulating any computer. computer systems ornetwork is liable to pay damagesnot exceeding newcrore to the person in office[24].

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

[24] Section 43 of the IT Act. 2000
[25] http: ~//www.asain laws./cyberlaw/library/cc/what_cc.htm


TYPES OF CYBER CRIME
CYBER EXTORTION
CYBER VANDALISM
CYBER HATE
CYBER HARASSMENT
E-MAIL FRAUD
E-MAIL FORGERY
E-MAIL SPOOFING
E-MAIL BOMBING
E-MAIL THREATENING
E-MAIL SPAMMING
DEFAMATORY E-MAIL
SPREADING MALICIOUS CODE THROUGH E-MAIL
E-MAIL HACKING
NETWORK HACKING
PASSWORD HACKING
COMPUTER HACKING
E-MAIL CRIME
HACKING
CYBER TERRORISM
FINANCIAL CRIME
CYBER SQUATTING
CYBER THEFT
IDENTITY THEFT
MALICIOUS CODE
DENIAL OF SERVICE
DATA DIDLING
CYBER PORNOGRAPHY
CYBER STALKING
CYBER LAUNDERING
CREDIT CARD FRAUD
SALAMI ATTACKS
ONLINE GAMBLING
SALE OF ILLEGAL ITEMS
SOFTWARE PIRACY
TRADE MARK VIOLATION
COPYRIGHT INFRINGEMENT
PHISHING
PHARMING
SMISHING
VISHING
INTERNET TIME THEFT
THEFT OF TELECOMMUNICATON SERVIES
MACRO VIRUS
STEALTH VIRUS
MALTIPARTITE VIRUS
BOOT VIRUS
VIRUS
WORM
TROJAN
PASSWORD ATTACK
SPY WARE
ADWARE
BOTNET
PROXY/WINGATE TROJAN
DESTRUCTIVE TROJAN
KEY LOGGERS TROJAN
PASSWORD SENDING TROJAN
REMOTE ACCESS TROJAN
P2P WORM
IRC WORM
INTERNET WORM
E-MAIL WORM
NETWORK WORM
HYBRID ATTACK
DICTIONARY
BRUTE FORCE ATTACK
KEYBOARD LOGGER
NETWORK SNOOPING

Prevention of cyber crimes

As per the recommendations of the International Maritime Organization (IMO), the cyber-attack risk must be approached using the following framework:

- The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management.
- The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted.
- To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans.
- It is also important to develop and implement measures to detect a cyber-attack as quickly as possible.
- Preparation and implementation of plans to restore critical systems for continued operations by providing resilience.
- Finally, identify and implement measures to be taken to backup and restore any affected systems.

The following can be the strategies can be used to prevent cybercrime:

Analyze your risk exposure:

To adequately prepare for a cyber-attack, you must assess the threat and give due consideration. Companies should consider the following:

- They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them.
- A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity.

- IT systems and operational technology systems should be checked by businesses.

Preventive measures:

It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures:

- Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account management, security updates and finally antivirus applications.
- Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that information.
- Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed.
- Securing critical systems by utilizing technology such as protocol-aware filtering and segregation.
- Ensuring that removable devices are encrypted, and that any USB used with any other device is tested for viruses.
- Furthermore, in order to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes.
- Additionally, organizing frequent training and awareness sessions for all employees can also help.
- Compliance audits of third-party service providers will also be beneficial.

2.4. Cybercrime laws in India

In terms of cybersecurity, there are five main types of laws that must be followed. Cyber laws are becoming increasingly important in countries such as India which have extremely extensive internet use. There are strict laws that govern the use of cyberspace and supervise the use of information, software, electronic commerce, and financial transactions in the digital environment. India’s cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security concerns. This has also made digital media accessible in a wider range of applications and enhanced its scope and effectiveness.

Information Technology Act, 2000 (IT Act):

The IT Act. 2000 came at a time when cyber-specific legislation was much needed. It filled up the lacunae for a law in the field of e-commerce. Taking cue from its base-document. i.e., the UNICITRAL Model Law anelectroniccommerce. adopted in 1996. a law attuned to the Indian needs has been formulated. Apart from e-commerce related provisions. computer crimes. and offencesalong by way of punishments have been enumerated. and defined. The power the police to investigate. and powerof search. and seizure. etc have been providedfor. However. certain points need is working right from the scratch or require revamping. At the first instance. though the IT Act. 2000 purports to have followed the pattern UNICITRAL Model Law anElectronicCommerce. yet what took people by surprise is coveragenotonlyof e-commerce. but somethingmore. i.e.,computer crime. and amendments to the Indian Penal Cede. The UNICITRAL Model Law did notcover any of the other aspects. Therefore, in a way. the IT Act. 2000 has been an attempt to include other issues relating to cyber world as well which might have an impact on the ecommercetransactions. and its smooth functioning. Though. that ofcourse is not reflected even form the Statements ofObjectives. and reasonsor the preamble of the Statute. Amendments to the Indian evidence Act are evidently made to permit electronic evidence in court. This is a step in the right direction. Secondly. a single sectiondevoted to liabilities of the Network Service Provider is highly inadequate. The issues are many more. Apart fromclassificationif the Network Service provider itself there can be variousother instances in which the Provider can be made liable specially under other enactments like the Copyright Act or the Trade Marks Act. However, the provision in the IT Act. 2000 devoted to ISP protection against any liabilities is restricted only to the Act or rules orregulations made there under. The section is not very clear as to whether the protectionfor the ISP's extends even under the other enactments.

Overview of the Act:

It is the first cyberlaw to be approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the *Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."*

However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being. made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act's scope has now been broadened to include all the latest communication devices.

The Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and be enforceable. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.

The important provisions of the Act

The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cybercrimes. Following are the appropriate sections:

- Section 43: This section of the IT Act applies to individuals who indulge in cybercrimes such as damaging the computers of the victim, without taking the due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.

In *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018)*, Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) ordered Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs 80.10 lakh from Mathura's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

- Section 66: Applies to any conduct described in Section 43 that is dishonest or fraudulent. There can be up to three years of imprisonment in such instances, or a fine of up to Rs. 5lakh.

In *Kumar v. Whiteley (1991)*, during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and changed files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cybercrime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar's computer. Kumar's wrongful act also caused the subscribers to incur a loss of Rs 38,248. N G Arun Kumar was sentenced by the Additional Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs 5,000 under Sections 420 of IPC and 66 of the IT Act.

- Section 66B: This section describes the penalties for fraudulently receiving stolen communication devices or computers and confirms a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed.

- Section 66C: The focus of this section is digital signatures, password hacking, and other forms of identity theft. The section imposes imprisonment upto 3 years along with one lakh rupees as a fine.
- Section 66D: This section involves cheating by personation using computer Resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs 1 lakh fine.
- Section 66E: Taking pictures of private areas, publishing or transmitting them without a person’s consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs 2 lakh fine.
- Section 66F: Acts of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- Section 67: This involves electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh.

Positive and negative aspects of the IT Act

This legislation contains the following benefits:

- Several companies are now able to conduct e-commerce without any fear because of the presence of this Act. Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online.
- Digital signatures are now able to be used by corporations to conduct online transactions. Digital signatures are officially recognized and sanctioned by the Act.
- Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under

the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government's standards are followed.

- Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by that government.
- It also provides information on the security concerns that are so crucial to the success of the use of electronic transactions. As part of the Act, the term secure digital signatures were defined and approved, which are required to have been submitted to a system of a security procedure. Therefore, it can be assumed that digital signatures are now secured and will play a huge part in the economy. Digital signatures can help conduct a secure online trade.

It is common for companies to have their systems and information hacked. However, the IT Act changed the landscape completely. A statutory remedy is now being provided to corporate entities in the event that anyone breaches their computer systems or network and damages or copies data. Damages are charged to anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge.

However, the said Act has a few problems:

- Section 66A is considered to be in accordance with Article 19(2) of the Constitution of India since it does not define the terms 'offensive' and 'menacing'. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.
- Considering how vulnerable the internet is, the Act has not addressed issues such as privacy and content regulation, which are essential.
- A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are.

- The Act doesn’t make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes.

ADVANTAGES

The Act offers the much-needed legal frameworkso that data is not denied legal effect. validities orenforceability. solelyon the ground that it is in the formofelectronicrecords. From the perspective of e-commerce in India. the IT Act 2000. and its provisionscontain many positive aspects. Firstly. the implicationsof these provisionsfor the e-businesses would be that email wouldnow be a valid. and legal formofcommunication in ourcountry that can be duly produced. and approved in a courtof law. Second. Companies shall now be able to carry outelectroniccommerce using the legal infrastructure provided by the Act. Third. Digital signatures have been given legal validity. and sanction in the Act Fourth. the Act throwsopen the dressfor the entry ofcorporatecompanies in the business of being Certifying Authorities’for issuing Digital Signatures Certificates. Fifth. the Act nowallowsGovernment to issue notificationon the web thus heralding e-governance. Sixth. the Act enables the companies to file any form. applicationor any otherdocument by way of any office. authority. bodyor agency ownedorcontrolled by the appropriateGovernment in electronicform by means of such electronicform as may be prescribed by the appropriateGovernment. Seventh. the IT Act also addresses the important issues of security. which are so critical to the success ofelectronictransactions. The Act has given a legal definition to the conceptof secure digital signatures that would be required to have been passed through a system of a securities procedure. as stipulated by the Government at a later date. Eighth. under the IT Act. 2000. it shall now be possibleforcorporate to have a statutory remedy in case if anyone breaks into their computer systems ornetwork. and causes damages orcopies data. The remedy provided by the Act is in the formofmonetary damages. not exceeding Rs. 1 crore.

DISADVANTAGES

The IT Law 2000. though appears to be self-sufficient. it takes mixed stand when it comes to many practical situations. It loses its certainties at many places like the newmentionedbelow: ~- First. the law misses outcompletely the issue of Intellectual PropertiesRights... and makes noprovisionswhatsoeverforcopyrighting. Trade marking or patenting ofelectronicinformation. and data. The law even doesn't talk of the rights. and liabilities ofdomain name holders. the first step of entering into the e-commerce. Second. the law even stays silent over the regulationofelectronic payments gateway. and segregates the negotiable instruments from the applicability'sof the IT Act. which may have major effect on the growthof e-commerce in India. It leads to make the banking. and financial sectorsirresolute in their stands. Third. the act empowers the Deputies Superintendent ofPolice to look up into the investigations. and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the contextofCorporate India as companies have public offices which wouldcome within the ambit of "public place" under the Act. As a result. companies will not be able to escape potential harassment at the hands of the DSP. Fourth. internet is a borderless medium. it spreads to every cornerof the world where life is possible. and hence is the cyber-criminal... then howcame is it possible to feel relaxed. and secured once this law is enforced in the nation? Fifth. the Act initially was supposed to apply to crimes committed all over the world. but nobodyknowshow can this be achieved in practice. how to enforce it all over the world at the same time? Sixth. the IT Act is silent on filming anyone s personalactions in public. and. then distributing it electronically. It holds ISPs (Internet Service Providers) responsiblefor third parties' data. and information. Unless contravention is committedwithout their knowledgeor unless the ISP has undertaken due diligence to prevent the contravention. This is a practically impossibleapproach. Further according to the researcher. the recently proposed IT Act. 2000 amendments are neither desirable norconducivefor the growthof ICT in India. They are suffering fromnumerous drawbacks. and grey areas. and they must not be transformedinto the law of the land. These amendments must be seen in the light ofcontemporary standards. and requirements.

Sameof the more pressing. and genuine requirements in this regard are 1. There are no securities concernsfor e-governance in India. 2. The conceptof due diligence forcompanies. and its officers is not clear to the concerned segments. 3. The use of ICT for justice administration must be enhanced. and improved. 4. The offenceof cyber extortions must be added to the IT Act. 2000 along by way of Cyber Terrorism. and othercontemporarycybercrimes. 5.. The increasing nuisance of e-mail hijacking. and hacking must also be addressed. 6. The use of ICT for day to day procedural matters must be considered. 7. The legal risks of e-commerce in India must be kept in mind. 8. The conceptsof private defence. and aggressive defence are missing from the IT Act. 2000 9. Internet banking. and its legal challenges in India must be considered 6. Adequate. and reasonableprovisions must be made in the IT Act. 2000 regarding “Internet censorship” 11. The use of private defence for cyber terrorism must be introduced in the IT Act. 2000 12. The legalities of sting operations (like Channel 4) must be adjudged. 13. The deficiencies ofIndian ICT strategies must be removed as soon as possible. 14. A sound BPO platform must be established in India. etc. The act. on an overall analysis. demonstrates a lack ofdiscussion. and incorporationofvarious issues relating to cyber law. Through the Act has been given the name „InformationTechnology Act yet many legal issues like online rights ofconsumers. privacy concerns. domain names disputes. payment. and security-bugbears. etc have not been addressed. Finally. haw the act will be implemented by a Courtof law. and its implementations. and flaws in the long run are yet to be tested in the case-specific factual terrain.

Constitution of India

Any person who fails to assist the Government agency in decrypting the information sought to be intercepted is liable for imprisonment up to 7 years. Article 300A of Constitution of India states that all persons have a right to hold and enjoy their properties. In a specific case of Bhavnagar University v. 34Palitana Sugar Mills Pvt. Ltd[26]. Supreme Court applied the constitutional clause with the interpretation that anyone can enjoy his or her property rights in any manner preferred. This also includes property rights to information stored on computers or in any electronic format. Articles 301 to 305 refer to the right for free trade. As long as an individual carries out a business in accordance with law, it cannot be interfered. Besides, free trade and any commercial activities cannot be visualized without technological rights, which mean that any distortion of those is illegal. In India these provisions have been effectively used to protect individual property rights against the actions of cyber criminals

Indian Penal Code, 1860 (IPC):

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

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

If the IT Act is not sufficient to cover specific cybercrimes, law enforcement agencies can apply the following IPC sections:

- Section 292: The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cybercrimes as well. A way obscene material or sexually explicit acts or exploits of children are published or transmitted electronically is also governed by this provision. The penalty for such acts is imprisonment and fines up to 2 years and Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second time) offenders.
- Section 354C: In this provision, cybercrime is defined as taking or publishing pictures of private parts or actions of a woman without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman’s sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.
- Section 354D: Stalking, including physical and cyberstalking, is described and punished in this chapter. The tracking of a woman through electronic means, the internet, or email or the attempt to contact her despite her disinterest amounts to cyber-stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases.

A victim in the case *Kalandi Charan Lenka v. the State of Odisha (2017)* has received a series of obscene messages from an unknown number that has damaged her reputation. The accused also sent emails to the victim and created a fake account on Facebook containing morphed images of her. The High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

- Section 379: The punishment involved under this section, for theft, can be up to three years in addition to the fine. The IPC Section comes into play in part because many cybercrimes involve hijacked electronic devices, stolen data, or stolen computers.
- Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section on cybercriminals doing crimes like creating fake websites and cyber frauds. In this section of the IPC, crimes related to password theft for fraud, or the creation of fraudulent websites are involved.
- Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.
- Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace are dealt with and punished with imprisonment ranging up to two years, or both. In *Anil Kumar Srivastava v. Add. Director, MHFW (2005)*, the petitioner had forged signed the signature of the AD and had then filed a case that made false allegations against the same individual. Because the petitioner also attempted to pass it off as a genuine document, the Court held that the petitioner was liable under Sections 465 and 471 of the IPC.
- Section 468: Fraud committed with the intention of cheating may result in a seven-year prison sentence and a fine. This section also punishes email spoofing.

Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cybercrimes, in addition to the laws listed above.

Even though there are laws against cybercrime in place, the rate of cybercrime is still rising drastically. It has been reported that cybercrime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cybercrime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness, and the increasing costs of investigation due to technology.

Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence was the receipt of stolen property, the offence under section 66B of the IT Act was bailable while the offence under Section 411 of the IPC was not. In the same manner, in respect of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable.

In *Gagan Harsh Sharma v. The State of Maharashtra (2018),* the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that is bailable and compoundable.

Information Technology Rules (IT Rules):

There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: According to these rules, entities holding individuals’ sensitive personal information must maintain certain security standards that are specified.

- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021: To maintain the safety online of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011: According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.
- The Information Technology (Electronic Service Delivery) Rules, 2011: Basically, these regulations give the government the authority to specify the delivery of certain services, such as applications, certificates, and licenses, by electronic means.
- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules): There are several ways in which the CERT-In rules provide for the working of CERT-In. In accordance with rule 12 of the CERT-In rules, a 24-hour Incident response helpdesk must be always operational. Individuals, organizations, and companies can report cybersecurity incidents to Cert-In if they are experiencing a cybersecurity Incident. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately.

Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(I) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In.

Companies Act, 2013:

A majority of the corporate stakeholders consider the Companies Act of 2013 to be the most pertinent legal obligation to properly manage daily operations. This Act enshrines in law all the techno-legal requirements that need to be met, implementing the law as a challenge to the companies that are not compliant. As part of the Companies Act 2013, the SFIO (Serious Fraud Investigation Office) is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors.

As a result of the Companies Inspection, Investment, and Inquiry Rules, 2014 notification, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management.

Cybersecurity Framework (NCFS):

As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures:

- A better understanding, management, and reduction of the risks associated with cybersecurity.
- Prevent data loss, misuse, and restoration costs.
- Determine the most critical activities and operations that must be secured.
- Provides evidence of the trustworthiness of organizations that protect critical assets.
- Optimize the cybersecurity return on investment (ROI) by prioritizing investments.
- Responds to regulatory and contractual requirements.
- Assists in the wider information security program.

Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication.

Why cybercrime laws in India

Just like the other countries, our country is too concerned about the issue of cyber security and related crimes. Particularly in India, there are a growing number of cyber security concerns, and its responsibility to resolve them is of critical importance. It has recently been revealed that the government is losing nearly R. 1.25 lakh crore per annum to cyber-attacks overall, according to an Economic Times analysis of cybercrime.

According to another study published by Kaspersky, the number of attacks in India increased from 1.3 million to 3.3 million from the first quarter of 2020 till the end of that quarter. A total of 4.5 million attacks were recorded by India in July 2020, which was the largest number recorded so far. In July 2021, In violation of the Reserve Bank of India's directions on the storage of payment system data, Mastercard Asia/Pacific Pte Ltd (Mastercard) was banned from onboarding new domestic customers. A cyber security policy, however, does not offer an adequate method of preventing the hazards posed by the internet, and the most effective means of confronting these threats is through training. There are significant resources that the government must dedicate to safeguarding important data assets. Cyberlaw needs to be updated to incorporate the latest legal and technological developments and to address the challenges posed by the rapid development of technology.

Importance of cybercrime laws

The following points can highlight the importance of cyber laws:

- An important goal of any cyber law is to prosecute those who undertake illegal activities using the internet. To effectively prosecute these types of crimes, such as cyber abuse, assaults on other websites or individuals, theft of records, disrupting every company's online workflow, and other criminal activities, significant efforts should be undertaken, and hence, which is where cyber laws come into the picture.
- In the cases involving a violation of cyber law, the action is taken against the individual on the basis of his location and how was he involved in that violation.
- Prosecuting or retracting hackers is the most important thing since most cybercrimes are beyond the reach of a felony, which is not a crime.
- The use of the internet is also associated with security concerns and there are even some malicious individuals who want to gain unauthorised access to the computer device and commit fraud using it in the future. Hence, all rules and cyber laws are designed to protect internet businesses and internet users from unwanted unauthorized access and malicious cyber-attacks. There are a variety of ways in which individuals or associations can take action against others who commit criminal acts or break cyber laws.

Causes of Cyber Crime in India

Cybercriminals always choose an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where the transaction of a huge amount of money is made on an everyday basis and hack sensitive information.

Catching such criminals is difficult. Hence, that increases the number of cyber-crimes. Computers are vulnerable, so laws are required to protect and safeguard them against cyber criminals. Following are the reasons for the vulnerability of computers:

- **Easy to access** – The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders etc. that can easily fool biometric systems and bypass firewalls can be utilized to get past many security systems.

- **Capacity to store data in comparatively small space –** The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for people to steal data from any other storage device and use it for their own profit.
- **Complex –** The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. The cyber criminals take advantage of these gaps.
- **Negligence –** Negligence is one of the characteristics of human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides a cyber-criminal the access and control over the computer system.

Loss of Evidence – The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crimes

Need for cybercrime laws in India.

Cyberlaw is of particular importance in countries such as India, where the internet is used widely. To protect both individuals and organizations against cybercrime, the law was enacted. The cyberlaw allows other people or organizations to take legal action against someone if that person violates and breaks the provisions of the law.

Cyberlaw may be required in the following circumstances:

- Since all the transactions associated with stocks are now executed in demit format, anyone who is involved with these transactions is protected by cyber law in the event of any fraudulent transactions.
- Almost all Indian companies have electronic records. A company may need this law to prevent the misuse of such data.
- As a result of the rapid development of technology, various government forms are being filled out electronically, such as income tax returns and service tax returns. Anybody can misuse those forms by hacking government portal sites, and thus, cyberlaw is required under which legal action can be taken.

- Shopping today is done through credit cards and debit cards. Unfortunately, some frauds perpetrated by means of the internet clone these credit cards and debit cards. The cloning of a credit or debit card is a technique that allows someone to obtain your information via the Internet. This can be prevented by cyberlaw as under Section 66C of the IT Act, there is 3-year imprisonment along with a fine up to one lakh rupees if anyone tries to make use of any electronic password fraudulently or dishonestly.
- Business transactions are typically carried out by means of digital signatures and electronic contracts. The misuse of digital signatures and electronic contracts can be easily accomplished by anyone involved with them. Cyberlaw provides protection against these types of scams.

2.5. Cybercrime and security

Cybersecurity can be defined as the collection of technologies, processes, and practices that are intended to prevent networks, devices, programs, and data from being attacked, damaged or accessed by unauthorized persons. Alternatively, cyber security may also be referred to as information technology security.

What is Cyber Security?

- **Cyber security** or information technology security are the techniques of **protecting computers, networks, programs and data** from unauthorised access or attacks that are aimed for exploitation of **cyber-physical systems and critical information infrastructure**.
  - **Cyber-physical systems** integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.
    - **Examples:** Industrial control systems, water systems, **robotics systems**, smart grid etc.
  - **Critical Information Infrastructure:** The **Information Technology Act of 2000** defines **Critical Information Infrastructure** as a computer resource, the

incapacitation or destruction of which shall have debilitating impact on **national security, economy, public health or safety**.

- **Cyber Threats:**
  - **Malware, Viruses, Trojans, Spywares, Backdoors,** which allow remote access.
  - **DDoS (Distributed Denial of Service)**, which **floods servers** and networks and makes them unusable.
  - **DNS (Domain Named System)** poisoning attacks which compromises the DNS and **redirect websites to malicious sites**.
- **Major Areas covered in Cyber Security are:**
  - **Application Security:** To **protect applications** from threats that can come through flaws in the application design
  - **Information Security:** To **protect information** from unauthorised access to avoid identity theft and to protect privacy.
  - **Disaster Recovery:** It is a process that includes **performing risk assessment**, establishing priorities, developing recovery strategies in case of a **cyber disaster**.
  - **Network Security:** includes activities to protect the **usability, reliability, integrity** and safety of the network.
    - Effective network security targets a variety of threats and **stops them from entering or spreading on the network**.

What is Cyber-Crime Vs Cyber-Terrorism Vs Cyber-War?

- **Cyber-Crimes:** Cyber-crime is **unlawful acts wherein the computer is either a tool or a target or both**.
  - Cyber-crimes can involve **criminal activities** that are traditional in nature, such as **theft, fraud, forgery, defamation and mischief etc**.
- **Cyberwars: Cyberwar** is an **organised effort by a nation state to conduct operations in cyberspace against foreign nations**.
  - Included in this category is the **Internet's use for intelligence** gathering purposes.

- **Cyber-Terrorism:** Cyberterrorism is the **convergence of cyberspace and terrorism**.
  - It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to **intimidate or coerce a government or its people** in furtherance of **political or social objectives**.

What are the Challenges Related to Cyber Security in India?

- **Profit-Friendly Infrastructure Mindset:** Post **liberalisation**, the **Information Technology (IT)**, **electricity and telecom sector** has witnessed large investments by the private sector. However, their inadequate focus on cyber-attack preparedness and recovery in regulatory frameworks is a cause of concern.
  - All **operators are focused on profits,** and do not want to invest in infrastructure that will not generate profits.
- **Absence of Separate Procedural Code:** There is **no separate procedural code** for the investigation of cyber or computer-related offences.
- **Trans-National Nature of Cyber Attacks:** Most cyber-crimes are trans-national in nature. The **collection of evidence from foreign territories** is not only a difficult but also a tardy process.
- **Expanding Digital Ecosystem:** In the last couple of years, India has traversed on the path of **digitalising its various economic factors** and has carved a niche for itself successfully.
  - Latest technologies like **5G** and the **Internet of Things (IoT)** will increase the coverage of the internet-connected ecosystem.
  - With the advent of digitalisation, **paramount consumer and citizen data** will be stored in digital format and transactions are likely to be carried out online which makes **India a breeding ground for potential hackers** and cyber-criminals.
- **Limited Expertise and Authority:** Offences related to **crypto-currency** remain **under-reported** as the capacity to solve such crimes remains limited.
  - Although most **State cyber labs** are capable of analysing hard disks and mobile phones, they are yet to be recognized as **'Examiners of Electronic Evidence'** (by

the central government). Until then, **they cannot provide expert opinions on electronic data**.

What are the Current Provisions for Cyber-Security in India?

- **Indian National Security Council:** To shape the ecosystem related to cyber policy.
- **National Cyber Security Strategy:** To focus on security in the early stages of design in all digitisation initiatives.
- **Computer Emergency Response Team (CERT-In):** For alerts regarding cybersecurity breaches and issues.
- **Indian Cyber Crime Coordination Centre (I4C):** To handle several issues regarding cybercrime in a comprehensive and coordinated manner.
- **Cyber Swachhta Kendra:** To create a secure cyberspace by detecting botnet infections in India

What Should be the Modern-Day Solutions for Modern Day Problems of Cyber-Threats?

- **Centre-State Nexus Towards Secure Cyberspace:** With **police and public order being in the State List**, the primary objective to check crime and create the necessary cyberinfrastructure lies with States.
  - At the same time, with the **IT Act and major laws being central legislations**, the central government should look forward to evolving **uniform statutory procedures for the law enforcement agencies**.
  - Centre and States must not only work in tandem and **frame statutory guidelines to facilitate investigation of cybercrime** but also need to commit sufficient funds to develop much-awaited and required **cyber infrastructure**.
- **Upgrading Cyber Labs:** Cyber forensic laboratories should be upgraded with the advent of new technologies.
  - **National Cyber Forensic Lab** and the **Cyber Prevention, Awareness and Detection Centre (CyPAD)** initiative of the Delhi Police, is a good step in this direction.

- **Capacity Building:** It is essential to build up sufficient capacity to deal with cybercrime. It could be done either by **setting up a separate cyberplaces station** in each district or range, or **having technically qualified staff in every police station**.
- **Reforming the Justice Delivery System:** As electronic evidence differs greatly from evidence of traditional crimes when it comes to breach of privacy, it is essential to **develop standard and uniform procedures to deal with electronic evidence** to ensure time-bound justice in order to maintain the safety of Indians as well as the infrastructure.
- **Developing Cyber-Defence Mechanism:** A holistic approach for dealing with cyber conflict is necessary, whether it's conducting **cyber search operations** or **extending the scope of countermeasures against cyber-attacks**.
    - A **clear public posture on cyber defence** and warfare **boosts citizen confidence** thus enabling a more **engaging, stable and secure** cyber ecosystem.

Several types of organizations, including government, military, corporations, financial institutions, and medical facilities use computers and other devices to process, store, and process extremely large amounts of data. Many of those records contain sensitive data including intellectual property, financial information, personal information, etc. for which unauthorized access or exposure could have negative repercussions. There is a growing area of cyber security dedicated to protecting the systems for processing and storing sensitive information that organizations send over networks and to other devices. Thus, cybersecurity is the field dedicated to securing this sensitive information as well as the systems by which such information is transmitted or stored. With the number of cyberattacks and the sophistication of those attacks moving up, companies and organizations, especially those that are tasked with safeguarding sensitive data, (including attacks pertaining to national security, health information, or financial information), there must be steps taken for ensuring the security of their proprietary business and personnel data.

2.5.1. Subject matter: Both fields are studied in different disciplines. Information Cyber security strategies

It is also extremely important for an organization to develop and build an effective cybersecurity strategy. The following must be included in cybersecurity strategies:

Ecosystem:

The ecosystem of an organization needs to be strong in order to prevent cybercrime. Generally, an organization ecosystem has 3 components, automation, interoperability, and authentication. By developing a safe and strong system, the organization would be likely to protect these components and could not be attacked by malware, attrition, hacks, insider attacks, and equipment thefts.

Framework:

A framework for compliance with security standards is an assure that can help to ensure that these standards are adhered to. Updating infrastructure is made possible because of this. Furthermore, it also facilitates collaboration between governments and businesses.

Open standards:

Enhanced security against cybercrime is a direct result of open standards. Through open standards, both businesses and individuals can easily implement proper security measures. These standards will also facilitate a greater level of economic growth and a broader range of new technologies.

IT mechanisms:

A variety of IT measures or mechanisms are available that can be beneficial. In the fight against cybercrime, it is essential to promote these measures and mechanisms. End-to-end protection measures, association-based protection, link-based protection, and data encryption are a few of the measures.

E-governance:

It is possible for the government to provide services online through e-governance. E-governance, however, is not taken advantage of in many countries. Cyberlaw should focus on advancing this technology to give citizens greater control.

Infrastructure:

As part of cybersecurity, protecting the infrastructure is one of the most crucial steps. This applies especially to the electrical grid as well as data transmission lines. Cybercrime is often perpetrated against outdated infrastructure.

2.6. Differences between cybercrime and cyber security

There is more to cybersecurity than just a set of guidelines and actions designed to prevent cybercrime. Ultimately, cyber-security aims to prevent hackers from finding and exploiting vulnerabilities in government and corporate networks, and therefore to make life difficult for them to do so. By contrast, cybercrime, compared to traditional crime, tends to focus more on preserving the privacy of individuals and their families while engaging in online activities.

Here is a list of the differences between cyber security and cybercrime that you should know about:

- Types of crime: The type of crime in cyber security is defined by those crimes in which a computer program, hardware, or computer network serves as the main target of an attack if it is compromised. On the other hand, cybercrime is concerned with a specific person or group of people, along with their data, as the main targets.
- Victims: Secondly, there are also differences in the types of victims in these two fields. Governments and corporations are the primary targets in cyber security while, in cybercrime, victims can range from individuals, families, organizations, governments, and corporations.

- technology, computer science, and computer engineering are the fields that cover cybersecurity. Code writing, networking, and engineering are used to enhance network security. In contrast, cybercrime falls under the criminological, psychological, and sociological categories. It refers to a theory of how crime occurs and how it can be prevented.
-

With the advancement in technology, disturbing elements are appearing on the dark web that is disturbing. The Internet has become a tool of evil deeds that are exploited by intelligent people for evil motives and sometimes for financial gain. Thus, now, cyber laws come into the picture and are important for every citizen. Because cyberspace is an extremely difficult territory to deal with, some activities are classified as grey activities that cannot be governed by law.

In India as well as across the globe, with the increasing reliance of humans on technology, cyber laws need constant up-gradation and refinement to keep pace. There has also been a significant increase in the number of remote workers because of the pandemic, which has increased the need for application security. There is a need for legislators to take extra precautions to keep ahead of the imposters so that they can act against them as soon as they arise. It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together. However, ultimately, it is up to the users to participate in the fight against cybercrime. The only way for the growth of online safety and resilience to take place is through the consideration of the actions of these stakeholders, ensuring they stay within the confines of the law of cyberspy.

2.7. Cyber Crime law international standards

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

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

Australia:

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

Canada:

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

Germany.

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

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 canter 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.

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.

Chapter 3

Implementation Of Cybercrime Laws and Regulations

3.1. PREVENTION AND DETATIONS OF CYBER CRIME

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 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 (Olemaun, 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, cybercrime 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. ৩. 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.

3.2. Prevention of cyber crimes

As per the recommendations of the International Maritime Organization (IMO), the cyber-attack risk must be approached using the following framework:

- The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management.
- The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted.
- To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans.
- It is also important to develop and implement measures to detect a cyber-attack as quickly as possible.
- Preparation and implementation of plans to restore critical systems for continued operations by providing resilience.
- Finally, identify and implement measures to be taken to backup and restore any affected systems.

The following can be the strategies can be used to prevent cybercrime:

3.2.1. Analyze your risk exposure:

To adequately prepare for a cyberattack, you must assess the threat and give due consideration. Companies should consider the following:

- They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them.

- A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity.
- IT systems and operational technology systems should be checked by businesses.

3.2.2. **Preventive measures**:

It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures:

- Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account management, security updates and finally antivirus applications.
- Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that information.
- Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed.
- Securing critical systems by utilizing technology such as protocol-aware filtering and segregation.
- Ensuring that removable devices are encrypted, and that any USB used with any other device is tested for viruses.
- Furthermore, to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes.
- Additionally, organizing frequent training and awareness sessions for all employees can also help.
- Compliance audits of third-party service providers will also be beneficial.

How to Prevent Cyber Crime

How can individuals and organizations help protect themselves from cyber-crimes? The following are examples of how to prevent cyber-crime, including tactics, steps, and strategies:

Follow Cybersecurity Best Practices and Guidelines

Employers typically establish cybersecurity policies or regulations based on best practices to protect their employees and critical business data. These policies can be adopted for personal use as well. Commonsense practices include backing up data and not sharing personal information such as Social Security numbers when responding to unsolicited emails. Additional practices include avoiding pop-ups and unknown email attachments and using strong passwords.

Use Digital and Physical Security Methods

Firewalls and antivirus software are a first line of defense to protect your devices from cyber-attacks. For example, a firewall is a technical tool that helps to prevent unauthorized access to unsecure websites. Antivirus software can detect viruses and defend your device from getting infected. Additionally, a commonsense strategy is to never leave a laptop unattended in a public place.

Update Software Regularly

Software developers periodically send automated software update messages. For example, Microsoft update messages can appear when starting up your laptop. These updates fix bugs and improve performance, and they enable individuals to manage security risks and keep their systems protected. These updates are vital to maintaining the latest version of software, which also includes patches to resolve previously identified vulnerabilities.

Become Cyber Aware

A key step to prevent a cyber-attack from affecting your device is to educate yourself. Cyber criminals often attack the edge of the network — that is, where end users are. For example, to gain access to a corporate database, a cyber-criminal may execute a phishing attempt on a single user. If that user clicks on the link in the phishing email, the cyber-criminal may be able to gain access to the company’s entire network. Therefore, organizations need to train their employees on how to identify threats.

Manage Your social media Settings

According to the Pew Research Center, YouTube is the most used social media site in the U.S. — 81% of Americans use it. When it comes to social media use, Facebook comes a close second at 69%. For younger adults, platforms like Instagram and WhatsApp are more popular. The common thread with all social media platforms is that anyone in the world can see users' activities — what they posted and what they liked, for example. Though social media platforms allow users to control who sees the information they share, the steps in implementing these security settings vary by site. By reviewing and adjusting the privacy settings in the platforms they use, users can protect themselves.

Talk to Your Children About the Threats

Common Sense Media reports that 84% of teenagers and about 53% of children own a smartphone. Children have access to a wide range of digital media, from TikTok videos to online learning platforms. Parents need to discuss the potential dangers of online threats with their children to help keep them safe. This requires listening while being straightforward about the types of content and contacts that are inappropriate.

Cyber Crime Prevention Resources

The following websites offer recommendations and tips for preventing cyber-crime:

- Delta Net International, "Why Is It Important to Manage Your Privacy Settings on Social Media?": This resource explains why managing privacy settings is important to mitigate dangers when using social media.
- Federal Trade Commission, Talk to Your Kids: This resource provides parents with tips on how to discuss privacy, identity, and online security topics with their children.
- Norton, "10 Cybersecurity Best Practices That Every Employee Should Know": This resource provides top cybersecurity best practices for employers.

3.2. INVESTIGATION AND PROSECUTION OF CYBER CRIME

In July 2021, hackers targeted Kaseya, a U.S. information technology firm, in a ransomware attack that affected up to 1,500 businesses worldwide, from the U.S. to Sweden to New Zealand. The hackers demanded $70 million to restore the impacted services. Nearly every type of organization from public schools and health services systems to oil pipelines and beef processing plants has fallen victim to this type of attack in 2021.

Criminal activity taking place in the digital world, known as cyber-crime, comes in various forms. Like in the physical world, cybercrime is investigated by trained professionals who gather and secure evidence to confront cyber-criminal activity and prosecute crimes. This type of investigation is known as a cybercrime investigation.

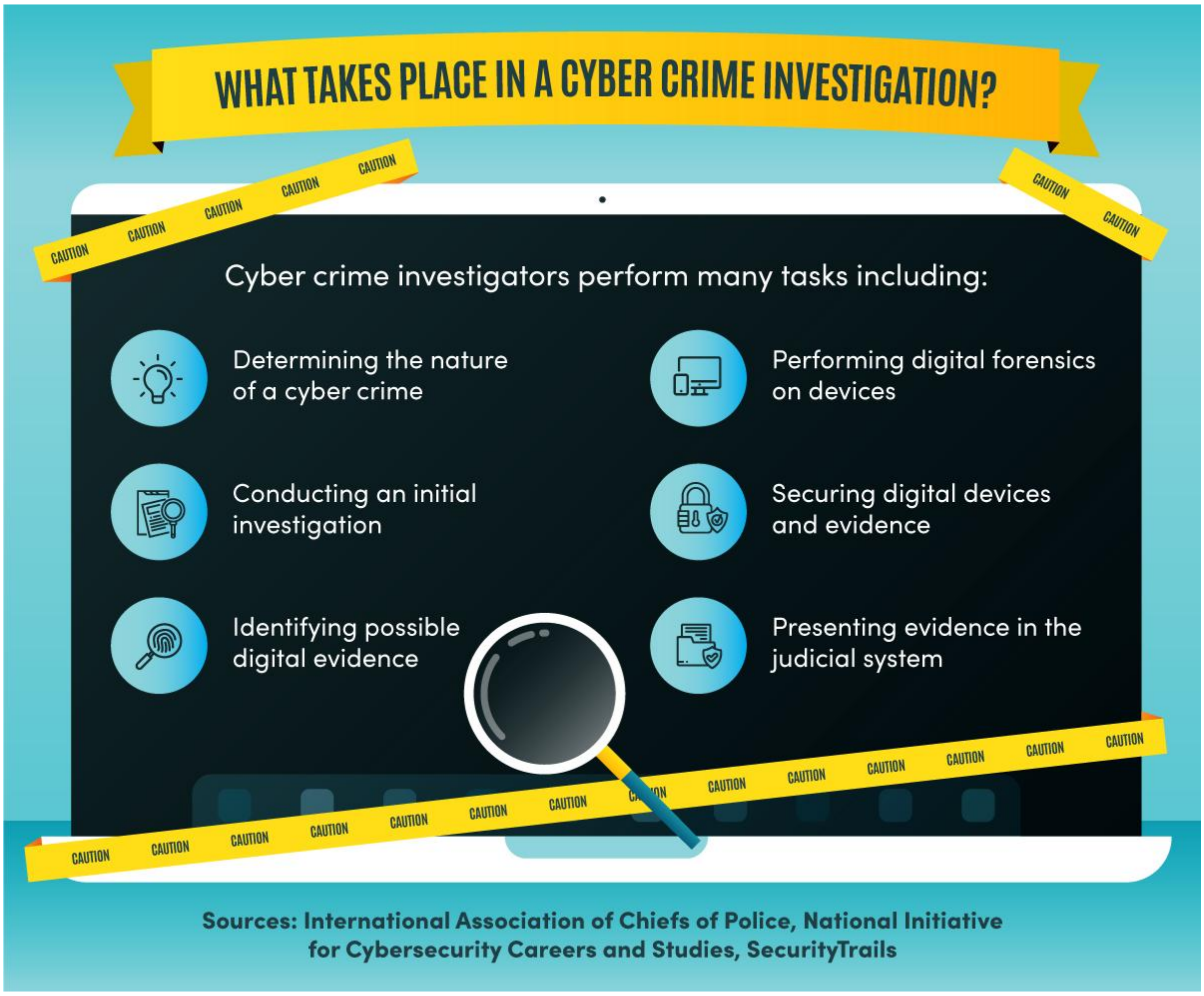
According to *Cybercrime Magazine*, the projected cost of cybercrime to the global economy will be $10.5 trillion annually by 2025. Cyber-criminal activity can also put lives at risk. Earlier this year, hackers threatened the water supply of a small town, raising concerns about the impact cyber criminals can have on the health and safety of entire populations. These threats highlight the importance of cyber-crime investigations and their role in making the internet a safer place for society and business.

What Is a Cyber Crime Investigation?

A comparison of cybercrime investigations and physical-world criminal investigations reveals a primary difference: evidence in criminal investigations is mostly digital in nature.

A cyber-crime investigation is the process of investigating, analysing, and recovering forensic data for digital evidence of a crime. Examples of evidence in a cybercrime investigation include a computer, cell phone, automobile navigation system, video game console, or other networked device found at the scene of a crime. This evidence helps cybercrime investigators determine the perpetrators of a cybercrime and their intent.

For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Due to the Information Technology Act, 2000 (“**IT Act**”), certain provisions of Criminal Procedure Code and the Evidence Act, have been amended. Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation.


WHAT TAKES PLACE IN A CYBER CRIME INVESTIGATION?
CAUTION
Cyber crime investigators perform many tasks including:
Determining the nature of a cyber crime
Performing digital forensics on devices
Conducting an initial investigation
Securing digital devices and evidence
Identifying possible digital evidence
Presenting evidence in the judicial system

Sources: International Association of Chiefs of Police, National Initiative for Cybersecurity Careers and Studies, SecurityTrails

Who can investigate cybercrime?

The power to investigate the accused in regard to the cyber offences, has been entailed in Section 78 of the IT Act, which says that "*notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act"*. Nevertheless, the IT Act is not sufficient to meet the necessity, therefore the Criminal Procedure Code, 1978 and the Indian Penal Code, 1860, were also amended accordingly to introduce cyber-crime under their ambit. This gives power to the Inspector to register and investigate the cyber-crime as like another crime.

Process of search & arrest

The power of the police office and other officers to enter, search etc. is entailed in Section 80 (1) of the IT Act, which says that, notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of the Inspector or any other officer of the Central Government or State Government authorized by the Central Government in this regard, may enter any public place, search and arrest without warrant any person, who is reasonably suspected of having committed or of committing or about to commit an offence under the IT Act.

Pursuant to Section 80 (2) of the IT Act, any person who is arrested under sub-section (1) by an officer other than a police officer then such officer shall, without any unreasonable delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

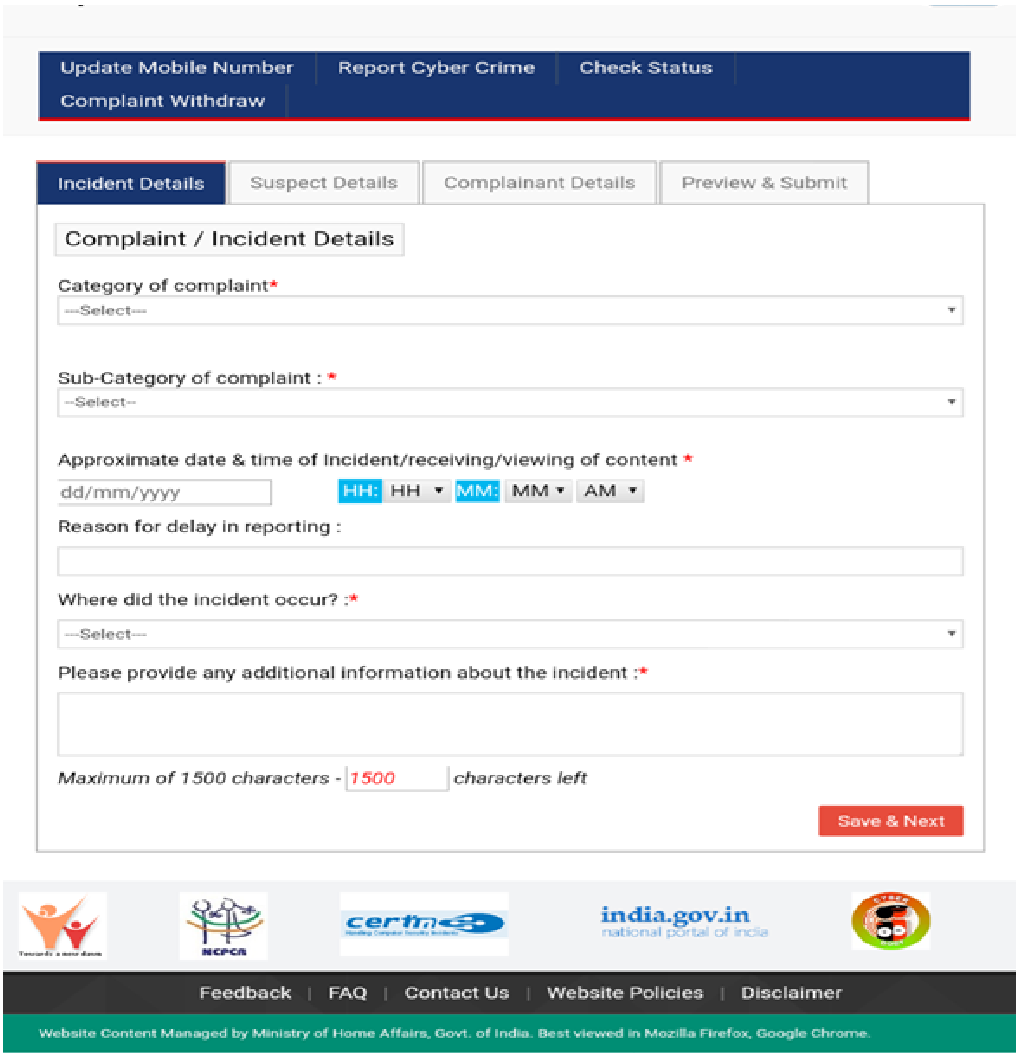
The Government of India had launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature. The Central Government has launched a scheme for formulating of Indian Cyber Crime Coordination Centre (I4C)[3] to handle the cybercrime incidents in India, in an inclusive & coordinated manner.

he said scheme has following seven components:

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Forensic Laboratory (NCFL)
- National Cybercrime Training Centre (NCTC)
- Cybercrime Ecosystem Management

- Platform for Joint Cybercrime Investigation Team
- National Cybercrime Reporting Portal
- National Cyber Research and Innovation Centre (NCR&IC)

- The government is also planning to set up Regional Cyber Crime Coordination Centers at respective States/UTs.
- By following below-mentioned steps, one can report a cyber-crime online:
- Step 1: Go to https://www.cybercrime.gov.in/Accept.aspx.
- Step 2: Click on '***Report Other Cyber Crimes***' on the menu.
- Step 3: Create '***Citizen login'.***
- Step 4: Click on 'File a Complaint'.
- Step 4: Read the conditions and accept them.
- Step 5: Register your mobile number and fill in your name and State.
- Step 6: Fill in the relevant details about the offence.



Update Mobile Number | Report Cyber Crime | Check Status

Complaint Withdraw

Incident Details | Suspect Details | Complainant Details | Preview & Submit

Complaint / Incident Details

Category of complaint*

---Select---

Sub-Category of complaint : *

--Select--

Approximate date & time of Incident/receiving/viewing of content *

dd/mm/yyyy HH: HH ▾ MM: MM ▾ AM ▾

Reason for delay in reporting :

Where did the incident occur? :*

---Select---

Please provide any additional information about the incident :*

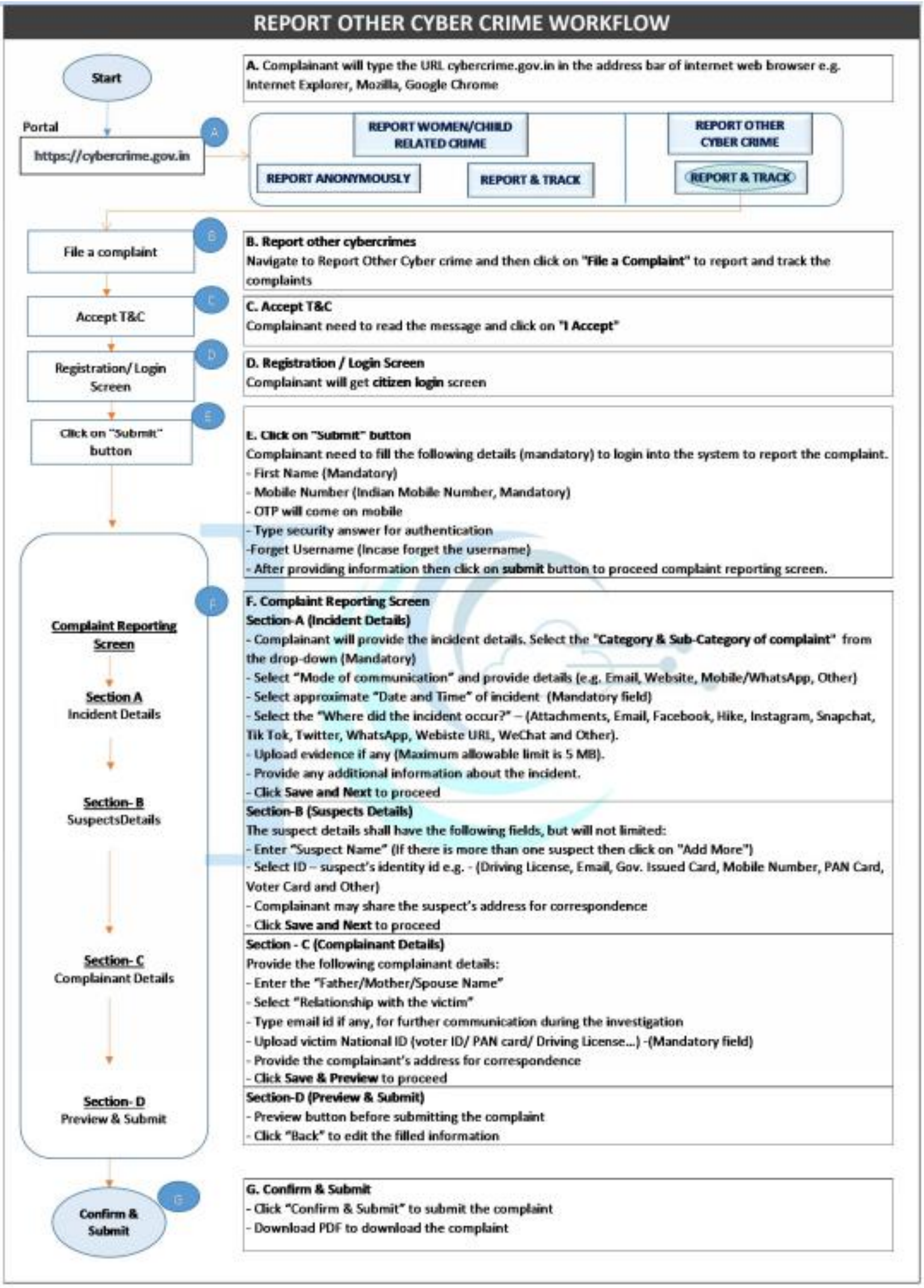
Maximum of 1500 characters - 1500 characters left

Save & Next

Feedback | FAQ | Contact Us | Website Policies | Disclaimer

Website Content Managed by Ministry of Home Affairs, Govt. of India. Best viewed in Mozilla Firefox, Google Chrome.

Note: One can also report anonymously.



REPORT OTHER CYBER CRIME WORKFLOW

A. Complainant will type the URL cybercrime.gov.in in the address bar of internet web browser e.g. Internet Explorer, Mozilla, Google Chrome

B. Report other cybercrimes
Navigate to Report Other Cyber crime and then click on **"File a Complaint"** to report and track the complaints

C. Accept T&C
Complainant need to read the message and click on **"I Accept"**

D. Registration / Login Screen
Complainant will get **citizen login** screen

E. Click on "Submit" button
Complainant need to fill the following details (mandatory) to login into the system to report the complaint.
- First Name (Mandatory)
- Mobile Number (Indian Mobile Number, Mandatory)
- OTP will come on mobile
- Type security answer for authentication
-Forget Username (Incase forget the username)
- After providing information then click on **submit** button to proceed complaint reporting screen.

F. Complaint Reporting Screen
Section-A (Incident Details)
- Complainant will provide the incident details. Select the **"Category & Sub-Category of complaint"** from the drop-down (Mandatory)
- Select "Mode of communication" and provide details (e.g. Email, Website, Mobile/WhatsApp, Other)
- Select approximate "Date and Time" of incident (Mandatory field)
- Select the "Where did the incident occur?" – (Attachments, Email, Facebook, Hike, Instagram, Snapchat, Tik Tok, Twitter, WhatsApp, Webiste URL, WeChat and Other).
- Upload evidence if any (Maximum allowable limit is 5 MB).
- Provide any additional information about the incident.
- Click **Save and Next** to proceed

Section-B (Suspects Details)
The suspect details shall have the following fields, but will not limited:
- Enter "Suspect Name" (If there is more than one suspect then click on "Add More")
- Select ID – suspect's identity id e.g. - (Driving License, Email, Gov. Issued Card, Mobile Number, PAN Card, Voter Card and Other)
- Complainant may share the suspect's address for correspondence
- Click **Save and Next** to proceed

Section - C (Complainant Details)
Provide the following complainant details:
- Enter the "Father/Mother/Spouse Name"
- Select "Relationship with the victim"
- Type email id if any, for further communication during the investigation
- Upload victim National ID (voter ID/ PAN card/ Driving License...) -(Mandatory field)
- Provide the complainant's address for correspondence
- Click **Save & Preview** to proceed

Section-D (Preview & Submit)
- Preview button before submitting the complaint
- Click "Back" to edit the filled information

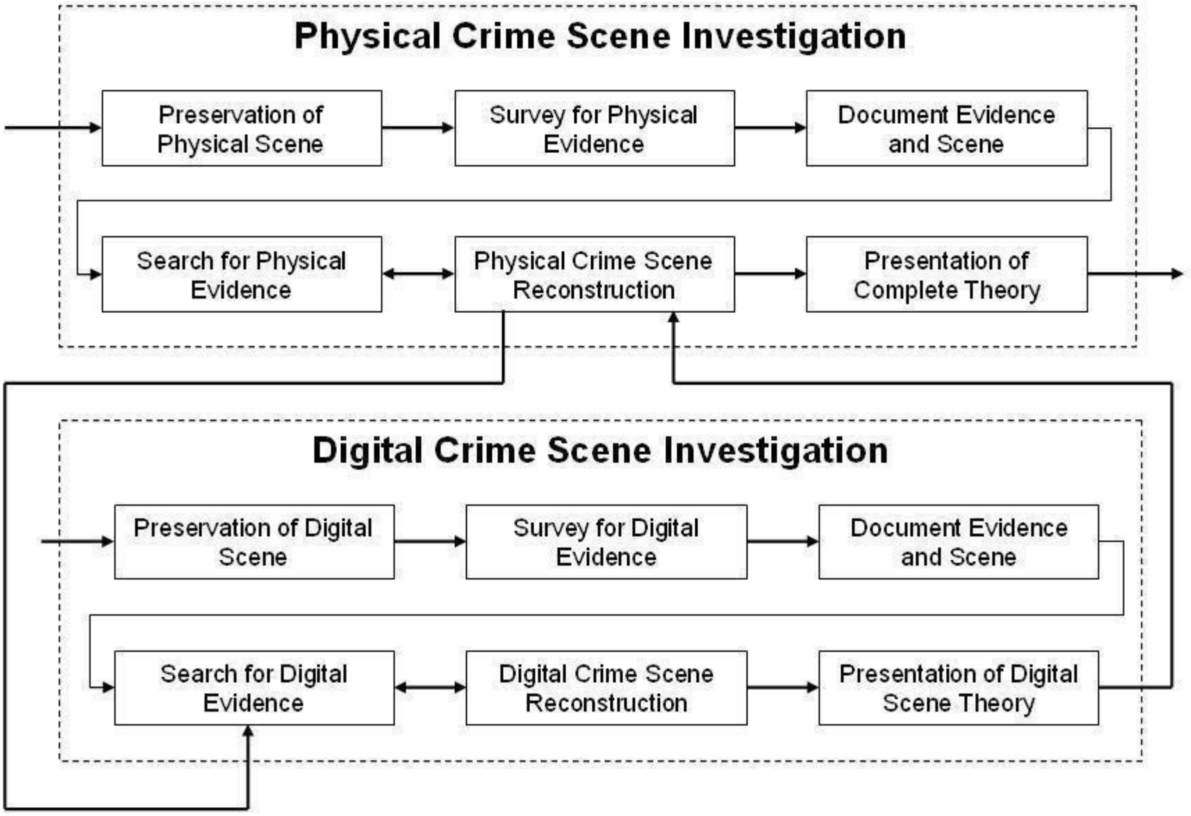
G. Confirm & Submit
- Click "Confirm & Submit" to submit the complaint
- Download PDF to download the complaint

Source: https://www.cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

One can report a cyber-crime by:

- Filing a written complaint in nearest, any Cyber Cell
- Lodging an F.I.R (First Information Report)
- Filing a complaint at https://www.cybercrime.gov.in/Accept.aspx

After filing of a complaint / F.I.R., the process of investigation, is hereby diagrammatically presented below:


Physical Crime Scene Investigation
Preservation of Physical Scene
Survey for Physical Evidence
Document Evidence and Scene
Search for Physical Evidence
Physical Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation
Preservation of Digital Scene
Survey for Digital Evidence
Document Evidence and Scene
Search for Digital Evidence
Digital Crime Scene Reconstruction
Presentation of Digital Scene Theory

Source: http://www.dynotech.com/articles/images/crimescene.jpg

In case the response has not been appropriate then the complainant can write to State / UT Nodal Officer and Grievance Officer, the details of which can be accessed here: https://www.cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx.

Recently, for Delhi only, a new feature "**Citizen Financial Cyber Fraud Reporting and Management System**" has been activated for prevention of money loss in case of Cyber Financial Fraud; for immediate reporting the complainant can Call 155260 (9 AM – 6 PM only) and further details can be accessed from 'Citizen Manual' under "Resources Section" at www.cybercrime.gov.in.

Prosecution for cyber-crimes

Some common cyber-crimes incidents which attract prosecution as per the applicable provisions of the IT Act, are provided herein below:

Online hate community

It is created for provoking a religious group to act or pass obnoxious/ objectionable remarks against a public figure or the country etc.

Applicable provisions:

Section 66A of IT Act + 153A & 153B of the Indian Penal Code (IPC)

Email account hacking

If a person's email account is hacked and offensive / indecent emails are sent to people who are in person's address book.

Applicable provisions: Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.

Web defacement

The Website's homepage is swapped with a defamatory or pornographic content/ page.

Applicable provisions: Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.

Cyber terrorism

The terrorists are using virtual & physical storage for hiding data & records of their illegal business.

Applicable provisions: terrorism laws apply + Section 66F & 69 of IT Act.

Phishing and email scams

It involves acquiring sensitive information fraudulently by masquerading as a reliable & legitimate entity.

Applicable provisions: Section 66, 66A and 66D of IT Act + Section 420 of IPC

The Indian Computer Emergency Response Team (CERT-In) is the national nodal agency established by the Ministry of Electronics & Information Technology (Meaty), Government of India, for responding to computer security incidents & securing the Indian cyber space. In the year 2019, CERT-In handled 3,94,499 incidents. The incidents handled were:

- Website Intrusion & Malware Propagation
- Malicious Code
- Phishing
- Distributed Denial of Service attacks
- Website Defacements
- Unauthorized Scanning activities and vulnerable service.

The CERT-In has executed a Memorandum of Understanding on cyber security co-operation with Finland, Estonia & South Korea, to strengthen & enable information sharing & collaboration for incidents resolution.[4]

The Meaty has also launched “Cyber Swachh Kendra”[5] (Botnet Cleaning and Malware Analysis Centre), to detect the botnet infections and create a secure cyberspace in India. This center is being operated by the CERT-In as per the provisions of Section 70B of the IT Act.

3.3. 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 excessive 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.[27]

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 cybercrime. Legalizing e-commerce is part of the law. This is, 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 cybercrime 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 cybercrime 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 cannot 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.

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

Chapter 4

4. IMPACTS OF CYBERCRIME ON INDIAN SOCIETY ANDECONOMY

In the most general form crime can be de-fined as the violation of law, especially a serious one Cybercrime is an unlawful act wherein the computer is either a tool or target or both. Cybercrime consists of specific crime dealing with computer and networks and facilitation of traditional crime using a computer. Cybercrime uses the unique feature of Internet namely the sending of emails, speedy publication of information through the web to any one the planet. These criminal activities can often be faster.

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 cybercrime using the Internet. Cybercrime 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 cybercrime, 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 are 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 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. '

4.1. 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.[28] '

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. 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

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

be a new wave in the future. Insects, viruses, are not considered quite mature compared to the probability of future attacks.

4.2. ECONOMIC IMPACT

Norton Cyber Crime has revealed that the in the United States, million 4 And more than a million people in cybercrime 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 because 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 cybercrime 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. 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.

4.3. IMPACT OF CYBERCRIMEON 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[29]. For instance, physical loss, a ruling in favour 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[30]. 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. 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 providing a way of identifying threats to security and assessing their severity. Based on 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

[29] Supra note 4

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

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.

3. 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 Femi stock price. "

Therefore, there is a need for a different approach to assess the risk of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself[31]. Moreover, managers aim to maximize a firm's market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value.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, areas adamantium-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

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

elongation Yogeeta facilities, such as the possibility of losing the intangible losses, intangible costs do not include violations because 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.

4.4. 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.

4.5. Impact on International Multilateral Partnership against Cyber Terrorism

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

Areas Ripe for Exploitation: National Security Modem military of most of the countries depends heavily on advanced computers. Information Warfare (IW) including network attack, exploitation, and defence, is not a new national security challenge, but since 9/11, it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration. The Internet has 90 percent junk and 10 percent good security systems, when intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of the residents of their own country. Most of such crimes have been originating in developing countries. The wide spread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

4.6. Cyber Crime and Its Effect on Society

4.6.1. impact of cyber hacking in India.

Cyber hacking does not mean no loss to human life because hackers are human being, and they are causing injury to human society. Especially Bhabha Atomic Research Centre servers and traffic control servers were hacked, which are direct examples of injury to human life. On 11th September 2001 and July 2005 recent attack on the USA and the UK are burning, painful and measurable instances in contemporary scenario which has impact of cyber barking and cyber terrorism. Those attacks are attacks to world not only to those countries. Therefore, our primary task must be the security measures in cyber world. Pakistani hacktivists are successfully defacing several Indian websites from 1999.44 Now-a-days it became common practice between hacker groups.

On 10th January 200145 R.K. Raghavan said it is very difficult to nail on Pakistani hackers because the Indian hackers are not conniving with the Pakistani law enforcers. Therefore, any prudent person can think about the kind of co-operation India may get from Pakistan. Hackers generally break-in and steal information from computer system by using software who have thorough knowledge of that software. In the year 200046 about 635 Indian websites were hacked. It was very complex phenomenon to even identify hackers. People of India are most of the times illiterate and reluctant about this crime and complaint. **Mr. Dewang Mehta**, **President of NASSCOM47** says that the lack of uniform laws against cybercrimes involving abuse of computer systems made prosecution of cross-border hackers difficult.

DELHI HACKERS' CASE. Delhi Police arrested two hackers on 6th February 2001.48 It was the most breaking news in India because two people were arrested by the Delhi Police for allegation of hacking a website. This was probably the first case in India where accused were arrested as said by Police Commissioner Rajan Bhagat. Both the hackers were detained for allegedly blocking the website named goZnextjob.com. This website provides support and information to prospective employers and jobseekers. The accused posted a message on that website declaring that it was closed but it was very much open. The hackers were sent to judicial custody for 14 days as they were charged under s. 406 of Indian Penal Code 1860 i.e., criminal breach of trust, and s. 66 of the Information Technology Act 2000 i.e., offence of hacking. Though they were denied bail by the Metropolitan Magistrate on 8th February 2001 after they were arrested on 6th February 2001; on 12th February 2001 **Additional Sessions**

Judge of Delhi, **Mr. P.K Gauba** granted bail to those two hackers who were the partners of software solutions **Mr. Amit Pasani** and **Mr. Kapil Juneja**.

In December 200149 Indian websites of AIIMS, the Atomic Energy Research Board, Delhi High Court Bar Association etc. were hacked eventually. Victims were busy developing their internal system, anti-virus software and firewalls rather than reporting the police. Perhaps they wanted to avoid negative publicity and they thought that it may deter their potential customers. Government was under false sense of security about companies, netizens, and websites. This is the scenario worldwide. However, at the same time, detections, investigations, convictions for cybercrimes systems are in existence and functioning worldwide. In India, police personnel are undergoing intensive training about prevention and control of hacking and other cybercrimes. India has constituted several Cyber Crimes Investigation Cells to the same end.

4.6.2.IMPACT OF CYBER FRAUD IN INDIA

The most complex challenges faced by the Government and law enforcement agencies since 1960s in the cyberspace are cyber fraud and other cybercrimes. This may be because the business world, financial sectors etc. were the most popular users of computer and internet from the early times of new multimedia technology.

The cyberspace becomes a media for the fraudsters where victims generally cannot recognize the accused. Therefore, cyber frauds become the most pervasive form of white-collar crime worldwide. On 7th April 1999, the online financial message of ‘yahoo! Inc.' was posted 'buyout news' that the 'pair gain'1 was being taken over by an Israeli company. Immediately after this news the company's publicity traded stock shortcoming was more than 30%. Subsequently the false story came out publicly. But by that time the company suffered significant financial loss and this incident caused financial loss to many investors. This is one instance of online fraud. The accused Raligh ofthe North Carolina was arrested by Federal Bureau of Investigation (FBI) through an internet protocol address which was used by the accused. The accused was thereby charged with securities fraud.

NEW DELHI ONLINE TRADERS CASE. One breaking news published b; Times News Network alarming people about hackers whack online trading of shares. The CBI controlled this case of cybercrime where the password of a Ghaziabad: based online trader was hacked by a hacker and caused loss of about Rs. 5 lakhs.

The traders were frequently cheated by such hackers who got trader accounts information and misused it by bringing shares at very high price and subsequently selling that share at very low prices causing financial losses. In Ghaziabad case the 'cyber-breaking' was noticed when debt became Rs. 5 lakhs against trader’s account. This was registered on 29th June by the CBI under s. 419 ofthe Indian Penal Code 1860 and s. 66 other Information Technology Act 2000. The hacker invested Rs. 5 lakhs from victims account 1 his own account. The Cyber Crime Cell of the CBI arrested 2 accused £ Bhavnagar, Gujarat.

HYDERABAD Rs. 20 CRORE DATA CONVERSION FRAUD. Mr. C. Suresh the Managing Director of Vin Sri InfoTech and owner of the website InfoTech Pvt. Ltd. had started his business in 1997 of data conversion, to give data entry works; to provide services for data entry, medical transcription, management, and e-Books etc. In 2002 January he fraudulently received Rs. 2.5 lakh (apex.) non-refundable deposits from each of the clients giving false promise to give data entry work. And in February 2003, when cheques issued to his clients by him were not cleared rather dishonoured because funds were not available; his clients started demanding either refund of their deposited amount or clearance of their bills and to provide work. But Mr. C. Suresh, the accused was silent. Therefore, his clients (about 1,500) went to police and lodged separate complaints. Then he was arrested from Secundrabad on the charge of cyber fraud i.e., about Rs. 20 crore data conversion fraud.

The Central Crime Station (CCS) investigators said that six more cases have been registered on cyber fraud and again police have identified at least 20 fake data conversion companies after this incident. Even in the branch offices the brokers collected falsely Rs. 10,000 to Rs. 50,000 from each client by giving such false promises.

Chapter 5

5. The Judicial Approachtowards Cybercrime Laws and Regulations in India

Jurisdiction - The Concept The effectiveness of a judicial system rests on bedrock of regulations, which define every aspect of a system's functioning; and principally, its jurisdiction. A court must have jurisdiction, venue, and appropriate service of process to hear a case and render an effective judgment. Jurisdiction is the power of a court to hear and determine a case. Without jurisdiction, a court's judgment is ineffective and impotent. Such jurisdiction is essentially of two types, namely subject matter jurisdiction and personal jurisdiction. Subject matter jurisdiction is defined as the competence of the court to hear and determine a particular category of cases. It requires determination whether a claim is actionable in the court where the case is filed, and personal jurisdiction is simply the competence of the court to determine a case against a particular category whether the person is subject to the court in which the case is filed. These two jurisdictions must be conjunctively satisfied for a judgment to take effect. It is the presence ofjurisdiction that ensures the power of enforcement to a court and in the absence ofsuch power, the verdict of a court, is of little or no use. Under the traditional legal systems, the transactions between two parties when both are situated in distinct territorial jurisdictions, are governed either by the laws of the country which the parties agree will govern the transactions, or by the laws of the country in which the transactions are performed. These traditional notions ofjurisdiction have no relevance to the activities carried out over the internet, as the internet has no relevance to the location. The internet can allow persons from geographically distinct locations and jurisdictions to transact with each other, with little or no comprehension of the consequences of their actions in the jurisdictions within which they are operating. In fact, the absence of geographical limitations could lead the incautious to believe that the laws of their home state apply to their actions, when in fact they are in inadvertent violation of the laws of another state.

5.1. **Jurisdiction** - The Concept

The effectiveness of a judicial system rests on bedrock of regulations, which define every aspect of a system's functioning; and principally, its jurisdiction. A court must have jurisdiction, venue, and appropriate service of process in order to hear a case and render an effective judgment. Jurisdiction is the power of a court to hear and determine a case. Without jurisdiction, a court's judgment is ineffective and impotent. Such jurisdiction is essentially of two types, namely subject matter jurisdiction and personal jurisdiction. Subject matter jurisdiction is defined as the competence of the court to hear and determine a particular category of cases. It requires determination whether a claim is actionable in the court where the case is filed, and personal jurisdiction is simply the competence of the court todetermine a case against a particular category whether the person is subject to the court in which the case is filed. These two jurisdictions must be conjunctively satisfied for a judgment to take effect. It is the presence ofjurisdiction that ensures the power of enforcement to a court and in the absence ofsuch power, the verdict of a court, is of little or no use. Under the traditional legal systems, the transactions between two parties when both are situated in distinct territorial jurisdictions, are governed either by the laws of the country which the parties agree will govern the transactions, or by the laws of the country in which the transactions are performed. These traditional notions ofjurisdiction have no relevance to the activities carried out over the internet, as the internet has no relevance to the location. The internet can allow persons from geographically distinct locations and jurisdictions to transact with each other, with little or no comprehension of the consequences of their actions in the jurisdictions within which they are operating. In fact, the absence of geographical limitations could lead the incautious to believe that the laws of their home state apply to their actions, when in fact they are in inadvertent violation of the laws of another state.

5.2. **Jurisdiction**over internet

The whole trouble with internet jurisdiction is the presence of multiple parities in various parts of the world who have only a virtual nexus with each other. Then, if one party wants to sue the other, where can he sue? Traditional requirements generally encompass two areas-firstly, the place where the defendant resides, or secondly, where the action arises. However, in the context of the internet, both these are difficult to establish with any certainty. Considering the lack of physical boundaries on the internet, is it possible to reach out beyond the court’s geographic boundaries to haul a defendant into its court for conduct in "Cyberspace"? Issues of this nature have contributed to the complete confusion and contradictions that plague judicial decision ininternet jurisdiction. Considering the lack of physical boundaries on the internet, is it possible to reach out beyond the court’s geographic boundaries to haul a defendant into its court for conduct in Cyberspace.

The decision in Cybersell, Inc. CyberSell, Inc, is a typical example of a fact situation involving a conflict over jurisdiction. The case involved a service mark dispute between two corporations, One at Orlando and another in Arizona. The court had to address eh issue to whether the mere use of a website by the Florida Corporation was sufficient to grant the court, in Oriando jurisdiction. The court answered the question in the negative, focusing on traditional analysis established by the US Supreme Court concerning the due process aspects ofpersonal jurisdiction: "It is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protection of its laws."

The decision in Cybersell, Inc. CyberSell, Inc, is a typical example of a fact situation involving a conflict over jurisdiction. The case involved a service mark dispute between two corporations, One at Orlando and another in Arizona. The court had to address eh issue to whether the mere use of a website by the Florida Corporation was sufficient to grant the court, in Oriando jurisdiction. The court answered the question in the negative, focusing on traditional analysis established by the US Supreme Court concerning the due process aspects ofpersonal jurisdiction: "It is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protection of its laws."

One early case, which appears to have set the standard to be followed, is CompuServe, Inc. v. Patterson. This case involved declaratory suit filed by the plaintiff in response to an elevation oftrademark infringement by the defendant. Finally, the court did not hold that CompuServe may sue a regular subscriber for non-payment of the service in Ohio regardless of the subscriber's residence. This language has been interpreted to suggest passive use of the Web will not confer jurisdiction in the service s home state, yet active use of the online service, e.g., solicitation and advertisement of products and services through the online service increase the likely hood of being subject to jurisdiction.

Sending E-mail to an individual whose location known to the sender is like sending regular mail addressed to an individual at a known location. Thus, one could argue that there is a little reason not to exercise jurisdiction over the sender in the location to which the e-mail was sent. Thus, in Resuscitation Technologies Inc. v. Continental Health Care Corp. the NewYork defendant had extensive communication with the Indiana plaintiff, including 80 emails. The court in Indiana found the level of activity directed to Indiana was substantial, thus giving Indiana personal jurisdiction over the defendant.

E-mail may also contribute to a finding of personal jurisdiction. Many websites allow users to contact a business or individual via e-mail. Although e-mail alone probably will not confer jurisdiction, its routine use may suffice to find jurisdiction in the same way that frequently sending or receiving regular mail from a state lead to jurisdiction. For instance, in Scherr v. Abrahams, the court denied jurisdiction even though the defendant's site allows users to contact him via e-mail and he sent his publication to them via e-mail. However, as cases like Cody v. Ward, demonstrate, courts will simply look at the volume of e-mail exchanged to grant jurisdiction. Again, as witnessed above, in presence of contacts besides the internet, the courts are fairly comfortable in granting jurisdiction. Such jurisdiction may even extent to a "general" nature, subjecting the party to suit in a forum on a ground of action not related to the internet itself. In general, courts applying the rules of person jurisdiction to cyberspace have required "something more" than mere electronic contacts to support an exercise of jurisdiction. In addition to electronic contacts, there must be some act purposefully directed towards the forum state. Thus, courts have focused on the purposeful ailment prong ofthe due process, minimum contacts test. Though, in exceptional cases courts have conferred jurisdiction in the absence of any connection beyond a web site, this is unlikely to be sustained in the long run. It is, firstly, impossible to enforce decision ofthis nature in every case, considering that often the website owner may be in a hostile country, or in a jurisdiction that simply refuses to recognize the jurisdiction ofthe court issuing the original decree. Secondly, such an approach would cause considerable inconvenienceto any large-scale form of e-business and could contribute to stagnation ofthe internet something that must be avoided at all costs.

5.3. Indian Context

The information Technology Act, 2000 passed in India, is illustrative ofthe prevailing confusion around jurisdiction in the context of the internet. Section 1 of the Information Technology Act, 2000, deals with the issue of applicability of this new law. Normally, the applicability oflaws within India can be broadly divided into the following major categories.

Laws applicable to all states ofIndia

Laws applicable to Jammu and Kashmir.

Laws applicable to entire country

The Act begins by saying, in cause (2) to section 1, that it shall extend to the whole of India and, save as otherwise provided in the Act, it applies also to any offence or contravention there under committed outside India by any person. Clause (2) ofsection 75 ofthe Act simply states that,"... this Act shall apply to an offence or contravention committed outside India by any person ifthe act or conduct constituting the offence or contravention involves a computer network located in India". Provisions ofthis nature are unlikely to be effective for a few reasons. Firstly, it is unfair to suggest that the moment an Indian computer system is used, an action defined by Indian laws an "offence" would be subject to jurisdiction ofIndian courts. To illustrate, let us consider a web site located in a foreign country. The site may host content that would be perfectly legal in its home country but may be considered offensive or illegal in India. If an Indian chooses to view this site on a computer situated in India, does that mean the site can be prosecuted in an Indian court? This would appear to violate principles of justice. As explained earlier, the judicial trend of examining the amount of activity that a site undertakes in a particular jurisdiction is a far more equitable method to determine jurisdiction. Further, even if Indian courts are to claim jurisdiction and pass judgments based on the principle expostulated by the IT Act, it is unlikely that foreign Courts will enforce these judgments since they would not accept the principles utilized by the Act as adequate to grant Indian court’s jurisdiction. This would also render the Act ineffective.

The Indian jurisprudence regarding jurisdiction over the internet is almost non-existent. In the first place, as the result ofthe strongly unitary model of government prevalent in India, interstate disputes never assume the level ofprivate international law. Hence, there has been precious little by way of development of private international law rules in India. Furthermore, there have been few cases in the Indian courts where the need for the Indian courts to assume jurisdiction over a foreign subject has arisen. Such jurisprudential development would however, become essential in the future, as the internet sets out to shrinks borders and merge geographical and territorial restrictions on jurisdiction. It is worthwhile to consider the issue ofjurisdiction at two levels. In the first place, given the way foreign courts assume jurisdiction over the internet related issues (as evidenced by the cases discussed above), the consequences of a decree passed by a foreign court against an Indian citizen must be examined. In other words, under what circumstances can the decision of a foreign court be enforced against an Indian citizen or a person resident in India? It is necessary to examine the circumstances under which the Indian court would assume jurisdiction over foreign citizens to better understand the rights of an Indian citizen who is affected by the act of a foreign citizen.

5.4. Effect of foreign judgment

Under the code of Civil Procedure, the effect of foreign judgment has been spelled out under the provisions of section 13, which reads as follows:

When foreign Judgment not conclusive - A foreign judgment shall be conclusive as to any matter thereby directly adjudicated upon between the same parties or between parties under whom they or any of them claim litigating under the same title except

where it has not been pronounced by a court of competent jurisdiction.

where it has been given on the merits of the case

where it appears on the face ofthe proceedings to be founded on an incorrect view of international law or a refusal to recognize the law of India in cases in which such law is applicable.

where proceedings in which the judgment was obtained are opposed to natural justice.

where it has been obtained by fraud; where it sustains a claim founded on a breach of any law in force in India.

Except for the six grounds specifically mentioned in the section, the Indian courts are bound to accept the decree of a foreign court as being conclusive. In order to enforce a foreign judgment, care must be taken to ensure that the judgment is not flawed in any ofthese ways. The language ofthe section clearly says that ifthe foreign court did not have jurisdiction over the matter, any decree passed by such a court would not be conclusive, as far as an Indian court is concerned. In various cases, the court has stated that where there has been voluntary consent to submit the jurisdiction of the court, the court would be recognized internationally to have competent jurisdiction over the matter and such jurisdiction would be binding. This principle is grounded on the foundation that a party having taken a chance of a judgment in his favour by submitting to the jurisdiction of the court, should not be allowed to turn round when the judgment goes against him to say that the curt had no jurisdiction. As a corollary, in the event an ex -Partee decree is passed by a court, in a matter where the person against whom the decree is passed, does not contest, or even appear in the court, the party cannot be said to have submitted to the jurisdiction ofthe court. The mere fact that the decision was passed ex-party, does not constitute sufficient grounds for declaring that the relevant court did not have jurisdiction, as will have to be seen whether the decision was merely passed as a formality or after a consideration of the plaintiff's case.

This position of law assumes significance in relation to the judgment of foreign courts over internet related disputes as in most such litigation, the main argument on behalf of the defendant is that the foreign court has no jurisdiction totry the matter. In the first place, it appears that a decree of a foreign court in a personal action., that was passed in absinthium an in respect of which the defendant did not even appear before the foreign court, could not be deemed to have been passed by a court of competent jurisdiction. This apparently opens the doors for Indian defendants to avoid the consequences of foreign decisions by staying away from the forum where the proceedings are taking place. Not being present at the trial, the decision of the court cannot be enforced against them in India. However, courts in India have not stuck to this narrow view and have at times enforced the ex-party decrees of foreign courts, where the decision has been arrived after a consideration of the evidence and where the proceedings have in general not taken place in a summary manner.

An important aspect is the fact that the decision of the foreign court must have been taken strictly in accordance with the principles of natural justice. It is well settled that a mere error in procedure in a foreign court will not affect its conclusive nature under section 13 of CPC if error in procedure does not amount to a violation of natural justice under section 13(d) CPC. There is no doubt, though that the nature of the violation must be substantial and not minor violation of natural justice. So also, where the judgment ofthe court has been obtained by fraud, the decree is liable to be set aside. However, in these matters, it is more relevant to consider whether the curt has obtained jurisdiction by fraud, rather than to examine whether the decision on the merits of the case was so obtained.

Finally, the last sub-section ofsection 13, states that the foreign judgment is not conclusive, ifthe judgment sustaining the claim is founded on a breach ofIndian law. Without putting too fine a point on it, the import of this section is merely this: where a dispute is governed by Indian law, the final judgment of the foreign court should not be in violation of Indian law. Thus, where the claim is not based on Indian law and where the court has accepted the plea that the law governing the dispute is not Indian law, no objection can be taken to the judgment under section 13(l)(c) on the grounds that it sustains a claim based on Indian law. Thus, the courts in India are not averse to upholding the decree of a foreign court and can, in fact only hold the decree of a foreign court to be non-conclusive, ifsuch a decree does not fulfil the criteria set out in section 13 of the CPC. Thus, in the event a decree is passed against and Indian citizen in respect of any perceived breach of the laws of another state, the decree will be upheld in India, against the Indian citizen, provided it does not suffer from any of the infirmities listed under section 13.

Coming to the primary issue ofjurisdiction over the internet, in the event a foreign court passes extra-territorial judgment over a citizen of India, the case law examined above would clearly indicate that the courts in India would have no hesitation in upholding a reasoned and sound decision of a foreign court. Indian citizens, who establish a presence on the internet would therefore need to be careful to follow the principles of law, set out in international jurisdiction to avoid prosecution under those laws. It is therefore not enough to be mindful of local laws alone. Any venture on the internet appears to be open to challenge from virtually any jurisdiction and form any country that has internet access.

Jurisdiction ofIndian courts over foreign citizens or residents Cyber Crimes: The Judicial Response 194 Under section 16 of the CPC, a suit in respect of immovable property or in respect ofmovable property that is actually under attachment or restraint, is required to be instituted in the court within whose local jurisdiction, the subject matter is situate. It is therefore not possible for an Indian court to assume jurisdiction over immovable property situated within the jurisdiction of a foreign state.

5.5. Jurisdiction of Indian courts over foreign citizens or residents Cyber Crimes:

The Judicial Response 194 Under section 16 of the CPC, a suit in respect of immovable property or in respect ofmovable property that is actually under attachment or restraint, is required to be instituted in the court within whose local jurisdiction, the subject matter is situate. It is therefore not possible for an Indian court to assume jurisdiction over immovable property situated within the jurisdiction of a foreign state.

Under section 19 of the CPC, a suit for the compensation ofthe wrong done to the person or to movable property may be instituted either at the place or residence or the place of business of the defendant or at the place where the wrong was committed. However, the main section in the code dealing with the jurisdiction of Indian courts over matters relating to personal injuries or damage to movable property is section 20 which has been extracted here.

Others suits to be instituted where the defendant resides or cause of action arises - Subject to the limitations aforesaid, every suit shall be instituted in a court within the local limits of whose jurisdiction –

the defendant, or each of the defendants where there are more than one, at the time ofthe commencement ofthe suit, actually and voluntarily resides, or carries on business, or personally works for gains; or

where the cause of action, wholly or in part arises.

Explanation: A corporation shall be deemed to carry on business t its sole or principal office in India or, in respect of any cause of action arising at any place where it has also a subordinate office, at such place.

The principle behind this section appears to be that suit against a given person may be brought at the place where such person resides or at least has his place of business. This is apparently prompted by the rationale that the defendant, not being the person who instituted the suit should not be put to undue hardship in defending such a suit when the suit may not be maintainable at all. There is, however, another aspect to this section that may warrant study the jurisdiction of the court where the whole or part of the cause of action arises, as this could have some bearing on the jurisdiction of the Indian courts over internet disputes.

In essence, this section is the equivalent of the US Long-Arm jurisdiction provisions. It is a section that enables a court to assume jurisdiction over a dispute regardless of where the principals are resident or carrying on business so long as a portion or the cause of action' took place within the local jurisdiction. Cause of Action' has been defined as follows:

The cause of action is the whole bundle of material facts, which a plaintiff must prove to succeed. These are all those essential facts without the proof of which the plaintiff must fail in is suit.

A cause ofAction is a bundle of facts which, taken with the law applicable to them, gives the plaintiff a right to relief against the defendant. It must include some act, not cause of action possibly accrue. It is not limited to the actual infringement of the right sued on but includes all the material facts on which it is founded. It does not comprise evidence necessary to prove such facts, but every fact necessary for the plaintiff to prove to enable him to obtain a decree. Everything which if not proved would give the defendant a right to immediate judgment must be a part ofthe cause of action. However, it has no relation whatever to the defence which may be set, up by the defendant, nor does it depend upon the character of the relief prayed for by the plaintiff.

Cause of action means and includes every fact which it would be necessary for the plaintiff to prove, if traversed, in order to support his right to the judgment and has no relation whatever to the defence that may be set up by the defendant, nor it does depend upon the character of the relief prayed for by the plaintiff. It refers to the media upon which the plaintiff asks the court to arrive at a conclusion in his favour.

The test for determining whether an allegation forms part of the cause of action is whether the plaintiff must prove the same to support his right to judgment ofthe court.

However, matters that are not necessary to be proved by the plaintiff for the plaintiff to succeed in his claim, will not form a part of the cause of action and thereof cannot confer jurisdiction on the court within whose territorial jurisdiction it occurred.

So also, the cause of action should be antecedent to the suit and an expectation of the performance of a contract within a particular jurisdiction cannot constitute a part of the cause of action.

Having said this, there is no requirement that the whole, or substantially the whole of the cause of action must arise within the jurisdiction of a court, to confer jurisdiction. It cannot be contended that because a very small fraction of the cause of action accrued within the jurisdiction of a court, the plaintiff would not be entitled to institute the suit in that court. Even a fraction of the cause of action is a 'part' of it its percentage to the whole cause of action is immaterial. However, where no portion ofthe cause of action arises, a suit cannot be filed under section 20(c) of the CPC.

The applicability of the Indian case law discussed above in the context of transactions on the internet, it was held that a court in this country has jurisdictionover a non-resident foreigner, although he has not submitted to its jurisdiction, provided the cause of action had arisen wholly or in part within its jurisdiction. It is thus clear that the Indian courts will assume jurisdiction over a matter if, even a part ofthe cause of action ofthe dispute arose within the jurisdiction ofthe specified court. What remains to be determined is what, in the context ofinternet transactions, would constitute a part of the cause of action. In this, we can take a cue from the cases decided by the courts of USA where similar ingredients (Long-Arm jurisdiction) had to be proved in order to determine the jurisdiction of the courts.

We have seen that the US courts have, on occasion, held that the mere fact that an individual can access a given site on the internet from within the jurisdiction ofthe court before which the suit was preferred, is justification enough for the court to assume jurisdiction over the dispute. Translated into terms applicable to a trial before an Indian judge, this principle could be interpreted to state that the fact that a site is capable of being viewed or read from within the jurisdiction of court within which the suit is filed, is an indication that a part ofthe cause of action arose in that jurisdiction and therefore a suit can be maintained in that court. There are similarities between the Long-Arm principles used by the US courts and cause of action' test used by the Indian courts. It remains to be seen whether these similarities would allow the Indian courts to analyse the development ofinternet laws in the US and to use this development of case law in their own judgment on matters involving internet transactions. There has also been considerable discussion as to what constitutes the cause of action in respect of a contract. It has been held that the cause of action arises in each of the following places:

where the contract was made.

where the contract was to be performed.

where the consideration under the contract was to be paid.

In most well drafted commercial contracts, the parties specify the jurisdiction of courts in the event of a dispute and agree to submit to the jurisdiction of a particular court. Where such a decision has been made, conferring jurisdiction on one of two courts that could have assumed jurisdiction over the dispute, the courts will normally accept the agreement between the parties to submit to the jurisdiction of the other court. However, the compulsive jurisdiction of a given court should be clear, unambiguous, and explicit and unless the jurisdiction ofthe courts is expressly excluded using words such as 'alone', 'only' or 'exclusive' the mere declaration that a particular court has jurisdiction over a contract would not suffice. Furthermore, where the court chosen by the parties under the contract would not, under the provisions of the CPC, have had jurisdiction over the subject matter of the dispute, in such cases, the choice ofsuch a court by the parties in accordance with the terms of the contract would not be enough to grant the court jurisdiction over the matte. Thus, the parties cannot by contract award jurisdiction where no such jurisdiction is statutorily available but may, by express declaration, choose a given jurisdiction in preference of another, provided jurisdiction could validly adjudicate over the subject matter ofthe dispute.

Finally, the execution offoreign arbitral awards is also the subject matter of jurisdictional concern. There has been considerable consensus in the world on this and the New York convention, 1958 specifies the way participating countries will deal with the recognition of foreign arbitral awards. The Government of India has notified several of the New York convention countries and passed the Foreign Awards (Recognition and Enforcement) Act 1961, in respect ofthe recognition of foreign awards. The newly enacted Arbitration and Conciliation Act 1996, at Chapter I of part II, lays down the current law relating to the enforcement of foreign arbitral awards.

5.6. Criminal Law

While the jurisdiction of the courts over civil matters is capable of different interpretation in the manner discussed above, in case of criminal action, the jurisdiction of the court arises on the basis of the location of the victim of the crime, or the actus reus Since the internet is everywhere, the commission of a crime by an individual by, for example, posting material to the internet results in this criminal act being simultaneously being committed everywhere on the internet. Thus, defamatory statements posted to news groups on the internet are accessibly by persons the world over, who have access to the internet. It is not too extreme to imagine that as a result of a posting to the internet, a user in the worst-case scenario, find himself the subject of an extradition request from a foreign government.

In the context ofthe Indian courts there is very little to offer in modification of the statement oflaw above. Chapter XIII of the Code of Criminal Procedure 1973 deals with the jurisdiction of courts in respect of criminal matters. It has been structured in such a manner as to enlarge as far as possible, the range oflocations in which the offence may be tried to minimize impediments to prosecution based on technical objections (such as the want of territorial jurisdiction). Ordinarily, the jurisdiction of the court relates to the place where the offence is committed. Section 177 reads as follows.

177. Ordinary place of inquiry and trial - Every offence shall ordinarily be inquired into and tried by a court within whose jurisdiction it was committed.

It is pertinent to note that this section does not purport to restrict territorial jurisdiction. It operates as a general provision that sets out where the offence may be tried ordinarily, without laying down exclusions to jurisdiction. It adopts the English common law position that crimes are essentially local and should be tried only by the local courts within whose jurisdiction they are committed. However, the inclusion of the term 'ordinarily' implies that the legislature is competent to provide for the trial of offences under the Penal Code otherwise than as prescribed under section 177. Proceedings along this line of analysis, the next question is whether the institution of proceedings before an inappropriate forum would in any way nullifies the proceedings. Section 462 reads as follows speaks of the relative insignificance of territorial jurisdiction.

462. Proceedings in wrong place - No finding, sentence or order of any Criminal court shall be set aside merely on the ground that the inquiry, trial, or other proceedings in the course of which it was arrived at or passed, took place in a wrong session, division, district, sub-division or other local area, unless it appears that such error has in fact occasioned a failure ofjustice.

The general rule of jurisdiction laid down in section 177 is subsequently sharpened in the following section. Section 178 deals with situations where there is uncertainty as to the local area within which the crime was committed.

5.7. SOME IMPORTANT CASES CONCERNING CYBER-CRIMES IN INDIA

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

5.7.1. ARIF AZIM CASE

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

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

The appellant is a prosecution witness in S.C. No. 9 of 2004 wherein respondents 2 to 6 are the accused facing trial for offences punishable under Section 67 of Information Technology

Act. 2000 r/w Section 6 of Indecent Representation of Women (prohibition) Act. 1986. Under Section 5 & 6 of Immoral Traffic (Prevention) Act. 1956. Under Section 27 of Arms Act. 1959. and Sections 120(B). 506(ii). 366. 306 & 376 I.P.C. The said trial relates to exploitation of certain men. and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos. and videos in various acts of sexual intercourse. and thereafter selling them to foreign websites. The said session's trial came to be allotted to the foreign websites. The said Session's trial came to be allotted to the V Fast Track Court. Chennai which is presided over by a lay Judge. When the said trial before the V Fast Track Court was pending certain criminal revision petitions came to be filed by the accused against the orders made by the said court rejecting their applications for supply of copies of 74 Compact Discs (CDs) containing pornographic material on which the prosecution was relying. The said revision petitions were rejected by the Madras High Court by its order dated 13th February. 2004 holding that giving all the copies of the concerned CDs might give room for copying such illegal material. and illegal circulation of the same. however, the court permitted the accused persons to peruse the CDs of their choice in the Chamber of the Judge in the presence of the accused. their advocates. the expert. the public prosecutor. and the Investigating Office. and observed that the case be transferred to another court by way of competent jurisdiction presided by a male officer at the option of the sessions judge. and taking the same the accused filed a revision petition for transferred to Fast track 4 court presided by the male officer. and the Appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer. and that the lady sessions judge did not object or the trial of the case. and the Appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer. and that the Lady sessions judge did not object to the trial of the case in the fast track 4.22. and the high court has erred in transferring the case. and the Appellant was not given any opportunities of being heard before the alleged transfer. The learned counsel for the respondents contended that the Appellant learned though erred as witness is for all purpose an accused herself. and law officer appearing in the case had expressed their embarrassment in conducting the trial before a lady Presiding Officer. and even though the Presiding Officer did not expressly record her embarrassment. it was apparent that she to wanted the case to be transferred to another court. therefore. this Court should not interfere by way of the order of transfer. It was held that this appeal must be allowed in the sessions case No. 9 of 2004 now transferred to the IV Fast Track Court Chennai be Transferred back to the V Fast Track Court. Chennai.

5.7.3. RITU KOHLI CASE - AN IPC CASE

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

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

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

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

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

5.7.5. STATE OF MAHARASHTRA V. ANAND ASHOK KHARE

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

5.7.6. STATE OF UTTAR PRADESH V. SAKET SINGHANIA

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

5.7.7. STATE V. AMIT PRASAD

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

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

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

5.7.9. STATE OF DELHI V. ANEESH CHOPRA

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

5.7.10. THE ARZIKA CASE

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

5.7.11. STATE OF TAMIL NADU V. DR L. PRAKASH

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

5.7.12. THE AIR FORCE BAL BHARTI SCHOOL CASE

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

CHAPTER-6

CONCLUSION AND SUGGESTION

Cybercrime is no longer an 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 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 cannot 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

SUGGESTIONS: -

Future Trends

One of the biggest concerns is that if there is a hack into the critical systems in government, companies, financial institutions etc? This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently. the internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the risk of money laundering through over-invoicing and under-invoicing is likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases. Online gambling also makes it possible to move money especially to offshore financial centres. Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous. Because mainly information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could argue in favour of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crimes. Some of the future trends predicted by Stephen Northcutt & Friend are briefly summarized in the following words. Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional parameter security measures. Social Media will provide the platform for the cyber-crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products, solving all these problems; some of them will stand out by allowing organizations to gradually control and monitor on-line social networking activities, while being mindful of users' privacy expectations. Humans are the weakest link, irrespective of the change in technology attackers know that they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in sophistication and numbers. Cyber attackers will always take the path of least resistance. Organizations and management will finally start doing something about it to secure the human. It is the sensitive issue for the people relying on iPhones for their day-today works that without issuing a warning that some worm will eat ail the iPhones and convert the Androids to bricks. However, the biggest issue seems to be applications with spyware. Even the apps that come loaded on the phones, are likely to phone home, it is a sure thing with third party apps. Memory scraping will become more common in the coming times. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys. The reason they are successful is that they get around Payment Card Industry, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, (PCI, GLBA, HIPAA, etc.), Security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resistant even after the fact. The data is encrypted on the hard disk, but again, the RAM likely maintains the clear-text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often miss configured, allowing malware to get into a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly. Audio Visual (AV) products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware. We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point of Sale (POS) systems. p51 Wireless adoption will continue brandling out into a larger number of purpose-focused protocols that fit Future Trends One of the biggest concerns is that if there is a hack into the critical systems in government, companies, financial institutions etc? This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently. p49 the internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the risk of money laundering through over-invoicing and under-invoicing is likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases. Online gambling also makes it possible to move money especially to offshore financial centres. Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous. Because mainly information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could argue in favour of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crimes. Some of the future trends predicted by Stephen Northcutt & Friend are briefly summarized in the following words. Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional parameter security measures. Social Media will provide the platform for the cyber-crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products, solving all these problems; some of them will stand out by allowing organizations to gradually control and monitor on-line social networking activities, while being mindful of users' privacy expectations. p50 Humans are the weakest link, irrespective of the change in technology attackers know that they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in sophistication and numbers. Cyber attackers will always take the path of least resistance. Organizations and management will finally start doing something about it to secure the human. It is the sensitive issue for the people relying on iPhones for their day-today works that without issuing a warning that some worm will eat ail the iPhones and convert the Androids to bricks. However, the biggest issue seems to be applications with spyware. Even the apps that come loaded on the phones, are likely to phone home, it is a sure thing with third party apps. Memory scraping will become more common in the coming times. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys. The reason they are successful is that they get around Payment Card Industry, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, (PCI, GLBA, HIPAA, etc.), Security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resistant even after the fact. The data is encrypted on the hard disk, but again, the RAM likely maintains the clear-text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often miss configured, allowing malware to get into a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly. Audio Visual (AV) products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware. We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point of Sale (POS) systems. p51 Wireless adoption will continue brandling out into a larger number of purpose-focused protocols that fit the needs of individual technology. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including ZigBee, Wireless HART and Z-Wave, as well as proprietary protocols. With this growing alternate wireless adoption, we are already seeing some of the past mistakes from earlier failed protocols repetition. Based on this exposure, and the trend of Wi-Fi failure and improvement, we will see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies. Security Continues to become the part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have”. The needs of individual technology. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including ZigBee, Wireless HART and Z-Wave, as well as proprietary protocols. With this growing alternate wireless adoption, we are already seeing some of the past mistakes from earlier failed protocols repetition. Based on this exposure, and the trend of Wi-Fi failure and improvement, we will see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies. Security Continues to become the part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have".

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

- There is a need of specific provision with a clear definition of 'cyber-crime'. We may say that 'cyber terrorism is the use of computer as tool or target to cause unpredictable violence and threat in the mind of general people about safety, security and in the mind of Government about national security, safety and interest etc
- Necessary steps must be taken to enable concerning bodies.
- Computer security and awareness training
- Continuing awareness and education regarding terrorist trends and methodologies
- Future readiness to defend against attacks
- Establishment of special court, e-court, in which complain can register on-line and on the date of hearing video conferencing should be used to avoid physical presence.
- Sensitive information should not be stored in the computer systems which are connected to the internet.
- Background of outsourcing agencies should be check prior to outsource any assignment, task to maintain information security inform of authenticity, confidentiality and authenticity of data
- Special training programmer for judicial officers to deal with cases related to cybercrimes.
- Effective use of intelligence gathered from all sources
- Ministries and departments have been advised to update IT systems and carry out regular audits to ensure an error-free system.

- Continued enhancement of resources which are essential to make Network mush secure and robust
- A techno-legal panel for provide training to various concerning departments.
- Public/Private interaction to get mixes approach of advanced technology and expert implementation mechanism
- Cyber ethics should be including as a subject in various curriculum at school and college level.
- Establishment of e-cops in those cities which contains economic importance
- There must be a specific police force to deal with cybercrimes in the country.
- Separate laws for each of the classification of cybercrime instead of amending the Information Technology Act.
- Creation of special enforcement agencies to deal exclusively with cyber laws.
- Government should impose a ban on websites that exclusively display pornography and hate speeches
- Promotion of Research and Development in the field of information security
- Last but not the least creation of awareness among each and every part of administration and society.

POLICIES RECOMMENDED FOR CYBER CRIME PREVENTION

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

i. Integrated policies are required to ensure the effective benefits from the Information system. The basic challenge and issue in the development of a cyber society, is the lack of financial and trained human resources.

ii. A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secure and free from cyber-crime and in reach to a common man

iii. Promotion of Research & Development in ICTs area and also in Human Resource Development as a core part of the system

iv. Up to date, common, and mutually supporting cyber laws should be there to fight with cyber-crime and protection of intellectual property rights towards the creation of cyber-crime free information society

v. Adoption of ICTs standards, regulation, and quality assurance to foster high quality and secure services and productions that keep competition in place for the benefits of the communities with in each country

vi. High levels of awareness among each part of the society should be there with regard to information security and cyber-crime.

vii. Effective mechanisms should be there for detection and prevention of cyber-crime and improving protection against, detection of, and responses to, cyber-crime, at the lower level itself

viii. Promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children

ix. Educate and involve the media professionals, citizen and then encourage them to increase public awareness. Engage large private sector corporations

x. Emphasis should be laid on less developed countries on effective systems, for protection against, detection of and responses to cyber-crime.

xi. Conduct national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and the private sector, using different media.

xii. Prevention is better than cure. Awareness regarding education and technical support to prevent e-crime is essential, but without discouraging the development of e-commerce.

xiii. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

xiv. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime

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

BIBLIOGRAPH

PRIMARY SOURCES:

List ofReport

- United NationCommission
- The CouncilofEuropeConvention
- The EuropeanCommission
- Asian ofSouth East Asian Nations
- Asia Pacific EconomicCorporation

Bare Act

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

SECONDARY SOURCES: ~

Articles:

- United Nation Draft (2013), Comprehensive study on cybercrimes, United Nation's Office on Drug and Crime Vienna, 2013 Retrieved from: http://www.un.org/en/index.html
- . National Crime Record Bureau (NCRB), Report 10, 2013 Retrieved form: http://ncrb.nic.in/
- Crime in India 2011 – Compendium (2012), National Crime Record Bureau, Ministry of Home Affairs, Government of India, New Delhi India Retrieved from: http://www.helplinelaw.com/1/CCII/cyber-crime-in-india-what-is-typesweb-hijacking-cyber-stalking.htm
- Buskin J. The Webs Dirties Secret. Wall Street Journal. Available: ~ProQuest: ~ ABI/ InformGlobal. 2000.
- Carter David L Computer Crime Categories. HowTechno Criminals Operate. FBI Law Enforcement Bulletin. July. 1994.
- VladimirGolubev. International cooperation in fighting cybercrime; Computer Crime research Centre