ABSTRACT

Computers and the Internet continue to pervade human life in everything from automobiles to kitchen appliances. With the invention of computers, has increased human dependency over the Internet. While we have gained manifolds advantages in terms of efficiency and management, it has also brought to the front many negative effects and disadvantages. Individuals or groups can now use Cyberspace to threaten International governments, or terrorize the citizens of a country. The crime of "cracking" can escalate into terrorism when an individual "cracks" into a government or military-maintained website. Cyber-terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge.

The information technology is a double edged sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions, as the case may be, of the person dealing with and using the technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, etc can bring only destructive results. These methods, however, may also be used for checking the authenticity, safety and security of one's technological device, which has been primarily relied upon and trusted for providing the security to a particular organisation. For instance, the creator of the "Sassier worm" has been hired as a "security software programmer" by a German firm, so that he can make firewalls, which will stop suspected files from entering computer systems. This exercise of hiring those persons who are responsible for causing havoc and nuisance is the recognition of the growing and inevitable need of "self protection", which is recognised in all the countries of the world. In fact, a society without protection in the form of "self help" cannot be visualised in the present electronic era. The content providers, all over the world, have favoured proposed legislations in their respective countries, which allow them to disable copyright infringers' computers. In some countries the software developers have vehemently supported the legislations which allow them to remotely disable the computer
violating the terms and conditions of the license allowing the use of the software. This position has, however, given birth to a debate about the desirability, propriety and the legality of a law providing for a disabling effect to these "malware". The problem is further made complicated due to absence of a uniform law solving the "jurisdictional problem". The Internet recognises no boundaries; hence the attacker or offender may belong to any part of the world, where the law of the offended country may not be effective. This has strengthened the need for a "techno-legal" solution rather than a pure legal recourse, which is not effective in the electronic era.

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

The roots of Internet can be traced from 1950s. In 1957 the Soviet Union launched the first Satellite, Sputnik I, triggering US president Dwight Eisenhower to create the ARPA agency in arms race. So, the evolution of internet is considered to be started with the use of ARPANET sponsored by the US military, which was set up in 1969.

The first communication took place between research Center at the University of California at Los Angles and the Stanford research Institute. The ARPANET was a joint venture of Massachusetts Institute of Technology and the American Department of Defense Advance Research Project Administration. It was a source to establish continued communication between remote computer resources in the event of war.
The communication links were confined to military, defense contractors and university laboratories involved in defense related research.

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

In the year 1990 the US authorities released ARPANET and transferred it to National Science Foundation (NSFNET).

In the year 1993 Time Berners developed the World Wide Web (www) in the European Laboratory for particle physics (CERN).

The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet explorer the preceding year. So, their browsers made Internet access possible from personal computers. From the year mid 1990’s various commercial Internet Services Providers (ISP) entered the market and offered the Internet connection through conventional telephone line.

Another key feature of the internet is that users do not have to reveal their true identity in order to send e-mail or post messages on bulletin boards. Users are able to communicate and make such postings anonymously or under psydo-nyms. This feature, coupled with the ability to access the internet in privacy and seclusion of one's own home or office and the interactive, responsive nature of communications on the internet, has resulted in users being far less inhibited about the contents of their messages resulting in cyber space becoming excessively prone to defamation.

The origins of hacking, in the sense of technological exploration and tampering, can be traced back to the phone phreakers of the 1960s and 1970s. The word journeyed from being understood as an adventurous achievement in the common parlance during its origin, to the most sought after, uncontrollable and mischievous criminal act in the present IT age. Hacking is described as "interacting with a computer in a playful; and exploratory rather than a goal-directed way". The word "hack" at the Massachusetts Institute of Technology (MIT) usually refers to a clever, benign, and "ethical" prank or practical joke, which is both challenging for the
perpetrators and amusing to the MIT community (and sometimes even to the rest of the world). Thus, hacking, prima facie appears to be a harmless activity, indeed it is widely commended and acclaimed as an adventure on wires.

At its core, hacking refers to activities involved in attempting or gaining unauthorized access to IT systems. With the widespread proliferation of computing technology, and the networks connecting it together, systems have come to represent both attractive and readily available targets regardless of whether the motive is idle mischief or something more sinister. As a consequence, hacking has become one of the most recognised and feared threats in cyberspace. For example, from the 671 security executives and law enforcement officials questioned as part of the 4th Annual E-Crime Watch Survey (conducted by CSO Magazine, the US Secret Service, the CERT Program and Microsoft), 26 per cent considered hackers to have been the greatest threat to their organisation over the previous year (placing them at the top of the list, ahead of current and former employees, competitors and foreign entities). Indeed, the same respondents considered that an average of 22 per cent of the security incidents they had experienced in this period, had been targeted attacks seeking to hit them specifically.

Cyber pornography is believed to be one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most of the countries.

The then CJI K.G. Balakrishnan advocated placing “restrictions” on websites that exclusively circulate pornography and hate content. Earlier he suggested for outright ban on such websites but later on he added that it would not be right to place a “blanket ban” on all categories of websites.

Pornography is a verbal or visual representation of sexual acts, it is a portrayal of people as sexual objects for pleasure of others. Pornographic material is intended to arouse sexual stimulation. It can lead the masturbation, just like a novel or film can lead to laughing or crying.
Pornography is looked differently by different people. Academician believes that pornography is an expression of male culture through which women are commoditized and exploited, liberal view combines a respect for free speech with the principle of “a woman's body, a woman’s right”.

The controversy between freedom of speech expression and pornography had been a debatable issue since time immemorial. So, the responsibility lies on the lawyers, legislators and courts to determine the exact line by that, what is obscene and what is not can be determined. Pornography corrupts one's moral senses and instigates them to participate in various sexual offences. Pornography is nothing but marketing of women's sex. Women are shown as "objects" which are longing to get involved into sexual acts.

The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism".

Cyber-terrorism is starkly different from common Internet crimes like identity theft and money fraud in that it can involve use of technology to divert or destroy systems and infrastructure, cause injury or death and undermine economies and institutions. To accomplish their goals, cyber-terrorists target the computer systems that control air traffic, electric power grids, telecommunications networks, military command systems and financial transactions.

The world was shocked by the despicable attacks and loss of innocent life on Sept 11, 2001, carried out by 19 airplane hijackers on a suicide mission. But that tragedy, horrific as it was, could be dwarfed by just one or two skilled Internet users who don't even set foot in their target country. It is frightening to imagine the human and economic toll if the computer systems that control air traffic, nuclear power
plants or major dams were brought down or thrown into confusion by cyber-terrorists.

In 1997 Barry Collin coined the term cyber terrorism as “the intentional abuse of digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action”.

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.

Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grew from 1.4 million in 1999 to over 125 million users by 2013 end. Though the rate of growth has slowed subsequently, with Internet users now approximately above 100 million, exponential growth is again expected as Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India. Similar figures have also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter,
the two top social networking sites. An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India's top e-commerce retailer. It saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million).

1. Statement of the Problem

The real issue is how to prevent cyber crime. For this there is a need to raise the possibility of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenges in cyber crime cases include getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries. The police have to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is based on the evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals, but from our ignorance and what is needed is the will to fight it. The law is stricter now on producing evidence. Specially where electronic documents are concerned.

Under Indian Law, cyber crime has to be a voluntary and willful act or omission that adversely affects a person or property. The Information Technology Act 2000 provides the backbone for e-commerce and India's approach has been to look at e-governance and e-commerce primarily from the proportional aspects. Looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take into consideration the security aspects. In the present global situation where cyber control mechanisms are important, we need to push cyber laws. Cyber crimes are a new class of crimes to India due to rapidly expanding extensive use of internet. Police in India is trying to become cyber crime savvy and hiring people who are trained in the area. Many police stations in various parts of India have computers, which are connected to their respective head quarters. Cyber police stations are functioning in major cities all over the country. The pace of the investigations can become faster, judicial sensitivity, and knowledge need to
improve. Focus need to sensitize our investigators and judges to the importance of the system.

2. **Objective of the Study**

The objectives of the present study are as follows:-

i) The main object is to specify the e-danger. The legal world familiar with theft and murder but now it is smuggling to macro terrorism from selling secrets to subverting systems from hijacking to hackling. The face of time has undergone a big change, its definition has changed its modus operandi has changed and the perpetrators are no longer Lombroso's bearded and hard looking criminal but a white collar criminal a fiddler or by an egomaniac.

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

iii) Emphasis has been laid to educate the investigating officers, prosecutors and judges about the need to amend the existing provisions of penal law to ensure efficiency in prosecution and trials.

iv) Measures adopted by various countries including the U.S. and other western countries having a high standard of connectivity and convergences are more vulnerable to cyber crime. They have a good number of cyber acts. India too passed IT Act 2000 and other relevant Acts. The object is to analyse various legislations in this area and to explore the possibilities of a stricter legal framework.
Abstract

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

3. Hypothesis

The research carried on the following hypothesis;

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

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

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

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

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

iii) How the internet has become a dangerous area for the children’s and finally strategies nations are adopting in combating this crime.
iv) Despite adequate safeguards and number of legislations, the problem of cyber crime continues unabated because of the poor machinery in our country and the major problem of jurisdiction.

v) The problem is multi-fold and it covers the crime related to economy as well as other crimes such as pornography which has its basis. Certainly moral standards degraded which leads indecency and obscenity as well as other sexual crimes.

4. Research Methodology

Law is a normative science that is, a science which lays down norms and standards for human behaviour in a specified situation or situation enforceable through the sanction of the state. What distinguishes law from other social science is its normative character. This fact along with the fact that stability and certainty of law are desirable goals and social values to be pursued, make doctrinal research to be of primary concern to a legal researcher. Doctrinal research, of course, involves analysis of case law, arranging, ordering and systematizing legal propositions, and study of legal institutions. Doctrinal research creates laws through legal reasoning or rational deduction.

The present study is based on the doctrinal method of research. The researcher has conducted the study with the help of books, Articles, newspapers, gazettes, report of commissions, committees and judicial decisions available on the topic.

The present study apart from introduction, conclusion and suggestions is comprises of five chapters.

Introductions refer the problem of cyber crime and cyber terrorism in India. It contain the review of literatures that provide a bird’s eye view of the research conducted in the field of cyber crime and cyber terrorism. It also explain the statement of the problem, hypothesis formulated for the purpose as well the objectives of the study and methodology adopted to conduct the research work.

Chapter First deals with conceptual analysis of cyber crime. In this chapter history and evolution of cyber crime has been discussed in detail. Categories of sub crime and their sub categories also explained with the help of case laws.
Chapter Second is divided into two parts. First part deals with the defamation in which the position of various countries has been taken and the punishment as prescribed by different legislation of that particular country. The second part of this chapter is related to hacking. In this part various types of hacker has been discussed and the punishment prescribed by the law is also taken for the study. Chapter Third is devoted with the study of obscenity and pornography. In this chapter the researcher has attempted to discuss about the obscenity, pornography and its impact on children and adolescents. This chapter also highlights the porn business and the income there from in various countries. Chapter Fourth discusses cyber crime against government. In this chapter terrorism through the internet and the reasons why the terrorist choose this medium to terrorize the government in particular and peoples in general has been discussed. The protection mechanism is also suggested in this chapter, either through technological or by legislation medium. Chapter Fifth is devoted for legal and technological measures that has been suggested to combat the cyber crime and cyber terrorism. In this chapter various issues of internet, like the impact of market value, consumer trust, potential economic impact etc. has been taken into consideration. Through the analysis of these, the measures have been suggested for protection and improvement.

Lastly the researcher made a modest but sincere attempt to conclude the study of the cyber crime and cyber terrorism in India and also made some humble suggestions under the caption Conclusion & Suggestions.

Since users of computer system and internet day by day are increasing worldwide, it has become easy to access any information within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by netizens while using the internet which will assist in challenging this major threat of Cyber Crime.

The researcher observed that the benefits of electronic revolution have reached each and every nation of the world, most of the nations have not got the separate laws, mutual agreement and multilateral treaties between the nations to deal with the
problem of cyber law nor there any such international agreement, convention, declaration, protocol or resolution to deal with the cross border cyber crime. The absence of all these have made countries vulnerable to the threats of cyber crimes. Therefore an international agreement in order to deal with cyber crimes is urgently required. Cyber Crimes are the 'Crimes against 'Humanity', 'Crimes against Development' and above all 'Crimes against Civilization.' The problems associated with the use of malware are not peculiar to any particular country as the menace is global in nature. The countries all over the world are facing this problem and are trying their level best to eliminate this problem. The problem, however, cannot be effectively eliminated without the support of public and judiciary.

The legislature cannot enact a law against the general public opinion of the nation at large. Thus, first a public support has to be obtained not only at the national level but at the international level as well. The people all over the world are not against the enactment of statutes curbing the use of malware, but they are conscious about their legitimate rights. Thus, the law to be enacted by the legislature must take care of public interest on a priority basis. This can be achieved if a suitable technology is supported by an apt legislation, which can exclusively take care of the menace created by the computers sending the malware. Thus, the self-help measures recognized by the legislature should not be disproportionate and excessive than the threat received by the malware. Further, while using such self-help measures, the property and rights of the general public should not be affected. It would also not be unreasonable to demand that such self-help measures should not themselves commit any illegal act or omission. Thus, a self-help measure should not be such as may destroy or steal the data or secret information stored in the computer of the person sending the malware. It must be noted that two wrongs cannot make a thing right. Thus, a demarcating line between self-help and taking law in one’s own hand must be drawn. In the ultimate analysis, it must not be forget that self-help measures are “watchdogs and not bloodhounds”, and their purpose should be restricted to legitimate and proportionate defensive actions only. In India, fortunately, we have a sound legal base for dealing with malware and the public at large has no problem in
supporting the self-help measures to combat cyber terrorism and malware. If still there remains any doubt or objection, then it will be sufficient to mention that only a computer can react fast enough to take care of the menace of malware and the traditional methods of law enforcement are helpless in this regard. The problems of lack of harmonization, doubt regarding jurisdiction, lack of a uniform extradition law between various countries of the world, etc. can be solved only by using a legitimate, proportionate and reasonable mechanism of self-help, which is not only instant but also free from technicalities and formalities.

Practices Recommended for Cyber Crime Prevention

**Firewalls:** These are programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people when the user permits.

**Frequent password changing:** With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.

**Safe surfing:** Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, visiting secure sites. Accepting data from only known users, downloading carefully and from known sites also minimizes risk.

**Frequent virus checks:** One should frequently check ones computer for viruses and worms. Also any external media such as floppy disks and CD ROMS should always be virus checked before running.

**Email filters:** These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.

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:

- **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.

- **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.

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

- **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.

- **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 within each country.

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

- **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.

- **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.

- **Educate and involve the media professionals, netizen and then encourage them to increase public awareness.**

- **Engage large private sector corporations and industry associations in the sponsorships of awareness programs.**
Abstract

- Emphasis should be laid on less developed countries on effective systems, for protection against, detection of and responses to cyber crime.
- 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.
- Law enforcement personnel must be trained and equipped to address on high-tech crimes.
- Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- Prevention is better than cure. Awareness regarding education and technical support to prevent e-crime is essential, but without discouraging the development of e-commerce.

Adoption of these measures will go a long way in preventing and controlling cyber terrorism and cyber crime which has not only reached menacing proportion but is also likely to increase in foreseeable future. To conclude this study, it may be said on the basis of the discussion in the five 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, with the use of internet.