CHAPTER VII
CONCLUSION
AND
SUGGESTIONS
CHAPTER VII

CONCLUSION AND SUGGESTIONS

7.0 Conclusion

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided. The truth is that the criminals have changed their methods and have started relying on the advanced technology, and in order to deal with them the society, the legal, and the law enforcement authorities, the private corporations and organizations will also have to change their mechanism to combat it. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardwares and softwares so that they can efficiently fight the cyber criminals. Thus, necessary facilities must be established in various parts of the country so that crime in the virtual world can be controlled. Another aspect which needs to be highlighted is that a culture of continuous cyber education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is very dynamic as the knowledge of today becomes obsolete in a very short time. Lastly the preamble of the Information Technology Act, 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the Act

1 Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.
has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act, 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the Act is not to suppress the criminal activity, but this act has defined certain offences and penalties to overpower such omissions, which is understood to come within the characterization of cyber crimes. From this, it can be inferred that the law cannot afford to be static, it has to be change with the changing times and viz. cyber space. This is all the more required, that many applications of the technology can be used for the betterment of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy-cam case. The bottom-line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

In the information age the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of trans-national crimes known as “cyber crimes”. Cyber crimes have virtually no boundaries and may affect every country in the world. Cyber crimes are “any crime which is committed with the help of computer and telecommunication technology”, with the purpose of influencing the functioning of computer or computer systems. To understand cyber crime as a significantly new phenomenon, with potentially profoundly new
consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently affecting countries worldwide. Free flow of uncensored information on electronic networks and web-sites is as attractive to insurgents and extremists groups as it is to dissidents proclaiming their human rights just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crimes.

Since users of computer system and internet day by day are increasing worldwide. It has become easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by 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 in each and every nation of the world. Neither the most of the nation of the world have got separate law, 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 all these have made countries vulnerable to the threats of cyber crimes. Therefore, there is no denying the fact that an international agreement on the ways and means of dealing with cyber crime is urgently required to address the problem in a
holistic manner. 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 without support of popular public and judiciary.

The extent of loss worldwide of cyber crimes is tremendous as it is estimated that about 500 million users of the internet can be affected by the emergence of cyber crimes. Cyber crimes are a very serious threat for the times to come and pose one of the most difficult challenges before the law enforcement machinery. Most of the cyber crimes do not involve violence rather than the greed, pride, or play on some character, weakness of the victims. It is difficult to identify the culprit, as Net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber crimes are considered as "White-Collar Crimes".

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.
Conclusion and Suggestions

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.

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

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

**7.1 Suggestions**

The judiciary can play a pivotal role in implementation of cyber law only if it is high-tech equipped. It has to adopt new mechanism of administration of justice to be known as *e-justice*. Electronic justice can provide speedy trial so as to convict cyber criminals without undue delay. Delay in trial may cause loss of evidence as electronic records are not of permanent nature in comparison to other records. It is suggested that the Indian Parliament should pass Electronic Code of Criminal Procedure for e-courts for expeditious trial.

The Law Commission of India has stressed the need for enactment of more cyber laws and for establishment of electronic courts to deal with cyber crimes. It is suggested that the scope of existing law may be extended to cover variety of cyber activities but enforcement aspect should not be ignored.

Prevention is better than cure, therefore, the preventive measures to protect electronic records may be more fruitful than enactment and high-tech professionals can better accomplish this task. Law is an effective weapon to
regulate human behavior yet in high-tech sphere the scientists and technical persons can play a better role.

It is observed that teenagers commit cyber crimes and sometimes they play hacking game to adopt adventurous task. They are ignorant of the consequences of their act. They are also unaware of the deterrent provisions of cyber law. Therefore, in school education cyber ethics should be incorporated in course curriculum. The services of the hacking minded children should be used for constructive purposes.

It is not expected from judge to possess high-tech knowledge to deal with cyber crimes and for that they can seek expert opinion. Forensic science experts always render their useful services to courts in administration of criminal justice. It is suggested that the institutions of forensic science should establish special cell to identify cyber criminals.

When a person beyond the territory of India commits cyber crime, damaging within the territory of India any computer system, there is no easy way to procure the arrest of such criminal in absence of extradition treaty. It is suggested that international law should be developed accordingly.

Perfection can be attributed only to Almighty. Whatever steps taken by India is good initiative in the field of cyber space and, I hope that in near future it will continue to take long strides on the path of curbing cyber crimes and to regulate other cyber activities. It will take lesson from its own past experience and the experience of other developed countries to make the
existing cyber law more comprehensive and to built an appropriate and efficient infrastructure to enforce it.

Nevertheless, to prevent and control cyber crime and cyber terrorism, there is a need to adopt several preventive and controlling measures through law and public awareness.

- There is a need of specific provision with a clear definition of 'cyber terrorism'. We may say that 'cyber terrorism is the use of computer as tool or target to cause unpredictable violence and threat in the mind of general people about safety, security and in the mind of Government about national security, safety and interest etc.'

- There is need to evolve international standard of security measures.

- Government agencies must specially choose Local Area Network (LAN) for international communications.

- They must adopt their own communication, secret and confidential fiber method; delete confidential information after use etc. to fight against virus, worm, hacking hijacking, net-war, cyber terrorism etc.

- Regular updating antivirus software, changing password, updating operating system etc. are few preventive measures.
Conclusion and Suggestions

- There is great need of awareness like IT education, and training among government agencies as well as general people.
- There is need to improve infrastructure of law enforcing agencies.
- Our Judiciary should also have some training and Infrastructure development in this field.
- To prevent and control net warfare, investigative agencies must be empowered to deface terrorists' websites and network.
- There is need to develop law to prevent and control cyber terrorism where mobile and wireless is used by terrorists. It required specific Law fixing responsibility, liability and accountability of the internet service providers: e.g., they must be prohibited from using the user numbers of their clients.
- Cyber terrorism may be controlled by investigating suspected wireless, mobile phones and service providers like 'history' in Computer, through 'menu' in cell phone.
- In 9/11 attack on WTC & pentagon, network of airways was attacked and it did not affect other networks. That is why others were not alerted about that attack. Network services must be connected with each other to share or exchange information to alert others for sudden attack.
- A committee must be constituted to study the various provisions.
Conclusion and Suggestions

under the Information Technology Act, 2000 and the provisions contained in the Indian Penal Code, 1860 to suit to the requirements in the administration of Cyber Justice.

- Identification of exposures through education will assist responsible companies and firms to meet out these challenges.

- One should avoid disclosing any personal information to strangers via e-mail or while chatting.

- One must avoid sending any photograph to strangers by online as misuse of photograph incidents is increasing day by day.

- An updated Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

- A person should never send his credit card number to any site that is not secured, to guard against frauds.

- In order to protect children from harassment and bullying parental control is necessary.

- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
Conclusion and Suggestions

❖ Web servers running public sites must be physically separately protected from internal corporate network.

❖ It is better to use a security program by the body corporate to control information on sites.

❖ Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.

❖ IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

❖ As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

❖ A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with rigorous punishment so that it will anticipate the criminals of cyber crime.

❖ It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

❖ Web site owners should watch traffic and check any irregularity
on the site. Putting host based intrusion detection devices on servers may do this.

- Make Backups of Important Files and Folders to protect important files and records on your computer if your computer malfunctions or is destroyed by a successful attacker.

- Habitually download security protection update patches & Keep your browser and operating system up to date.

- Change administrator’s password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.

- Turn off the network during extended periods of non use, disable file sharing on computers, etc.

- Check your online account frequently and make sure all listed transactions are valid. Use a variety of passwords, not same for all of your account.

- Never respond to text messages from someone you don't know and open email attachment carefully.

- Never let someone you don’t know use your cell phone and avoid posting your cell phone number online.

### 7.1.1 PRACTICES RECOMMENDED FOR CYBER CRIME PREVENTION
Firewalls: These are the programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom 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 the 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.

### 7.1.2 Policies Recommended for Cyber Crime Prevention

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

- **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.

- 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
tackle 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 foregoing chapters that cyber world is a recent origin. Various preventive measures have been taken law & mechanism evolved to check the crime in the cyber world. But these mechanisms are not sufficient to check or control the cyber crime, although the law and enforcement agency has been evolved to check this particular crime. There is however need to undertake research work on the protection of the cyber crime from different angle and so as to find out how it can be minimize it and with the use of internet.