SUMMARY

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world. Further, all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime. It can be concluded with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment." The hallmark of criminality is that, it is breach of the criminal law. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel.

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of
criminal activity and include everything from electronic cracking to denial of service attacks. Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cyber crime in the context of national security, may involve hacktivism, traditional espionage, or information warfare and related activities. Cyber crimes have been reported across the world.

The study has been undertaken with the help of empirical research tools. The collection of data would be done from available books, articles, conference reports and also taking interviews of the concerned people who are responsible to implement the laws to mitigate such crimes. Therefore, the methodology would involve a synthesis of primary and secondary sources to be documented in the descriptive analysis.

We were ascertained and the investigation have revealed share frauds; credit card crime, financial thefts etc. Indian Detective Agency can detect and help prevent such crime by providing a complete package to counteract related frauds and abuses. The interviews of the authorities responsible for lodging complaints of cyber crime made it possible to record all about the reported cyber crimes. It is revealed that unreported cyber crime surpasses the actual numbers of cases. Interviews of Yahoo Mail and Hotmail, MSN India Representative offices in India having responsibility as service providers for any Cyber Crime committed in India under Information Technology Act-2000 or other laws would also provide information on detection, identification, curtailment and prevention of cyber crime.

The case studies have been selected from the reported cyber crimes. The interviews would include the officials responsible for control and detection of cyber crime. This includes the various officials of CBI, police and Special Task Force and Cyber Cells. The Bank officials engaged in electronic banking would also be interviewed. The office of the local web
sites have been consulted and interviewed. The sufferers of the cyber crime have been enlisted for interview. To trace the sociological impact and cause of cyber crimes the interviews of cross Section of the society have been taken.

Today, an increasing number of companies are connecting to the Internet to support sales activities or to provide their employees and customers with faster information and services.

The modern world relies on computerized system for almost everything in the life, from air, train and bus traffic control to medical services. The rapid expansion of large-scale computer networks and the ability to access systems through regular telephone lines increase the vulnerability to these systems. The virtual world has taken over the real one, e-business and e-commerce, which are the new mantras and electronic transactions and dominate the overall business paradigm.

Modern business is quickly replacing cash with deposits transacted on computer system creating computer fraud. Credit card information as well as personal and financial information on credit card has been frequently targeted by organized criminal crimes. Intangible assets represented in data format such as money on deposits or hours of work are the most common targets related to fraud. Assets represented in data format often have a considerably higher value than traditionally economic assets resulting in potentially greater economic class. Computers however can also be used as instruments for committing forgery. A new generation of fraudulent alteration or duplication emerged when computerized color laser copies became available. These copies are capable of high-resolution copying, modification of documents that are even creating false documents without benefit of original. They produce documents with an equality that is indistinguishable from original documents. In this rapidly evolving e-world that depends on free flowing information, security is the major
problem to be considered. Security on Internet is challenging. Security on an Internet is important because information has significant value. Implementing security involves assessing the possible threats to one’s network, servers and information.

In the light of the above- analysis, there is a rationale to understand the problem of cyber crimes, its magnitude and dimensions and to minimize the threat as much as possible. Therefore, the present study of understanding the nature, extent and the impact of sociological and economic aspects of cyber crime is of immense significance. This piece of research work is therefore, a pioneering effort to help expand the knowledge base on the act of cyber crimes thereby assisting people to be more careful about their information, money in the bank and other valuables.

As we know that prevention is always better than cure. It is always better to take certain precaution while operating the net. The present study advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. The thesis also highlights that one should keep in mind the following things-

1. to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

2. always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3. always use latest and update antivirus software to guard against virus attacks.

4. always keep back up volumes so that one may not suffer data loss in case of virus contamination.
5. never send your credit card number to any site that is not secured, to guard against frauds.

6. always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

7. 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.

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

9. use of firewalls may be beneficial.

10. web servers running public sites must be physically separate protected from internal corporate network.

Role of Policy Measures: In May 2000, at the height of the dot-com boom, India enacted the IT Act and became part of a select group of countries to have put in place cyber laws. In all these years, despite the growing crime rate in the cyber world, only less than 25 cases have been registered under the IT Act 2000 and no final verdict has been passed in any of these cases as they are now pending with various courts in the country.

Although the law came into operation on October 17, 2000, it still has an element of mystery around it. Not only from the perception of the common man, but also from the perception of lawyers, law enforcing agencies and even the judiciary.

The prime reason for this is the fact that the IT Act is a set of technical laws. Another major hurdle is the reluctance on the part of companies to report the instances of cyber crimes, as they don't want to get negative publicity or worse get entangled in legal proceedings. A major hurdle in cracking down on the perpetrators of cyber crimes such as
hacking is the fact that most of them are not in India. The IT Act does give extra-territorial jurisdiction to law enforcement agencies, but such powers are largely inefficient. This is because India does not have reciprocity and extradition treaties with a large number of countries.

What India needs to do in this backdrop, is to be a part of the international momentum against cyber crimes. The only international treaty on this subject is the Council of Europe's Convention on Cyber Crime, formulated primarily by the European Union. By signing this treaty, member countries agree on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals. At the last count, there are 43 member countries, including the US and South Africa. India is not yet a part of this group and being a member would go a long way in addressing this issue of cross-border cyber terrorism.

The Indian IT Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crimes and criminals. We are now beginning to see new categories and varieties of cyber crimes, which have not been addressed in the IT Act. This includes cyber stalking, cyber nuisance, cyber harassment, cyber defamation and the like. Though Section 67 of the Information Technology Act, 2000 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to two years and with fine which may extend to twenty five thousand rupees on first conviction and in the event of second may extend to five years and also with fine which may extend to fifty thousand rupees, it does not expressly talk of cyber defamation. The above provision chiefly aim at curbing the increasing number of child pornography cases and does not encompass other crimes which could have been expressly brought within its ambit such as cyber defamation.
The present trend of legislation and also the judicial approach to such offences appears to be such that these offences are treated lightly and the punishments are not adequate having regard to the gravity of such offences. Though the Government of India sought the Law Commission to come up with a well-considered opinion as regards desirability of dealing with adequately and swiftly certain anti-social and economic offences, such as, those offences calculated to prevent or obstruct the economic development of the country and endanger its economic health, evasion of taxes, hoarding and black-marketing etc.; but it has not expressly included cyber crimes such as defamation in cyber space.

The intense volume of information and the simplicity of its transfer make Internet a very critical source of defamation, while the electronic based trading systems are affecting all aspects of commercial and business entities. The IT revolution is sprawling new business and forcing the old modes to either change or die out. Hence most commercial organizations around the globe will be affected in some significant manner by the internet and therefore crimes in cyber space as well.

It may be noted here that there has been an increasing awareness among law enforcement agencies on the need to set up special cells to handle cyber crimes. The CBI has a well-established cyber crime cell. The first such cyber crime police station has also come up in Bangalore. As the network environment becomes more pervasive and easier to use, it will also be a medium through which crime and fraud can take place. It is therefore necessary to review the current legislative provisions to ensure that the network environment is adequately protected against criminal activities. Under the current legislation there is no definition of damage and it is consequently difficult for the current enhanced penalties to be imposed.

In the short term, the following may be likely:

- The old laws will prevail until more cases and legislation emerge to
provide a more refined and a more contemporary application of libel laws to the Internet.

- All Internet users will be exposed to liability for libel on the Internet, whether they are e-mail publishers, owners and/or operators of bulletin boards or home page operators. Individuals or corporate organizations who establish bulletin boards on their web sites are particularly vulnerable.

There is unlikely to be an explosion of libel actions against individuals for several reasons.

a) The cost of libel actions.

b) The jurisdictional problems.

c) The unlikelihood of recovering many assets.

d) The opportunity and ease of immediate reply.

There are likely to be more lawsuits against the operators of bulletin boards, whether they are corporations, organizations or individuals. There will be actions against owners and/or operators of web sites for statements made by their employees or their organizations.

In our opinion the Law Commission should take up the brave task of analyzing such crimes, which are at the threshold and come up with recommendations in order to equip the existing legal machinery against such offences. For the said purpose necessary amendments could be made.

Thus, to conclude, the whole study has reviewed and analyzed the various dimensions of cyber crime, cyber laws and other related aspects in the society. We have found very interesting issues and viewpoints during our analysis pertaining to the research area. The same has been described vary widely in the thesis and in each related chapters. It may further be inferred that in the era of globalization the cyber crimes have an increasing trend. They need to be checked through a broad set of policies, guidelines
and spreading education in the society. Also there is a need to tighten the implementation of cyber laws whilst spreading awareness about the law through media and education. Our society is hetrogenous consisting of the wide variety of strata's, groups etc. The issues related to the security of cyber aspects need to be tackled through prudent laws and participation of all the stakeholders in this whole campaign.