Conclusion and Suggestions

The cyber crime is a new invention of crimes made by a class of intellectual, sophisticated criminals. Since long time the criminal jurisprudence was totally ignorant of such types of crimes, although these were committed in different forms during early development of crimes and criminology. One can say that the cyber crimes started to operate when technology reaches its peak and took new turn to satisfy human needs and desires.

Because such crimes being committed with the help of machines and on arithmetical formulation, are different types in nature from that of ordinary types of crimes. These crimes contain the elements of blue colour and white colour crimes. These are blue colour crimes because these are not very different from other prototype crimes, though recognized by various names. These are also white colour in nature because crimes are usually committed by a class of criminals who are having knowledge about science and technologies. For this reason I dare to say that cyber crimes are an amalgamation of blue colour and white colour crimes.

In the selected subject of work, I made a thorough study on the new forms of crimes. The criminals of this advanced age endeavour to commit this new crimes with the help of computers through Internet by exploiting cyber space. This is a new subject and the world facing problem to tackle the situation.

In Chapter I and II, I discussed about the development of computer and Governance in cyber space. In Chapter III to V, I discussed on cyber crimes, statutes dealing with cyber crimes and its prevention, protection and control. In Chapter VI to VIII, I discussed on Intellectual Property Rights, the I.P. Crimes and Treaties and Human Rights. And in last Chapter I discussed on Digital Dilemma.

To realize the subject of 'cyber space' and 'cyber crime', it is important to know the history and gradual development of modern computer and its application. Historically the modern computer of the first decade of 2nd century directly descended from calculating machines, like IBM-I, Automatic Sequence Controlled calculator. The history of computer is directly linked with the history of computation. The modern computer can work with number, its main use for storing and manipulating information. The outcome of the computer is the result of the contributions made by unknown persons. The cyberspace is a world in which every (digital) product carries with it the
possibility of an almost magical speed, and precision of replication. The Internet is a vast worldwide network of powerful computer sensors which are constantly connected to each other via high speed communication cables. All the information that is on the Internet is stored on one of the servers. The Internet is a virtual space in which user send and receive e-mail, log in to remote computers, browse-databases information and send and receive programmes contained in the computers.

In above mentioned Chapter III, various types of cyber crimes and criminals have been cited along with their mode of operation. These are new type of operation, usually and frequently adopted by the cyber criminals and such operations are peculiarly different from traditional types of commission of crimes. Since long the criminologists found to have been engaged in traditional crimes have paid little attention to this type of crimes. It has been the time of birth of the computer when cyber crimes taken its birth also. It may be said when we compare the impact of traditional crime with that of crimes committed through computer on cyber space, the cyber crime is much more pervasive causing injury to country’s economic structure, legal frame work and also to human rights. This sort of crimes always prevents human being to live with dignity. The time has come to consider the impact of such type of crimes on the society with due perspective, so that the cyber criminals can not go escort free. The protection of cyber crimes is the prime concern of these days and is a vital part of social, cultural and security aspect of a country. Different Treaties and Agreements came into being for protection of cyber crimes and intellectual properties.

The cyber crime is a primarily example of cross-border crime. The jurisdiction in this area is a tricky and is still unclear.

The Government of India has enacted Information Technology Act, 2000 to deal with cyber crimes. The Act further amends the Indian Penal Code, 1860, the Indian Evidence Act, 1872 the Banker’s Books Evidence Act 1891 and the Reserve Bank of India Act 1934. The cyber crime cell and police station have also been created for detection and investigation of such crimes. A multi pronged strategy is required to fight along with legal measures.

The cyber crime is a great threat to the human rights. The number of security attacks being designed to steal personal information is increasing with accelerating pace. The attackers are targeting personal information to make a profit out of their operation and threatening the basic philosophy of ‘right to live with dignity.’
As the cyber criminals' are masters of using the modern Science and Technology and it is very much complicated for effective law enforcement. Some times technologies provide benefits to criminals. Effective law enforcement is equally complicated by its transnational nature of cyber space. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations.

Cyber crime may originate in any part of the world and can pass easily across many national boundaries. Such a situations increase both the technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to combat the cyber crimes.

The advanced country like the United States has enacted some Acts dealing with the cyber and intellectual property crimes. The Economic Espionage Act, enacted in 1996, created the first federal Sanctions for theft of trade secrets. In 1996, threats of virus attacks and disruptions of computer networks prompted the justice Department to create the computer crime and Intellectual property section within its Criminal Division. The United States also passed the Computer Fraud and Abuse Act. At this point of juncture some suggestions and opinions to tackle this new form of crimes have been made :

1. Improvement of technology is in need of the days. Cyber crimes are such types of crimes which can primarily be prevented along with other measures. Technological improvement may be helpful for detection, prevention and commission of such crimes. High standards for security and network reliability have to be required. Effective technological “locks” to prevent end users from copying and distributing copyrighted music in digital form.

2. Special Statutes on cyber crime is required to be passed to deal with the new form of crimes and to protect digital data. It will include Intellectual Property crimes and crimes relating to human rights.

3. The Government has to create a special branch of Cyber crimes and Intellectual Property Crimes within its criminal infrastructure, so that the enforcement personnel may take quick action against the Cyber Criminals.

4. All sorts of infrastructure facilities are required to be available to the investigating officers, especially in regard to mobility, connectivity, use of technology. Scientific training to be provided to the investigating officers to
deal with the new problems under separate investigating agency to deal with the cyber crimes.

5. The Economic Espionage Act like law is required to pass for the protection of trade secrets, pragmatic steps is required to protect confidentiality of trade secrets during investigation and prosecution.

6. An Act having objectives to prevent computer fraud and abuses are to be enacted to combat criminal operations. It may be helpful particularly during investigation and prosecution of criminals. It will deal with security and safety of certain computers, computer networks and data stored on the computers and unauthorized access to Government Computers. The Act will also deal with hackers.

7. In case of digital technology, various problems are experienced. Problems of distribution, catching, protection of confidential information, payment mechanism of e-commerce are few among these. In view of such situation Intellectual Property Laws till require major amendment to deal with challenges posed by the internet and digital revolution.

8. It has been the fact that there is some grey areas in Intellectual Property regarding “domain name”. Though the domain names are protected under relevant I.P. Law. There is scope of further amendment of such laws to make this more clearer for ends of effective increase of the commerce.

9. Good infrastructure and facilities be provided by the Government to the Cyber Crime Cell and the Cyber Crime Police Station to deal with the cyber crimes. With weak infrastructure facilities the police personnel facing tremendous problem in detecting and investigating of crimes and sometimes they fell helpless. To train law-enforcement personnel and the prosecution for understanding the technological aspects and their use in crimes. The Government has to establish advanced cyber labs and to provide different levels of training to police. Creating awareness on data security understanding cyber crime, to understand how to survey a crime scene and preservation of evidence, identification of digital evidence, understanding computer hardware and data storage.

10. It also requires the maintenance of compulsory Register of every cyber cafe for detection of cyber criminals who are sending threat e-mails and are interested to
practice such other acts involving the question of the country’s safety and security.

11. The users are not aware of using computer and Internet. The ISPs have to provide some sort of warning on the Internet. Awareness of general public and investigation agencies is essential. Active involvement of the Government is also essential. ISPs have to be more accountable to the Government and also to the public for providing required information. The Government has to frame stringent law upon the ISPs.

12. The punishment for commission of cyber crimes to be increased to deter future offence. It must not only be deterrent but must also be exemplary.

13. For increasing awareness the emphasis has to be laid on cross-border investigation and exchange of measures for prevention of Cyber Crimes among various nations.

14. The Interpol, the Police Organization may be utilized for speedy exchange of information and materials required for prosecution of cyber criminals for its trans-border nature. In absence of extradition treaty with number of countries it has been difficult to apprehend the cyber criminals and to have necessary information from other countries when criminal operation is being done from other countries. It is therefore urgent need of time that Government may consider to take the help of INTERPOL. It is also intended that necessary legal provision should be included in the proposed new Act.

15. Alike Green Bench, a Special Bench for dealing with cyber crimes may be created at least in each and every High Courts. Special branch may also be created in every metropolitan cities and districts.

16. The last but the vital one is to train and equip judges and criminal lawyers and investigating and enforcement agencies to deal with this new transnational, complex, high-tech crimes to understand investigative and prosecution process that are unique to cyber crimes.