CHAPTER SEVEN

CONCLUSION AND SUGGESTIONS

7.0 CONCLUSION AND SUGGESTIONS
Legal control of Cyber Crime has been the most common form of management as in the case of other traditional crime management in different countries. A crime has been defined as the intentional act or omission in violation of criminal law for the time being in force (nullum peona sine lege) the other elements are the involvement of a human being and some injury to property, person including intangible aspects of human being. The existing crime management infrastructure working for traditional crime control has been the basic foundation in the case of cyber crime also.

The question of criminal liability of a remote operator (actor) has been under serious scrutiny of the legal community on the basis of the physical participation of an actor. This issue has been widely debated throughout the civilized society but the involvement of a hacker doing harm to others has been recognized as an offence against society and as such has been recognized as an act of crime. The 1st Convention on Cyber Crime, Council of Europe, held in 2001 and the United Nations Recommendations of Permanent Monitoring Panel etc. have recognized the wrongful offensive activities in Cyber Space as crime against society. So far the control of cyber crime in concerned, the involvement of several national territories in a single act of crime is very common in the borderless nature of the cyber-space. And as such, frequently the national governments find the need to have immediate active co-operation from other nations. To manage the cross border investigation evidence collection and tracking the offenders - round the clock (24/7) networks and Contact Points have been developed in all technically advanced countries.

The existing set up of investigation, law-enforcement the substantive and procedural laws the presiding officers in the courts etc. all are under the process of learning and developing themselves to deal with the new high tech-crimes involving information and communication technology (ICT). In India, we have entered the age of cyber space in 1995 when VSNL opened the GIAS (Gateway Internet Access Service) for common people. And the SEBI (Securities And Exchange Board of India) allowed online trading in 2000 Jan. Thus the online activity in all sectors including commerce, trade, administration took a new and massive turn. And the law enforcing agencies have been receiving necessary training to combat the new high tech crimes. And the legislation has also passed the Information Technology Act – along with necessary changes in the Evidence Act – 1872, Indian Penal Code - 1860 and some others.

And the IT Act – is being already invoked in deciding cyber crimes in India-i.e. Chennai – Cyber Stalking Case - Suhas Shetty. (NOV-2004).

In the United State the Internet was opened to the full commercial use i.e. 1995 and the Universal Access Program was taken for the Information Super highway- the Internet.
And the United Nations published UN - Model Law (UNCITRAL) on international trade and commerce involving the Internet in 1998. Indian Legislature accordingly drafted the Electronic Commerce Bill in 1998, left it incomplete, then the issue went to the newly opened Department of Information Technology. The Information Technology Act went into force on 17th October 2000.

The IT Act is a timely and neatly drafted piece of legislation, which has been overdue for several years. The Act though focuses on trade and commerce, necessarily deals with cyber criminals also.

The scheme of crime management in the Act has been that a group of wrongs described U/s-43 has been kept under civil management – adjudicating officer S/48, and the civil rules S-46(5).6.

The other group of offences like tampering S/65 hacking S/66, obscene materials S/67 access to protected computer S/70 etc. have been kept under the general control of existing criminal administration and criminal courts. The overall working of the scheme has been effective so far with some points requiring further and careful scrutiny for the purposes of better working and complete justice.

Points :-

1) S/80 – Power of Police Officer and other Officers to enter- search etc – the law provides extensive power to enter and search any public place. This requires further clarification and better protection against abuse especially in the cases of educational institutions, religious places, health centers, hostels, etc.

2) S/80(2) – Provides for – taking or sending arrested person to the magistrate without unnecessary delay – this is a vague term likely to be abused and (a) the Constitutional mandate of 24 hour limit to be expressly mentioned and also.

(b) The rights of the arrested person to be made known to him as a statutory duty of the Officer arresting.

3) The provision U/s-65,66,67 & 70 do not mention the computer or the device used by the accused in the commission of the crime. But in most cases of investigation, the computer used as a tool is a subject matter of search and seizure. So this device may be mentioned in the express provisions of the crimes.

4) The IT Act does not mention interception by the accused as an offence – this requires notice of the concerned authorities.

5) The provisions of S/65-66-67- don’t mention about the liability in case of abetment and/or attempt excepting S/70- this requires express mention to avoid confusion in the courts.

6) The provision U/s-67- Publishing of information which is obscene in electronic form – attracts a penalty of imprisonment upto ten years and a fine upto two lakh rupees.
The attitude of the legislature here appears to be inconsistent. With the real cyber crimes that can't be digested by a reasonable man for many reasons - 
(a) punishment is excessive
(b) fine is compulsory not alternative
(c) obscenity itself is vague, can never be defined with precision
(d) injury can be checked using filters
(e) no imminent danger of actual damage incase of so called porn web site
(f) scope of abuse of the provision under section 67 is very high.
(g) freedom of speech and expression at the source can't be checked.
(h) closed door communications among adult don't require legal intervention.
(i) right to privacy may be damaged.

7) S/70 – Protected System – the absolute liability in accessing or attempting access the government computers is against the rule of criminal liability so the language might be changed to include “Knowingly or knowing it to be a protected system”.

Because access may be so easy with tools available that if sufficient protection is not taken for the computer so protected – access by innocent (idle curiosity) may take place without any ill motive whatsoever.

8) A complete set of expert investigators – and the judicial officers in two cases of civil management as well as criminal management of the same type of cyber offences certainly will create problem due to shortage of expert personnel in all sectors.

9) S/43 – provides for securing access as civil offence and tampering source code (S/65) and tampering computer data base (S/66) as criminal offence but no – offence U/s 65 or 66 can be possible without securing - access. Sometimes access itself is committed to get data transferred not to delete etc. like Trojan Sniffer program. So access, transmission of data and hacking can't be isolated and kept in different provisions.
10) Dropping worm may be made a criminal wrong instead of a civil wrong U/s-43.

11) Disruption and damage to Computer System network U/s-43 will be better managed if put under criminal wrongs.

12) Penalty provision may include community service or some soft measures.

13) S/75 – Offence Committed outside India – but involving Computer in India – requires further clarification as to the liability of the owner of the Computer / System / network and the Concerned ISP.

14) That all ISP and computer vendors may be required to give the address of CCIC (Mumbai) and other web sites or address relating to cyber crime to all customers coming to them.

15) LEA to keep contact with some agent hackers.

16) A good human intelligence network is also necessary for this part.

17) A good system to keep crime record and a data base is required.

18) Every PS to have one officer to deal with this part of crime.