CHAPTER ONE

INTRODUCTION
CHAPTER - 1

INTRODUCTION

The present work-A study of the legal control of cyber crimes with special reference to the Information Technology Act - attempts to study the shape and working of the legal framework necessary to deal with the criminal activities in the cyber space with special reference to the IT Act.

The new Information and Communication Technology (ICT) in the last quarter of the 20th century has presented us with a very high-tech method of communication, storage and processing of information. All the social institution have been transferred into this electronic media. So the law as a social science requires to be familiar with this new environment. The cyberspace as a store house, public and highway requires protection patrolling, surveillance and law and order enforcements. So it is the need of the hour to become familiar with this new world its working, bright & shadow sides, strength and vulnerabilities, rules & regulations, duties liabilities rights and opportunities. “Inventions discoveries and technologies not only widen scientific horizon but also pose new challenges for the legal world. Computer, Internet and cyber-space together known as information technology have also posed new problems in Jurisprudence. It has shown in adequacy of law while dealing with the
(i) information technology itself;
(ii) changes induced by the information technology in the way we live, perceive and do business. The courts throughout the world have been dealing with these problems and coming up with inconsistent answers. Sometimes these problems have arisen in separate tight compartments mentioned above; Sometimes in combination with each other. These problems have arisen in different areas. These areas are; intellectual property, electronic commerce or e-commerce (commercial laws), Jurisdictional issues, safety concerns, criminal law, evidential issue(i.e. admissibility and relevancy of electronic documents or computer printouts in courts), moral issues and freedom of expression and privacy protection. The law (statutory or providing answers to these problems or dealing with the information technology is often loosely referred to as the computer laws or Information Technology Laws or Cyber Laws”.

India has very fast entered the cyber age in mid -1990s when VSNL opened GIAS for common people in 1995 August. The USA the motherland of cyberspace also took universal access program in 19954. In 2000 January – SEBI has granted permission for online trading. Thus by 2000 AD, India has created basic framework for the electronic century or 21st Century. And cyber-crime as such can’t be neglected in India also:

TABLE - 1 * IA

<table>
<thead>
<tr>
<th>PROJECT INDIA CRACKED</th>
<th>No of Indian websites hacked &amp; defaced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td></td>
</tr>
<tr>
<td>1999</td>
<td>47</td>
</tr>
<tr>
<td>2000</td>
<td>131</td>
</tr>
<tr>
<td>2001</td>
<td>431</td>
</tr>
<tr>
<td>2002</td>
<td>225(up to May)</td>
</tr>
<tr>
<td></td>
<td>834</td>
</tr>
</tbody>
</table>

The telecommunication network already developed in 19th & 20th century has provided for the country-wide physical cabling network for the rapid expansion of INTERNET. The Information & Communication Technology (ICT) including wireless and satellite communication system were also developed by this time. So in the closing years of the last Century Indian technical community – government and political motivation quickly and confidently accepted the new age- the Cyber age.

A separate department Ministry of Information Technology was established as high priority section and new ISP policy was taken up issuing private ISP licenses in May 2000 (about seventy five ISPs immediately started working in May 2000). * 1B The existing law-the Indian Telegraph Act- 1885 was found to be inappropriate in the new sector. And in response to the UN call and the Model Law UNCITRAL – 1998-India quickly framed the Electronic Commerce Bill-1998. This was however left in the mid-way and the present Information Technology Act was then enacted and enforced on 17-Oct-2000. The vices of the real space have quite obviously been transferred into this new area and undesirable activities are spreading here. In India the modern crime management system based on Criminal Science, was introduced by the British rulers, especially by Macaulay in the second half of 19th Century.* 2 The Indian Penal Code- 1860, the Criminal Procedure Code – 1860 the Indian Evidence Act – 1872 etc. all were framed by British Jurists on the basis of the rules and principles of the Juridical Science. This provided for a revolutionary change in concept and process of crime management.

This basic framework comprising time-to-time legislative updating, court system police and prison and the legal education as a separate branch of academic discipline provided the new modern and scientific mechanism both in theory and practice for the proper management of crime in India.

IA * PIC – www.srijith.net - download – 10-09-04
This general formula has been applied in all Common Law countries and other countries also with some modifications (such as burden of proof etc.) accepted this modern method of crime management in respective societies. This rough and ready framework with already developed – universal rules, principles and doctrines of criminal law throughout the world have been the appropriate system to deal with the present wave of cyber crimes also. *3

In the new environment the important issue is to update the legal rules and procedures and to become familiar with the new technical system (ICT). The method of investigation search and seizure, evidence collection preservation chain of custody, production, recognition and admission of electronic evidence, rules of interception, evidentiary value of electronic document, methods of surveillance in the cyber-space, trap and trace, rules of criminal liability for authorized access, tampering and defacement, worm-dropping, privacy, human right, intellectual property right-copyrights and trade marks, technical innovations (MP3 & Napster) in the context of old property concept, taxation of information flow, Jurisdictional issues, framing and hyper linking and many like issues are coming up requiring legal interpretation and address. *4

The basic needs of legal control are the substantive and procedural laws, cross border-mutual assistance for investigation, harmonization of different national laws on Cyber crime. The European Convention on Cyber Crime 2001 has already- made an attempt in this direction to have uniform rules on criminal liability of cyber wrongs. Various national laws those of USA, UK, Germany, Australia, Singapore, Malaysia, India etc. have framed laws with almost in the same spirit of criminal liability for access, hacking, worm-dropping, interception etc. “Challenges to law enforcement agencies. The Law enforcement agencies are facing the following challenges in controlling Cyber Crimes.

(a) Legal Challenges which are dependent on the statutory provisions to be used as a tool to investigate and control the cyber crimes.

(b) Operational challenges require a well trained and well equipped force of investigators operating and co-coordinating at national and international level.

(c) Technical challenges thwarting the efforts of law enforcement agency’s ability to catch and prosecute the on line offenders. In order that the corridors of communication are not used as a den to promote and perpetuate crime. Government, Law enforcement agencies, Industry, users and consumers all have to co-operate and co-ordinate in elimination thereof. *5

Every aspect of the present law and order issue in the cyber space is related to the electronics technical devices, communications lines and the computers. The electronic telegraph lines have been modernized by placing electronic processing computers at all exchanges and nodal centers. So the telecommunication system is also controlled by electronic computers.

---

4* Sup ----1 -------------edn-2001-----------P-----165
The INTERNET in the meantime in 1970s onward has again introduced a developed model of information communication. And these two-the traditional Telecommunication system (fitted with electronic computers) and the new INTERNET system. The wireless and the V S A T systems both operate as efficient tools for telecom as well as the INTERNET systems.

The electronics as a separate discipline of physical science has been developed and has been enriched gradually by the devotion and dedication of a series of talented researchers and scientists. Thomas Alva Edison had detected the new sub atomic particle in 1883, Sir J.J. Thomson recognized and identified the said particle as ELECTRON in 1897. And electronic valves were invented in 1904 by John Ambrose Fleming and these valve rectifiers were quickly accepted by newly developed wireless technology invented by Sir. J.C. Bose and G. Marconi in late 1890s.

The electronic valves were used by Prof John Vincent Atanasoff to build electronic prototype computer in 1939. Howard Hathaway Aiken, a Harvard researcher designed the first fully automatic giant calculator and it was built by the IBM in 1943. This 5 ton giant - an electro - mechanical device could perform 3 basic operations/Sec. The Defense department developed the first electronic calculator EDVAC in 1945. Before that, John Mauchly and John Presper Eckert designed and developed a complete electronic machine ENIAC (Electronic Numerical Integrator And Calculator) having 18000 electronic valves. This machine had a capacity of doing 5000 basic operations per second. But this machine was a military secret. * 6 In the mean time Manchester University (on 21.06.48) and Cambridge University May 1949, developed two smaller but efficient electronic calculators which were known to the common people.

In the meantime William B. Shockley and his colleagues invented TRANSISTOR in December 1947 and the electronic valves were replaced by these much smaller size-Device transistor. Integrated circuit (IC chips) Chips were invented on 24-7-58 by Jack Kilby (b. 1923-2005) of Texas Instruments and also by Robert Noyce (b. 1927) of Fair Child Semiconductor on 23/6/1959 both in Silicon Valley, California, the center of microelectronics industry. * 7 The I C chips were then used in the computer causing great reduction in volume and cost called 3rd generation computer. Again Ted Hoff of Intel Corporation invented a general purpose chip (micro-processor chip) in 1971. This invention again reduced the size and cost of computer now called micro-computer. The first model Altair - 8800 was made in 1975 at price of $ 397 only as against the million dollar mainframe big computers in 1960s.

And in the meantime, the electronic computers were fitted with the existing tele communication network. And the US defense department and the Advanced Research Project Agency (ARPA) invented a novel technology of computer controlled communication in 1969. * 8

Through the inventions of Charles Babbage (b. 1791), George Boole (1891-1864), Claude c. Shannon (1916-2001) and many others the INTERNET technology became a successful technical adventure which provide an information super highway connecting every individual with any other in real time and without any cost as such. And by 30 years from the invention of Internet technology in 1969, it has become a symbol of revolution in communication storage and processing of information, data and knowledge resources in all spheres of human life. Entire human society has been transferred to the counterpart or virtual world. The space provides for storage, trade and commercial activities, education and research work, administrative and governmental activities, entertainment and library facilities and the like. The information highway turned to be huge store house of valuable information, financial resources, business secrets, personal resource information and the like, the underworld activities also have become very common and frequent in this new world. The scope of anonymity and remote operation have been the great opportunity for the evil mind. * 9. A survey was conducted by the United Nations in 1991 covering 3000 sites in U.S.A. Canada, & Europe. “Eight percent of the respondents were uncertain whether they had experienced a breach of security, forty three percent of the respondents said they experienced a security incident that had been a criminal offence. Seventy two percent of those who responded said they had been the victims of, computer related crime within the past twelve months.” * 9a In the 1980s the entire Internet and telecommunication networks were left unprotected against unauthorized access and thereby causing damage, dislocation, unlawful gain, fraud gambling and such others. Gradually different technical devices like firewalls, intrusion detection system, filters, tamper proof log files, password protection, encryption etc. were developed to guard against hacking, cracking and tampering with computer resources and computer efficiency.

However the wrongful activities done by ill-motivated persons so far, could not be completely eradicated from the human society and so also the issues of offensive activities will remain both in real world and the cyber-space. So the process of controlling and managing crimes in the cyberspace has been recognized as a separate and urgent branch of criminal law. A survey on Computer Crime & Security was conducted in 1999 under the F.B.I – U.S.A among various government agencies, private corporations & financial institutions as under –

**TABLE – 2 * 9B**

<table>
<thead>
<tr>
<th>Nature</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. System penetration by outsider</td>
<td>30%</td>
</tr>
<tr>
<td>2. Attack Through Internet 1996</td>
<td>37%</td>
</tr>
<tr>
<td>3. Loss suffered by 163 units</td>
<td>$123 M</td>
</tr>
<tr>
<td>4. DOS attack</td>
<td>93%</td>
</tr>
<tr>
<td>5. Financial fraud</td>
<td>27%</td>
</tr>
<tr>
<td>6. Vandalism</td>
<td>98%</td>
</tr>
</tbody>
</table>

33% of respondents had no knowledge whether they had been attacked

New Delhi – (Sybex Computer Books Inc-USA)------------------------P – 408.
9 a* sup 1 b – 2001 -------------------------------P.522
9 B* Winn Schwartau- Cyber Shock-2000-Thunders Mouth Press NY----P.15
The issue of crime management in cyber space has raised several complex issues, requiring legal interpretation. These are the criteria of criminal liability, recognitions record, cross border investigation, law of jurisdiction, right to encryption, legal interpretation of remote access, virtual presence and uniform definition and concept of cyber-criminal. * 10 Remote connection to distant online computer has been recognized as an access and as such a criminal trespass, attracting penal provisions. So the real world concepts of physical presence, commission of crime, Actus reus, legal injury and trespass etc. are being reconstructed for the purposes of cyber crime. * 11 The issues like international trade and commerce, commercial and business torts, high sea offences, international smuggling gangs etc. are not new thing in international crime management. New thing is the issue of the extent of liability of website owners to the other nationals, the issue of forum in criminal wrongs, the issue of dual criminality i.e. the same definition of a particular crime in both the states of the accused and the victim. A/29 (4) of C O E Convention 2001. * 12 At all levels the serious effort have been taken to harmonize different national laws on crime and also to extend ready and instant cooperation as to investigation, search and seizure, collection of electronic evidence among different national governments.

The present work a study of legal control of cyber-criminal obviously can not be complete unless the study is conducted in the context of the international experiences, and observations in cyber crime management. The cyber space being a global phenomenon it is observed that “All nations face roughly the same basic problems as the United States. Most developed nations and an increasing number of developing nations face the same problems with cyber crime and hacking and many are the subject of ideological attacks on their information systems and vulnerable to cyber-war”. * 13 A. The A.I.D.P conducted a survey in 1992 which revealed that “Less than five percent of computer crime was being reported to law enforcement authorities.“ *13B The working of the Internet is qualitatively different from telecommunication network and hence the basic working principle of both electronic computer and the Internet based on hardware and software technology is relevant to assess the Landscape, the bright and dark sides of the cyber space the mechanism of the Internet is aptly exploited by the cyber criminals to hide their activities (anonymizers) to erase their own tracks to evade track-and-trace by LEAs—to place cookies to collect information from the target computer or network etc. *14 Apart from introductory chapter, others chapters are as follow:

The second chapter the historical background and working principle of computer and Internet has though in brief, dealt with an overview of Internet mechanism which may provide a route chart for tracking and tracing the cyber criminals.

13B * Sup 1 B --------2001 --------P --------523
The third chapter on Governance of the Cyber Space presents the very peculiar nature of the cyber regime. No other communication or transport medium on the planet has such characteristics of the Internet where there is no control planning or Head Office but a group of NGO like voluntary bodies, mostly composed of academicians, computer professionals, civil liberty associations manage day to day functioning, space allocations and domain name registration etc. * 15 But this peculiar system, though under recent political stress, provides less support to crime management for which, however different national LEAs are actively facing the issue.

The fourth chapter on the legal control of traditional crimes, have been included for the reason that the modern human society in every national territory has developed own system of crime management. This existing infrastructure (and network) is a vast organization with valuable experiences, knowledge and resources.

Hence this existing set up along with the basic values, rules and principles form the foundation of the cyber crime management in every society. More so because, cyber crime is also a kind of crime involving the criminal intent, act or omission, an injury to the victim concerned. * 16 So the traditional process of investigation, prosecution, trial, evidence and punishment is followed in cyber cases also as a general rule.

The fifth chapter on the legal control of cyber crimes deals with the concept and definition of cyber crime as has been attempted by different international bodies and national legislatures as - UN Permanent Monitoring Panel (2000), the European Convention on Cyber Crime (2001), legislation of US, UK, Australia, Germany, Singapore, Malaysia India, and like others. The scope and extent of cyber crime, some facts and modus operandi have been included in the study. The issues like electronic evidence, investigation, computer forensics, interception etc. are also included in the international context. The Judicial and legislative interpretations as to criminal liability, Jurisdiction, and conflict of law enforcement and civil rights, human rights issues have been focused.

The issue of violations of Intellectual Property rights have been highlighted as an important point. The existing law enforcement network and the system of criminal courts have found to play the important role in the subject of cyber crime also. * 17 . The new developments in the nature of electronic evidence, computer forensics, track and trace, investigation, interception, data collection, preservation and production etc. have been included. (Cyber Crime Code of Practice). * 18 The Sixth chapter highlights the relevant provisions of cyber crime in the I T Act. The I T Act however divides the cyber wrongs in two groups-one group provided U/s. 43 attracting civil liabilities. But the offences U/s. 65, 66, 67-- tampering with source code, hacking with computer system, publishing obscene materials. S/70-- access into a protected computer or system etc. have been kept under the criminal law and system of the country along with Indian Penal Code- 1860, Criminal Procedure Code-1973, the Indian Evidence Act- 1872. This separation however appears to create more trouble than convenience.

15 * Internet Governance Project - on US role as to ICANN independent status – http://dec.syr.edu/igp - home htm ------------------------ down load – 8 – 9 – 05.
7 is going :-

18 * Supra – 12 -----Edn. 2004------P – 955
The last part deals with the general approach taken in the enactment to deal with the cyber torts. The IT provisions are being currently invoked to deal with cyber wrongs and crimes. Suhas Shetty -- Case * 19 u/s - 67 IT Act & S/465 & S/509 - IPC - at Chennai. This part also includes some insights in the form of suggestions, recommendations and opinions for due consideration of all concerned.
9.

METHODOLOGY

So far the methodology of the study is concerned, I found only analytical method was insufficient, so I had to pursue other methods like historical method, arm chair and empirical methods also. Basically I had to depend on the empirical method of study. I collected information, data, opinion and suggestions from various sources like libraries, journals and magazines, newspapers, periodicals, articles published in conferences, website materials. I also visited persons dealing with the subject matter under study, such as lawyers, police officials, computer professionals and experts and academicians.

I consulted teachers teaching computer science in colleges and instructors of college computer labs. I also visited IT consultants of established and well known consultancy firms like Price Water House, Salt Lake, Kolkata. I got the opportunity to see Mr. Sangram Keshari Das, (Manager - Engg.) VSNL – Kolkata – 54. And I meet Sri Sanjoy Sharma of CMC Ltd., Kolkata – 16. I visited the BSNL office at CTO Kolkata 700 011 and met Mr. Shiva Ratan, the Deputy General Manager (IT). According to him, the threat mail has been a common form of offence in the Internet. In early this year an e-mail was sent to Mrs. Sonia Gandhi, New Delhi AICC President, with a threat on her person by a man, Sikh by faith, from a Cyber Café in Durgapur. The Cyber Investigation Cell however rightly tracked and traced the offender and prosecuted him. Another recent case of threat mail has been recorded in Durgapur and in the investigation stage under the SDPO there.

I also visited the Technical Officer In-charge of the IN F L I B N E T - Computer Section and the Computer Department of this University. I visited the Cyber Crime Cell of Kolkata Police at Lal Bazar, Kolkata and talked with the responsible officials there on the subject of Cyber Crimes in India. I collected information from the Website of Indian Cyber Police, Mumbai, Bangalore and Chennai (www.indianchild.com.).

I regularly visited American Information Resource Centre (AIRC) in Kolkata to collect information, data and development in the concerned issues. The PIC Website (Project India Cracked) provided data about the hacking and defacements of Indian Websites by various hacking groups of different countries.

*******