INTRODUCTION

In my subject matter of interest “A Legal Study of Cyber and Intellectual Property Crime” I concentrate to study new forms of criminal activities with astounding advances in the Internet and web-based information and communications technologies (ICTs) and by exploiting the cyber-space. I made a thorough study on existing statutes, laws both national and international, various international treaties and conventions.

The object of my research work is to focus new insights into the new burning problem of the world with a desire to face the new challenge in solving the unsolved problems. This is a new and challenging subject and has ample scope for further research for contribution in this arena.

The crime on the cyber space is a threat to this new electronic field not only to our nation but it is an international problem. In India the subject is new, and little development has been made especially in the legal field. In India still there is no Specific Act or Special Statute on the subject except the Information Technology Act, 2000 which provides some sections under Chapter-X and XI deals with cyber crimes, penalties and constitution of Cyber Regulation Appellate Tribunal.

So far as the methodology of the study is concerned, I found only analytical method is insufficient, so I had to pursue with doctrinal and non-doctrinal methods as well. Myself confined with literary books, journals, reported cases of different courts, national and international. I have taken also help from various non-doctrinal research works. Some sorts of Social investigation, I have to visit the Criminal Investigation Department (CID), Bhowani Bhavan, Police Head Quarters – Lal Bazar, Telecommunications and I.T. Sectors.

To realize the subject of ‘Cyber Space’ and cyber crime’, it is pertinent to know the history and gradual development of modern computer and its application. The modern computers are the outcome of human efforts and geniuses of the world. With the advancement of Science and Technology, especially the Applied Physics, Electronics and Technology the modern computer reaches its peak. The Cyber Crimes on the other hand, are parallelly taking place with advancement of such Science and Technology.
Now we are on the deep wave of social anxiety with tremendous advances in Internet and web-based Information and Communication Technologies (ICTs). The law enforcement agencies are under great stress with the detrimental effects of ICTs upon various aspects of law enforcement, security and social order. The Internet is frequently depicted as a kind of dark virtual domain inhabited by mixture of computer hackers, organized criminals, extremist, and purveyors of pornographic images. Cyber Criminals exploiting the cyber space, Information and Communication Technologies to achieve their end. The present world facing the challenges of the cyber criminals against legal systems critical national infrastructures and security agencies as a result of the use of the new Information and Communication Technologies by criminals. The International bodies have to take effective measures to govern cyber space and to tackle the emergent situation.

“In true sense of the term ‘cyber space’ it was developed through the successful and interactive networking of four computer centers in 1969-70 in the U.S. The IPTO under ARPA achieved this through some novel technological break through like packet switching, Interface Message processors and the appropriate software. “The Internet began in 1969 as ARPANET and effort by the U.S. Department of Defense to enable diffuse researchers at various sites across the country to communicate and collaborate”¹.

“The new world of digital technology presents difficulties for law-makers as well, largely because this world of information differs in some important ways from the world we have grown used to inhabiting. Cyber-space is an added new world, where our ordinary intuitions are not always reliable. It is also an area where legislation is not always easy to craft. The law (Statutory or otherwise) providing answer to these problems or dealing with the information technology is often loosely referred to as the ‘Computer Laws’ or ‘Information Technology laws’².

“Cyberspace is a world in which every (digital) product carries with it the possibility of an almost magical speed, ease, and precision of replication. Cyberspace possess difficulties for those who understand something about copyright because, for the most part the status quo of the print world does not carry over into the digital world.”³.

---

India has entered into the new information age in the mid of 1990. The VSNL opened Gateway Internet, Access Service (GIAS) in the month of August 1995. In January, 2000 Securities And Exchange Board of India (SEBI) has granted permission for on line trading.

A separate department, Ministry of Information Technology was established as high priority section and new Internet Service Provider (ISP) policy was taken up issuing private ISP licenses in May, 20004.

In the current age of advancement and revolution of Information and Communication Technologies, the Government, organizations and people are getting hooked into the cyber world for their various needs and operations. The people are relying on computers and Internet for mail, on-line shopping and banking, airlines and rail tickets, trading (e-commerce) and intellectual properties. This new technologies sometimes poses dangers to us in an unprecedented way by exposing their identities in the public domain. We recently witnessed that details of our personal information, such as name, address, passwords and bank accounts are in the process of being attacked by hackers, fraudsters, terrorists and criminals freely roaming the cyber world.

The users are under various risks and threats of hostile viruses, hackers accessing computer system and stealing vital information like credit card details and committing fraud, unsecured wireless networks, spy ware on system, identity theft and crimes on copy-rights, trademarks and trade secrets.

In Chapter-III I discussed brief history of cyber crimes. The opportunity for creative computer hardware and software invention became available in the 1970s through the academic explorations at the all-made Massachusetts Institute of Technology (MIT), Tech Model Railroad Club (TMRC). The TMRC was formed in 1946 and continues to this day as an actual model railroad club. The original members used their skills learned at MIT to employ advanced control systems and became the white hat backers.

During this period the word hacker began to represent a technologically focused individual and the term was applied to those who spent time crawling under the railroad tracks at the Railroad club facility with the primary objective of connecting switches to relay with the cables. Back in the early 1960s and 1970s a “back” meant a prank of the kind that the student and the MIT faculty played on their

School or on their rivals as wrapping the entire root in tin foil. A “good hack” would have been some creative exploit that would have impressed observers to remark”, How in the [heek] did they do that? Famous White Hats (a term borrowed from black-and-white early western movies that indicated the heroes, a good guys of the story) at MIT included Alan Kotok, Steward Nelson, Richard Green-blatt, Tom Knight and Bill Gosper. These early hackers were known to work in the lab for 30-hours-plus shifts and found the primitive computers so fascinating that they forgot about everything else while they were working on them. They even fought themselves to pick locks in the MIT, Computer Science building to gain access to the computers after hours. From the white hats’ perspective, this lock-picking was not criminal activity because they felt they were simply putting all available equipment to its best use. These early hackers were not the criminals. But highly talented programmers committed to finding novel solutions to difficult problems. If the type of software or hardware they wanted was not available, these hackers would develop it. The search for new solutions created a hacker community of people who began to share computer code while building an open and freely accessible body of knowledge among peers. It was the sort of intellectual environment that is afforded to academics and is protected by academic freedom and tenure.

After the 1960 and 1970s, the cyber frontier blow wide open, with white Hat hackers across the United States exploring and figuring out how the wired world worked and paving the way for incredible growth along the information super highway. 

Besides, the white hats the black hats originated in the United States from black-and white western movies and was meant to represent the villains, or bad guys. The Black Hat hackers are typically not committed to or behaviorally ruled of the Ethic. Though there is considerable debate about when the term ‘Black Hat’, or ‘Cyber Criminal’, was actually coined.

In 1984, BT prestal operated a text information retrieval system that was accessible over the public switched telephone system by means of a modem. The electronic mailbox information could be retrieved and viewed on a personal computer or on a television screen.

In 1988, the British press reported the cyber crime exploits of Nicholas Whitley known as the Mad Hacker. In May 1990, he was one of the first crackers in Britain to be convicted under the Criminal Damage Act of 1971. Whitely was given a

---


custodial sentence for cracking into the computer system at the Universities of London, Bath and Hull, causing them to crash (Mulhal, 1977a).

From 1971 through 1998, both 'White Hat hackers’ and Black Hat crackers’ received media air time for a variety of cyber exploits. Then in 1999, a new cyber-related fear emerged. Two professional soldiers in China’s People Liberation Army proposed a new way of waging war by using terrorist attacks and cyber attacks on critical infrastructure as a way to key a super power adversary reeling. But it was unclear whether this threat was an emerging real one just fiction.

What Is Cyber Crime?

'Cyber Crime', is a rather pretensions expression to refer simply to the use of computers by criminals. It is a crime by criminals by exploitation of computer and Internet. Cyber Crime is a new form of crime now being committing by criminals of the modern times. It has gained very fast recognition demanding immediate attention, follow-up and combat. The legislature, judiciary and the law enforcing authorities have to face this new challenge.

Who are the Cyber Criminals?

Understanding who the new cyber criminals are not simply a matter of thinking about old crimes in a new ways. Cyber criminals are the new criminals who use and exploit ICTs for the commission of new forms of crimes.

There are three basic categories in which we can categorize cyber criminals: hackers and phreaks, information merchants and mercenaries and terrorists extremists and deviants.

Chapter-IV deals with statutes dealing with cyber crimes.

Every state has a statute deals specifically with computer crime. The first wave of computer crime legislation appeared in the late 1970s, as computers became more widely used in business, legislative activity in the mid-1980s was likely a part, a response to the report of the American Bar Associations.

The Indian parliament enacted the Information Technology Act, 2000. This Act is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations.

The “intellectual property crime” in the cyber space encompasses three general areas of criminal endeavour. The criminal infringement of copyrights, the criminal misappropriation of trademarks, and the theft of trade secrets have been discussed in Chapter VII.

It includes the strategy for prevention and protection of intellectual property crime. Intellectual property protection is a vital part of social, cultural and economic development. A country could reach these goals with the strong Intellectual Property Protection. Recently world observed the downloading of movies and songs are on the rise. The creators of songs have known that whatever they produce will be immediately pirated-stolen – and they will not be provided, the means to develop their talent. Crimes on the NET over trade-marks and trade secrets are also prime concern of world’s anxiety.

Chapter-VIII covers International Intellectual Property Treaties and Human Rights. The last Chapter of the thesis contains some observations which I have drawn in course of investigation of various modus operandi adopted by the cyber criminals.