CHAPTER – 1

CYBER CRIME IN TAMIL NADU (AD 2000 to AD 2009) – A STUDY

INTRODUCTION

The foremost reason for the expeditious advancement in technology is the computer. The Inter Networking Group was set up with Vint Cerf as the Chairman during the year 1972 who became popular as the “Father of the Internet”. The term “Internet” was used for the first time in 1982. Transmission Control Protocol or Internet Protocol became the global language of the internet in 1983. The scientists of United States of America began research on computer networking and based on the research carried over by the Advanced Research Projects Agency (ARPA), the Internet came into existence with its first name, ARPANET. This was first bestowed on military department of USA. In 1991, for the first time, the National Science Foundation (NSF) which funded the Internet infrastructure in the United States relaxed its ban on commercial applications and this facility came into effect for public usage.

The internet is a global network of individual computers which are interconnected through a complicated structure of servers. It is a network, linking various computers and these are functioning on hardware and software. The internet is considered as the voluminous library and search engines in the world at our fingertip. This is the transport instrument for the information stored in files between computers. In 1984, William Gibson coined the term “Cyber Space” in his fiction novel “Neuromancer”. Cyber space is a bio-electronic environment that is literally universal. It exists wherever there are telephone wires, coaxial cables, fibre-optic lines or electro-magnetic waves. This environment is inhabited by
information and knowledge, existing in electronic form. The online world had now linked the average person to cyber space.

The innovation of the Internet and the World Wide Web (WWW) in the past two decades seems to have conquered the cyber space and thus created a fictitious world filled with an unlimited amount of information. India is fast emerging as a major hub of cyber crime.

Tamil Nadu was one of the forerunner state to come out with an I.T. Policy in the year 2005. With the passage of time and the immense changes that have taken place in technology, a new I.T. Policy is not only essential, but also necessary to take Tamil Nadu to attain an eminent position in I.T. Tamil Nadu has been amongst the top three states in terms of Information Communication Technology investments and production. The mushrooming multinational and national business establishments having presence in Tamil Nadu is a testimony to this.

Cyber crime, computer crime, e-crime or electronic crime, hi-tech crime refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Cyber crimes may be unleashed against persons, property and government. It is the latest and perhaps the most complicated problem in the world. It is being increasingly used as a place to commit crime using personal computers, as well as networked computers. Net-crime refers more precisely to electronic cracking and to denial of service by the exploitation through internet. Online fraud or cheating is one of the most lucrative businesses that are growing today in the cyber space. Our dependence on cyber space is bound to grow in the future.
Cyber crime is an ever-growing social problem that poses new challenges for computer security specialists, legal professionals, academics, public citizens, and law enforcement agencies, regarding the detection, prevention, investigation and prosecution of cyber crimes. There are several types of cyber crimes and they include among others, Hacking; Spam; Credit Card Fraud; Cyber Bullying; Phone Phreaking; Cyber Terrorism; Piracy; Cyber Stalking; Identity Theft; Denial-of-Service attacks; Computer Worms and Viruses and Physical damage to computer etc.

Internet in India

Videsh Sanchar Nigam Limited (VSNL), a public sector company, was the first to introduce internet in India in 1995 in 6 cities. Internet has brought great changes in the Indian economy, and now Indians are among the most frequent users of the internet. Before that, Internet had been in India for many years in the form of ERNET (Education and Research Network). However, it was not possible for common people to get access to it, as it was meant for only the educational and research communities. This followed the policy laid down by the American Internet manager National Science Foundation (NSF), at that time. At present, internet is operated not only with the help of computer, but also with cellular phones.

Consequently issues surrounding cyber crime have become high profile. These encompass a broad range of potentially illegal activities which paved the way for enacting the law. Hence, the Government of India introduced Information Technology Act, 2000 which came into effect from October 2000. This Act addressed the issues including tampering with computer source documents, hacking into computer system, publishing of information which is obscene in
electronic form, breach of confidentiality & privacy and publishing false Digital Signature Certificates.

The Act also made consequential amendments in the Indian Penal Code, 1861 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions that deal with offences relating to documents and paper-based transactions. In view of the fast growing internet users, Information Technology (Amendment) Act, 2008 was introduced and that came with effect from 27th October 2009. The new and improved Act aims at tightening procedures and safeguards for monitoring and interception of data to prevent cyber crimes.

Computer Emergency Response Team-India (CERT-IN) was established by Department of Information and Technology, Government of India in January 2004 with a specific mandate to respond to computer security incidents. It has been designated as Nodal Agency for coordinating all matters related to cyber space for enhancing cyber protection, enabling security compliance and assurance in Government and critical sectors which facilitating early warning and response as well as information sharing and co-operation.

**Review of Literature**

The issues of cyber crime had been addressed by the researchers, academicians, law makers. Various books and articles have been published on this theme.

R.K.Suri and T.N.Chhabra in their book ‘Cyber Crime’ (2002) discuss the encryption being used by criminals and terrorists through advanced technologies to hide their activities. Indications are that use of these technologies will continue and expand, with a growing impact on law enforcement.
Paul T. Augustine in his book ‘Encyclopaedia of Cyber Crime’ (2007) talks about Computer Crime or cyber crime as a crime where a computer is the target of a crime or is the means adopted to commit a crime and in his another book ‘Combating Cyber Crime’ (2007) discusses the impact of Information and communication technologies on societies bringing positive change faster than any other current phenomenon.


Colonel R.S. Prasad in his book ‘Cyber Crime Combat Strategies’ (2004) opines that cyber crime is the new social phenomena and turning out to be the most dangerous one and it is affecting everyone – individual, organizations, governments, nation states and the international community.

Atul Jain in his book ‘Cyber Crime Issues, Threats and Management’ (2005) has discussed the stability of modern society in relation to the ubiquitous nature of information and communication technologies which pervades all aspects of human activity.

Melanie Kowalski in his e-Article by name ‘Cyber-Crime: Issues, Data Sources and Feasibility of Collecting Police: Reported Statistics’ points out that the cyber crime is very difficult to crack down, because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too,
which can make things really complicated when a criminal launches an attack in another country.

Hemavathy Alaganandam, Pravin Mittal, Avichal Singh and Chris Fleizach in their e-Article under the title of ‘Cyber Criminal Activity’ talk about the rapid growth of the Internet, not just in terms of users, but also in terms of functionality which has allowed entire industries to move their operations, and importantly their money, onto the Internet. This channelised naturally towards a prolific growth in criminal activity conducted solely through virtual means. Although cyber crime is not a new phenomenon, computers have always proved to be valuable targets, the essentials of the Internet has necessitated a change in our understanding of security, risks and threats.

In the Annual Report of National Crime Record Bureau (NCRB) for the year 2002, it has been said that Cyber crimes are new to India that is expanding rapidly on use of internet spreads. Till now, the complete data on cyber crimes were not available. Concerned with the seriousness of these crimes, NCRB has endeavoured to collect statistical information on cyber crimes under Offences registered under the Information Technology Act, 2000 and Offences under the Indian Penal Code. Since then NCRB has been publishing, in its Annual Reports, the data related to cyber crimes.

In the publication of Crime Branch C.I.D., Tamil Nadu under the heading of ‘Crime Branch CID, Tamil Nadu - A Retrospect (1906-2010)’, highlights the use of modern technology particularly by criminals who are educated, intelligent, highly motivated and techno-savvy. Statistics clearly suggest that cyber crime is one of the sporadic growing areas of criminality. The Government
of Tamil Nadu through State Crime Record Bureau (SCRB) of Tamil Nadu Police has been publishing the statistics on the incidents on cyber crimes.

AIMS AND OBJECTIVES OF THE RESEARCH

Though several books and articles have been published in India, they do not reflect the emerging cyber crime scenario in Tamil Nadu. Hence, an attempt has been made to capture and highlight multiple facets of the issue with particular reference to Tamil Nadu.

The main objectives are:

• to trace the evolution of cyber space.
• to examine the background and provisions of the Information Technology Act, 2000.
• to study the types and incidence of cyber crimes in the global and Indian contexts.
• to address the cyber crime scenario in Tamil Nadu.
• to assess the impact of cyber crime with special reference to Tamil Nadu.
• to address steps to prevent cyber crime.
• to present conclusion and make suggestions to shrink the cyber crime.

PERIOD OF STUDY

The period of study commences with 2000 and ends with 2009. It was in the year 2000 that the Information Technology Act came into effect, which was amended in 2008. Ten years of its existence and impact on society will be reasonable period to assess the Act. Hence, 2009 has been fixed as terminal year.
METHOD OF STUDY AND SOURCES

Historical and analytical methods are used to study the phenomenon. The study is carried out with the help of both primary and secondary sources. The primary sources are mainly on statistics from the Annual Reports of the National Crime Record Bureau of India, State Crime Record Bureau of Tamil Nadu and details furnished by the Crime Branch C.I.D., Tamil Nadu. Statistical tools have been employed to highlight various dimensions of cyber crime. Certain details were obtained through Government Orders, Magazines, Journals, Newspapers, Books, Pamphlets and Interviews. Extensive use of web sources has been made to collect data on cyber crime.

There are number of secondary sources which give more information about the cyber crimes. English and Tamil daily newspapers Dinakaran, Dinamalar, The Times of India, Daily Thanthi, The Hindu, Deccan Chronicle have provided informations on cyber crimes.

CHAPTERISATION

The work is divided into eight Chapters including Introduction and Conclusion.

The first chapter, Introduction, covers the significance of the theme of research; the history of cyber space, cyber crime, objectives of the study, Scope of the Study, Methodology adopted, Sources used and the Chapterisation.

The third chapter titled “Cyber Crime: A Global Perspective” presents the global cyber crime scenario using data from diverse sources. The chapter highlights the growing incidence of cyber crime.

The fourth chapter titled “Cyber Crime in India” presents the cyber crime scenario in the Indian context using data from National Crime Record Bureau. This chapter also highlights the trends of cyber crime.

The fifth chapter under the heading of “Cyber Crime Scenario in Tamil Nadu” highlights types of these crimes occurred in Tamil Nadu broadly using data of National Crime Record Bureau and State Crime Record Bureau and the efforts taken by law enforcement agencies.

The sixth chapter titled “Impact of Cyber Crimes” details the impact of cyber crimes at the level of individual, organisation and Government level.

The seventh chapter under the heading of “Preventive Measures in respect of Cyber Crimes” deals with the precautionary methods to be adopted to fight cyber crimes.

The last chapter, Conclusion, sums up the findings of the thesis and make suggestions to reduce the cyber crime.