CHAPTER - VIII

CONCLUSION

A slew of amazing technological innovations disrupted and transformed the life and work environs. Such innovations have been relentless in diverse fields such as robotics, genomics, computation, automation and communication, principally through internet. In particular, internet has radically reshaped the way people live and work. It has truly globalized the world, erasing time zones, consequently, leading to the ‘death of geography.’ It created a new world, the cyber world. At once, it created plethora of opportunities, immense benefits and enormous challenges.

An outcome of US Defense Department research project, ARPA, internet evolved over the years with the creation of Internet Protocol and World Wide Web. The entry of internet into the public domain massively augmented productivity and helped the delivery of services efficiently. The global impact of internet is indeed immeasurable. The adverse impact of internet, however, became manifest within few years. The genesis of online predators spawned a new genre of crimes which are of several types and included hacking, cyber terrorism, identity theft, email spoofing, cyber stalking, software piracy, digital forgery, child pornography, distributed denial of service attacks and others. These crimes engendered immense misery and anxiety at the individual level, caused massive economic loss for the individuals, commercial establishments and the governments.

The United States of America, the originator of Internet, responded to the emerging scenario of cyber crimes by pursuing different means and methods. It
created National Cyber Investigative Joint Task Force which coordinates with law enforcement agencies and intelligence community including CIA, Departments of Defense and Homeland Security and the National Security Agency. President Ronald Reagan signed the Computer Security Act of 1987, an attempt to protect federal agencies' computer databases. In 1988, Computer Emergency Response Team (CERT) Coordination Center was founded with money from Advanced Research Project Agency of Defense Department – the same agency that developed the Internet's predecessor ARPANET.CERT is a central reporting center for Internet security problems. It is part of the Networked System Survivability Program.

Internet has made cyber crime a trans-border problem which assumed global dimension. Not surprisingly, international responses also emerged to curb cyber crime. Efforts are also on to harmonize national legislations. The Interpol is seized with the issue. Globally, 82 countries have signed and/or ratified a binding cyber crime instrument.

Since the advent of internet in India, in the year 1995, the number of internet users has surged phenomenally. The current statistics (2016) reveal that there are 462 million internet users, constituting, approximately 35 percent of the Indian Population. Surprisingly, Indian internet users surpassed the number of internet users in the United States, occupying the second position in the world, behind China. Inevitably, therefore, the issue of cyber crimes garnered public attention. Unlike other countries where security establishment raised the subject of cyber crime, in India the legal initiative came from the business community involved in paperless international commercial transactions. The lead was taken,
in particular, by National Association of Software and Services Companies (NASSCOM), a trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) industry and a global trade body with over 2000 members, of which over 250 are companies from China, European Union, Japan, the United States and United Kingdom. NASSCOM's member companies are in the business of software development, software services, software products, IT-enabled services and e-commerce. NASSCOM argued forcefully that existing laws were inadequate to address the problems arising out of cyber crimes. Convinced by the arguments, the Government of India enacted the Information Technology Act, 2000. The Act gave legal recognition to transactions, carried out by means of electronic data interchange. To facilitate such transactions the Government amended several existing legislations.

To enable effective enforcement, the IT Act defined terms associated with computer and commerce including computer network, secure electronic record. Several Sections of the Act detailed the nature of the crimes, levied penalties of fines and imprisonment accordingly. The crimes were made cognizable and non-bailable. The original intention of the enactment of the IT Act seems to protect the economic interests of the business community. However, the Amendments to the IT Act, 2000 carried out in 2008 enlarged the scope of the Act to cover a few more cyber crimes under its ambit. The new and improved Act aims at tightening procedures and safeguards for monitoring and interception of data to prevent cyber crimes. Amendments laid down the procedures of investigation and the powers of the police to do so. The Nodal agency, Computer
Emergency Response Team–India (CERT-IN) is vested with the authority to issue instructions to block offending websites.

Even as countries grapple with the spike in the cyber crime, the outcome of the efforts to curb the same is apparently unsatisfactory as evidenced in the statistics on global cyber crime. The United States of America, according to the available data, continues to record steady increase in the commission of various cyber crimes. Money lost by the United States through cyber crime has been progressively increasing since 2005. Similarly, United Kingdom also lost vast amounts of money because of cyber crimes. The scenario is no different in other countries. While some countries are classified as low risk countries, other have been categorised as high risk countries depending on their vulnerability. India finds a place in the latter. Obviously, cybercrime is trending on internet.

India, too, witnessed a surge in cyber crimes. National Crimes Record Bureau began collecting data on cyber crimes in 2002. In the first year of data collection, a total of 809 cases were reported. While 70 cases were related to IT Act, a substantial number of others were related to Indian Penal Code (IPC) sections. Majority of the cases under IT Act were concerned with hacking and cyber pornography. Of the 738 cases registered under Indian Penal Code, majority of them fell under criminal breach of trust or fraud, forgery and counterfeiting. The number and types of cyber crimes followed similar pattern in the following years till 2007. However, in 2008, of the 468 cyber crimes reported the number cases under IT Act exceeded the number of cyber crimes related to IPC sections. Nevertheless, the pornography and hacking dominated other cases related to IT ACT. The nature of crimes under IPC sections also followed the pattern of earlier
years in which criminal breach of trust, forgery and counterfeit dominated. Majority of the criminals were relatively young, most being in the age group of 18 to 45. This can be countered by including in the curriculum of the school and college students about the cyber crimes and the related penal provisions. This will deter the above mentioned age group offenders from resorting the cyber crime. Many important cases were reported in the media focusing more attention on cyber crimes. The convictions in cyber crime cases were few and sporadic in comparison to the number of cases reported. The increasing rate of conviction is necessary which will pose a direct threat to cyber offenders.

Taking serious note of the increasing trend of cyber crime, the Government of India and business community joined hands in the creation of agencies to deal with diverse aspects of cyber crime. In addition to the aforesaid Computer Emergency Response Team–India (CERT-IN) established by the Government of India, NASSCOM stepped in with the establishment of Data Security Council of India (DSCI) as a Self Regulatory Organization (SRO) to promote data protection through best practices and standards, in line with the evolving global regulatory landscape.

Tamil Nadu, a major destination for leading national and multi-national software companies, has witnessed the commission of cyber crimes. The State Crime Record Bureau began collecting data on cyber crime in 2000 itself, much before the National Crime Records Bureau started doing it. Initially, the number of cases was few. In 2000, for instance, only six cases were reported, two were related to IT Act and the remaining was related to IPC sections. The number did not increase in the next few years. The number of cyber crimes doubled in 2004
and since then, the number of crimes remained in double digits. Between 2000 and 2009, the period of the study, a total number of 143 cyber crimes were reported, in which 106 cases were related to IT ACT and rest of the cases were registered under various sections of IPC. In keeping with the national trend, the cases related to pornography, hacking and breach of confidentiality dominated the cyber crime scenario in Tamil Nadu.

The State was one of the first ones to come out with the Information Technology policy as early as 2002. One of the major objectives of the policy was to develop Research and Development capabilities. It has created a Computer Forensic Lab and equipped it with updated software. In 2002, two Cyber Crime Cells were created, one exclusively for Chennai City Police and the other with state wide jurisdiction under Crime Branch-CID. Both were adequately staffed. Necessary facilities, in terms of computers and software, were provided to these units. Sufficient funds were allocated for the efficient functioning of the cyber crime units. The nature of cyber crimes reported in Tamil Nadu included online fraudulent fund transfer, hacking of e-mail ids, fraudulent online job market, posting of obscene messages, fraudulent use of ATMs, e-mail threats to Very Important Persons (VIPs), bomb threats to vital installations, misuse of net banking. Though the crimes have been investigated, the conviction rate is low, again, in keeping with the national trend.

As elsewhere in the world, cyber crime caused incalculable damage to personal reputations, left a trail of misery among the victims and devastated the fortunes of several companies. The government institutions like banks and recruiting agencies fell victim to cyber crimes. The revenue loss was massive. The
proliferation and extensive usage of social networking sites such as Facebook, Flickr, LinkedIn and importantly, the smart mobile phones increased the probability of the commission of cyber crimes.

Unless adequate safety measures are instituted and adhered to diligently, cyber criminals will continue to operate with impunity. As the jurisdictional conundrums in investigation and conviction will facilitate them, it can be safely predicted that only international co-operation coupled with national capabilities can counter, effectively, the trend of increased cyber crime. Also, there is a compelling need to create awareness of the cyber crimes and their consequences, particularly among the younger generation. This onerous task can be taken up by the specialized agencies involved in dealing with the cyber crime, Non-Governmental organizations, legal fraternity, media houses and also by the research institutions for creating awareness among unwary parents and youngsters about the dangers inherent in treading dangerous areas in the cyber-world. Academic institutions can direct research on the theme focusing on different dimensions of cyber crime. Dynamic public–private partnership can indeed structure a safety net against cyber crimes.