CHAPTER 7

CONCLUSION AND SUGGESTIONS

The conclusion and suggestions arrived at after completion of study is not a monolithic one. They are, more often than not, layered one. It was realized that in a research it is not possible to proceed with an unencumbered arguments in most of the circumstances. These conclusions and submissions must also be read in conjunction with conclusions at the end of each chapter. To avoid repetitions some of those ideas which have been already referred in those conclusions have not been much emphasized here.

Information Technology has transformed the world into a global community. It has entered into our homes, and all at increasing risk of being affected by cyberattack. Everything about human lives is in some manner affected by computers. So, it has been observed by Waleter B. Wriston in his book that “Technology has made us a ‘global community’ in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long.”1

The law breakers get a space where they remain unidentified and can lure the prey. In reality, cyber terrorists not only target individuals or a nation, but they have world on the target. Cyberspace is one such gray area, which provides heaven to the cyber terrorists. Now internet made the world borderless so criminal activities done by the terrorists in the cyber space attract the attention of the world. Most of the financial institutions and critical infrastructures all over the world have embraced IT to its full optimization. Reports suggest that cyber attacks are understandably directed towards economic and financial institutions. Increasing dependency on the information technology leave nations on a platform where no alternative finds, once it collapses.

Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. However, it has also added a new dimension to terrorism. Cyber terrorism has developed with the development of computer network. Cyber terrorism is any harmful activity in the cyberspace which may cause damage to a person, property or even the state or society as a whole or in another words ‘Terrorism’ related to cyber is popularly known as ‘cyber terrorism’.

Cyber terrorism is different from the conventional crimes so the law enforcement agencies find helpless to curb it within the existing framework of infrastructural mechanism. India is not armed with to fight with the menace of cyber terrorism, except the Information Technology Act, 2000 and National Cyber Security Policy, 2013. Critical infrastructure has not defined and identified in the policy and in IT Act, 2000. This is the main reason that cyber terrorism relatively new variety of terrorism is posing a challenge to the legal regime.

The menace of cyber terrorism is a ‘technological scorn’ which is not confined to one or two countries but the whole world is at stack and India is no
exception to this new age menace. However, Indian Parliament has enacted the Information Technology Act, 2000 which came into force on October 17, 2000. This Act is only source to deal with the cyber criminality. To fulfill the gaps, it was amended in 2008, came with the meaning and punishment of various other kinds of cyber crimes, including cyber terrorism. The Indian Penal Code, 1860 is found insufficient to reply internet age crimes, particularly cyber terrorism. The great architect of Indian Penal Code, Lord Macaulay did not imagine about computer or internet, when he prepared it.

In the era of computer where Information Technology and other developments have crossed the national frontiers whereas the law is still struggling to define and redefine the boundaries to check on cyber crimes. The cyber laws specifically, the Information Technology Act, 2000 is for the prevention and control of cyber crimes within the country’s territorial jurisdiction. A common vision is required for the secure and hygienic cyberspace.

7.1 Conclusion

The information age is developed as heaven for the terrorists, large terrorist organizations are using information technologies, where they can select targets and types of weapon and can finalize their plans of attack not only in physical world but in virtual world as well. Under these circumstances it is high time when one and all have to take notice of the danger involved in the information highway. Cyber terrorism is not a problem of one person or country. It has seen that Internet offers terrorists unparalleled opportunities. There is a saying “diamond cuts diamond” in the same way Information is the best form of

\[\text{Section 66F, Information Technology Act, 2000. As Amended 2008.} \]
protection. Empowered and safe cyberspace from all kind of disruptions is the best measure to deal with the menace of cyber terrorism. It is necessary to make cyber system enough strong to give better protection from any cyber intrusions. In addition, new rules and regulations must be developed by law enforcement agencies and new software and techniques to address the new challenges in the cyber world.

Cyber terrorism having international character, usually it interrupts and destroys the critical infrastructure far away from the place of offence. Sometimes it may be in the same country or some other country. Therefore, it is dire need of the hour that an active cooperation is required at international level for making policies and common programmes. All the nations in the 21st century has considered the cyber threat and started to adopt strategy to address the new challenges in the borderless world. The European Convention on Cyber crime was an admirable effort in this regards as it laid down guidelines to be followed by the member states in combating cyber crime also suggested measures to be initiated by the states for restructuring their cyber laws to meet the new challenges.

All kinds of cyber crimes are not included as crimes by many countries, which become a real challenge when cross-country cyber crimes are involved. The only way out is to enact a global cyber law applicable to all the countries of the world. The point is that cyber terrorists should not be spared, wherever they are in this world.

A world wide survey suggests that only a few countries have updated and come with effective cyber policy on cyber terrorism and protection of information

---

4 Effective from June, 2001.
and critical infrastructure. This indifferent or conflicting approach of nations towards the curbing of cyber terrorism pose a real trouble in replying the cyber terrorism and at the same time it also provides heaven for the cyber criminals to flee from detection and punishment. Cyber terrorism perhaps is the heinous and deadliest form of terrorism spreading over the world in the internet age, which has to be curbed by adopting a global preventive strategy. The solution to the problem therefore, lies in the concerted and united efforts of nations around the world and their mutual cooperation in fighting against cyber criminality.

Other way round it can be submitted that all the law enforcement agencies are facing four main problems relating to detection and prosecution of cyber terrorists which may be technical, legal, operational and jurisdictional.

In relation to technical challenges, cyber crimes such as hacking of a website, data didling, espionage, fishing, blackmailing etc. involve finding the actual source of communication and which is itself a complicated task. So, the cyber terrorists find it easy to impersonate on the internet and hide their identity.

The legal challenge to tackle the cyber terrorism criminality is no longer only a job of the developed countries alone but in recent decades it becomes worldwide problem. The accepted techniques to deal with the cyber terrorism are laughable particularly, in case of cross-country crimes. It becomes more challengeable, when there is no fixed meaning or definition on the cyber terrorism, crime in one country may not necessarily a crime in another country. There are hardly thirty countries in the world which have enacted comprehensive laws on cyber crimes. In the absence of an adequate cyber laws, the cyber

---

criminals carry on their illegal activities undeterred. Therefore, effective handling of cyber crimes requires a legal framework which is equally applicable to all the countries. The cyber laws should also be responsive to the fast developing information technology.

The operational challenges faced by the law enforcement agencies because of lack of adequate cyber forensic technology for dealing with cyber crimes constitute another in-road which renders it difficult to collect and preserve sufficient evidence against the person accused of cyber crime, thereby resulting in his acquittal by the court. The traditional modes of procuring evidence are unsuited in case of cyber crime investigation because most of the evidence exists in electronic form. Therefore, there is dire need to develop suitable computer forensic mechanism for effective handling of cyber crime investigation.\(^6\)

In the context of electronic evidence, it is noteworthy to point out that despite of the fact that e-commerce has achieved a new success point by reducing paper-work and ensuring quick transactions. If we see Indian scene, it has not been generally accepted because of the technicalities involved in it. People still believe paper-based documents are considered more trustworthy than the paperless electronic records. Although all above are true but not in totality, after the entering of computers and internet into our houses and with the expansion of e-commerce and legal recognition of e-contracts in business transactions, there is change in the mindset of the people and they are gradually adapting themselves to the new e-environment and finally switching over to paperless electronic transactions.

\(^6\) Id. p. 11.
The jurisdiction is the worst causality of the technological spree. It creates hurdles in efficient handling of cyber terrorism investigation. In fact, jurisdiction is a broad concept which refers to whether a court has power to adjudicate. By their very nature, the majority of Internet crimes, including cyber terrorism, are State or country. In case of cross-country cyber dispute or crime, the problem often arises as to the law of which country would be applicable to the case in hand. “While some statutes such as the CEAA as shown in United States v. Ivanov\(^7\) explicitly state they are to be applied extraterritorially, many contain no such provisions and leave the jurisdictional questions for courts to decide.”\(^8\) Other then this National Informatics Centre (NIC), Indian Computer Emergency Response Team (Cert-In), National Information Security Assurance Programme (NISAP), Indo-US Cyber Security Forum (IUSCSF), and India Anti Bot Alliance, etc. are doing their job well in protection information critical infrastructure.

### 7.2 Suggestions

The world is changing very fast as the internet has grown exceptionally and gets space in our life. Dependence of human being on cyberspace for social, economic, governance, and security and other purposes has increased. At the same time the dimensions of computer-related crimes are also expended. Therefore, it is need of the time to adopt appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cyber terrorism with stern hands. A slight delay in detection gives enough time to cyber terrorists to manage or delete or destroy the important data to evade detection. Very important point is that the peculiar nature of cyber terrorism provides safe zone to the terrorists and they never be face to face, as happened in traditional terrorist attacks. This

---

\(^7\) 175 F Supp 2d 367 (D Conn 2001).

\(^8\) F. Lawrence Street, Mark P. Grant, *Law of the Internet*, pp. 7-18, LexisNexis, 200).
peculiar nature facilitates the terrorists to continue their terrorist activities without difficulty and even without the fear of any identification, arrest or prosecution. Therefore, a multi-facet and concerted approach of all law enforcement and IT experts is required to curb this menace in the cyber world. International cooperation is a key element in addressing the challenges of cyber security particularly exchange experiences and share best practices for protection of information infrastructures.

A cumulative and active approach of citizens, institutions, industries and the government is required for the prevention and detection of cyber terrorism. Therefore, an effective and sound strategy on cybersecurity is the only solution for the prevention and combating of cyber terrorism. All nations who are vulnerable to cyber attack shall come at one platform for curbing this menace by information sharing of the incidents of any cyber attack and strategy to protect the information critical infrastructure. L.C. Amarnathan also suggest that media can play an important role to play in warning people against the possible dangers and evil effects of cyber crimes on victims and also the nation and the safety measures which are necessary to combat this high-tech criminality.

Effective implementation of law and policy is another appropriate regulatory measure to address the new challenges of information technology. It also reduces the incidents of cyber crimes.

---


Prevention is always better than cure. It is always better to take certain precaution while operating the net. Some other suggestions to prevent and reduce the incidence of cyber terrorism at domestic level are as follows:

7.2.1 Take Basic Computer Security Precautions on your Computer

It has shown by researches that users are unlikely to be the victim of an Internet security attack. Statistics indicates that instead of hacking by outsiders, maximum security breaches are the consequences of insider misconduct it may be ignorance of the users. Users must take reasonable precautions to secure files and data on their computers, e.g., back up important files, use an updated virus scanner, regularly monitor for download and install security patches from the vendors of the software, use a strong secure password for network access controls, and ensure permissions are set properly on files that can be accessed by others.

7.2.2 Self-Regulation by Computer and Net Users

Individuals generally reveal their personal information while transacting online. In this process their personal information becomes available for unwanted cybercriminals. A self-regulatory approach is the best way for protecting privacy on the Net is worthwhile both in itself and as a way to avoid government regulation. Self-regulation may be suggested as one of the practicable solution to reduce the incidence of cyber crime. It is a process of developing a healthy code of conduct by adopting a policy of restraint by both, the computer users as well as the service providers. Internet Service Providers (ISP) can play a crucial role in eliminating online crimes taking some self regulatory initiatives. To start with, ISPs can collectively set out an ethical code of conduct to be followed by them while extending internet services/facilities to the users. Likewise, they can lay down the conditions through a written agreement binding the users to refrain from
indulging in illegal activities. Besides, they may also specify in the contract that breach of these conditions would lead to termination of the internet services.

7.2.3 Encryption Technology

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. This process protect the information from unauthorized persons and it can be used only when it decrypt by the authorized person. Therefore, encryption technology shall be made mandatory at all levels of government, semi-government and non-government organizations and commercial organizations which are depended on the computer technology and having critical infrastructure. They also appoint well trained Information Security Officers who should be responsible for overall protection of computer resources. The encryption technology also helps to protect data and communications from unlawful and unauthorized access, disclosure or alteration and also helps to keep safe valuable secret information over inter-connected computer and networks. In the same way another technique also used for cyber security, known as steganography. It is used as a safeguard against network invasion. It is a technique of obscuring information in a manner so as to prevent its detection. It involves writing that is not readily discernible to the casual observer.

7.2.4 Intrusion Management

The centralized management of intrusion-based security technologies can be used as preventive strategy called as the ‘intrusion management’. It can be used for testing, detection and investigation of cyber crime. Intrusion management technology is highly recommended for the entities which are dealing in the information critical infrastructure. The users of the computers should adopt
security measures, including protection against viruses by adopting anti-virus strategies, use of firewalls, authentication and encryption technology.

7.2.5 Need to Empower Regulatory Machinery

It is suggested here that the regulatory machinery must be empowered to control global cyber terrorism. The law enforcement agencies must perform their tasks without any fear or pressure. All laws related to search, seizure and arrest of cybercriminals shall be liberalized and the investigating agencies need more teeth, in the form of training and powers.

7.2.6 Encourage use of Biometric Techniques and Cyber Forensics

Biometric techniques can be the best tool identifying the real perpetrator of cyber crime. Biometrics involves electronic analysis of attributes arising from a person’s physical characteristics that are unique to that person. For example, the codes derived from electronic analysis of fingerprints, footprints, retinal scans, body odor, etc. can provide important clues to identify the person accused of cyber crime, though it needs to be corroborated by other material evidence.

Cyber forensic will help investigating agency in identification, location, preservation and extraction of digital information from a computer system. It also helps the courts to decide the matters on the basis of cyber evidences. It consist computer forensics, cyber forensics and software forensics. All three are inter-dependent and inter-related to constitute a compact cyber crime detection mechanism. The use of computer forensics as a technique of analyzing the legal evidence would certainly facilitate cyber crime investigation and help in reaching the criminal and establishing his guilt on the basis of evidence procured and produced against him before the court.
7.2.7 Global Regulatory Mechanism

Last few decades change the nature and intensity of the crime. Terrorists have become more equipped with the latest technology and computer and internet gives them a divine space to continue terrorist activities. Law and criminal justice delivery system have not kept pace with the technological advancements made around the world. The conventional laws are proving useless in replying the cybersecurity issues. Therefore, it is the need of the hour and strongly suggested that there is a dire need for restructuring both, substantive and procedural law which can bring all the cyber terrorists and cyber criminals before the court of justice.

In the present scenario of the world a very few countries are sensitive regarding the issue of cyber terrorism. Internet has no boundaries, so cross-border crime cases are not replied at the best way. The laws and procedure are different in different countries and the treatment to cyber terrorism instances accordingly. Major issues relating to cyber terrorism may be eliminated only by adopting uniform cyber penal laws. Since crimes in the cyber world have wide ranging ramifications, so the penalties imposable on cyber terrorists should be stringent and even exemplary so that they may desist from indulging in cyberspace criminality.

The jurisdictional issue also be consider while address the menace of cyber terrorism. Cross border nature of cyber terrorism can be tackled by international cooperation. Therefore, in order to meet the jurisdictional challenges involved in cyber terrorism, it has been suggested in the Paris Convention in 2000, to establish an International Criminal Tribunal with global jurisdiction having power to investigate, try and punish cyber crime criminals.
7.2.8 Globalization of Cyber Laws

It has been observed in many instances that the cyber terrorists usually exploit the weaknesses of cyber laws. It is, therefore, the cyber criminal laws of various countries including cyber law should be universalized so as to extend adequate protection to citizens, institutions, organizations, government and nongovernment agencies and society as a whole against the menace of cyber terrorism.

7.2.9 Co-operation with INTERPOL and Emergency Response and Computer Security Team

International Police Organization known as ‘INTERPOL’ is working at global level to facilitate police co-operation from different countries and provide essential tools and services for effective detection and investigation of cross-country cyber crimes. Its efficiency is hampered due to the lack of desired co-operation from the affected countries. INTERPOL has a network linking of nearly 190 countries with the Interpol General Secretariat and it is actively engaged in crusade against cross-country cyber criminality. This network helps the countries in sharing information regarding the instances of cyber attacks on critical infrastructure through e-mail to the General Secretariat. Thus, it makes that information available to every country or those countries which are owners of such authorized information.

Many countries also have established their own Forum of Incident Response & Computer Security Teams (FIRCST) to tackle cyber crime within
their territorial boundaries. The praiseworthy success of US Forum is the good example to control over the cyber attacks within jurisdiction. So, in the Proceedings of the Asian Pacific Law Enforcement Conference against Transnational Organized Crime, Tokyo (Japan), 2001 has been suggested for the establishment of such a Forum at the international level.

7.2.10 Well Equipped Special Cyber Crime Investigation Cell

To pace with time and development in the technology, Cyber crime Investigation Cells were set up September, 1999 under the Central Bureau of Investigation (CBI). It started functioning from March 31, 2000. There are at present 6 cyber crime investigation cells, headed by Superintendent of Police, has the power to investigate the offences specified in Chapter XI of the Information Technology Act, 2000, functioning in India with headquarters at Delhi, Mumbai, Chennai, Bangalore, Hyderabad and Kolkata.

First Cyber Crime Police Station was set up by the State of Karnataka in 2001, which has jurisdiction all over the State. Afterward, Cyber Police Cells were also set up in the metropolitan cities, manned by qualified and trained police officials assisted by computer experts as and when required for the investigation of cyber crimes. But, there are States which does not yet have any special police cyber cells and the hi-tech crimes are being handled by the general police.

---

11 Nearly 25 countries have set up Forum of Incident Response & Computer Security Teams (FIRCST). So far India is concerned, Section 70B of the Information Technology (Amendment) Act, 2008 provides for the appointment of Indian Computer Emergency Response Team (CERT-IN) by the Central Government, which would serve as a national agency for incident response. Its main functions are collection, analysis and dissemination of information regarding cyber incidents, forecast and alert of cyber security, emergency measures and coordination of cyber incidents response activities etc.


13 “Bangalore to have country’s First Cyber Crime Police station”, Indian Express, August 31, 2001, p. 4; For details see www.indianexpress.com
Therefore, it is highly suggested that all States shall have to set up at least one, well equipped and armed with trained staff, a Special Cyber Crime Police Station. It expedites investigation and prosecution the hi-tech cyber crimes.

7.2.11 Complete the E-Judiciary Project within the Time Frame

In order to address the new age challenges, nations have to evolve right standards and practices in the emerging area of cyberspace crime adjudication. The e-Courts project was conceptualized on the basis of the “National Policy and Action Plan for Implementation of Information and Communication Technology (ICT) in the Indian Judiciary - 2005” has suggested three phased e-judiciary framework must be completed within the prescribed time limit. This policy ensures speedy disposal of cyber crime cases. The National e-Court Project started in July, 2007 for the creation of e-judiciary and e-governance grid covering India’s entire judicial system would certainly ensure transparency, speed and fairness in the adjudication of cyber crime cases.

The courts in India, have already adopted the system of video-conferencing for recording evidence of witnesses or under trial prisoners. There are many benefits of adopting the e-court system, e.g., dreaded criminals can be tried without risk, trial is expedited with use of this facility, multiple trials of an accused lodged in one jail is possible in different states (Telgi case can be the best example), evidence of witnesses unable to come to Court can be recorded, etc..

At the district level it is doing well but it is required expansion and accelerates at subordinate courts as well. It will helpful to enhance the productivity of the judiciary as well.
7.2.12 Extradition Treaty

Cyber terrorism is a borderless crime, to punish cyber terrorists, who are outside the jurisdiction of the affected country. As the Indian information technology law also consider extra-territorial jurisdiction of cyber law. So it is highly suggested for the effective implementation of law to have extradition treaties with the other countries. Extradition treaty will solve the problem and cyber terrorists and criminals can be brought to India and vice-versa for trial and prosecution in accordance with the established principles of international law.

7.2.13 Planting of Baits in Cyberspace for Worms and Viruses

According to one study the number of cyber crimes in India may touch 3,00,000 in 2015, almost double the level of last year, causing havoc in the financial space, security establishment and social fabric. This is an eye opener situation so the Government has to work on new strategies like planting of baits in cyberspace for worms and viruses. As in 2007, the Department of Information Technology (DIT) had signed Memorandum of Understanding (MoUs) with McAfee and Microsoft for tighten the cyber security. This technology will attract unusual internet traffic patterns. The unusual pattern will be analyzed so that timely warnings can be issued before any damage is done. Government has to work at more on such kind of technologies for the protection of critical information infrastructure. Like USA is working on digital ants in cyber space to control and predict cyber attacks.

7.2.14 Regulate the Social Networking Sites

Social networking sites like Facebook, Twitter, Xing, LinkedIn, etc. have made life easy and brought friends together but many a time it has found a best
way to spread rumors. In 2012 due to the rumors of attacks on North East residents in Bangalore created panic and as per the government reports about 9000 people boarded trains to Guwahati. The main motto of the cyber terrorists is to cause panic among the people so Government comes down on its feet and accept their demands.

7.2.15 National Informatics Centre - Needs to Reconstruct

In the age of internet India is not an exception, it is on way to computerization of all data. All the networks relating to the government are controlled and managed by the National Informatics Centre (NIC). The history of cyber attacks shows that the cyber terrorists always prefer to attack the primary source of network. So, it is high time to reconstruct National Informatics Centre for the better cyber security.

7.2.16 Spread Awareness about Cyber terrorism and Impart Training

It has been found that the countries faced cyber attacks are not aware or take cyber security lightly. It is suggested that the Government must ensure their people that information collecting activities are to support national security rather than to breach personal privacy. To refer the instance of Estonia, cyberterror attacks left handicapped the national critical infrastructures, including, governments, broadcasting, and banking. The Estonia instance indicates that it is need of the hour to have an efficient cyberterror prevention system for prompt response and repair systems. It is suggested that mass level awareness programme must be conducted, where the cyber experts provide the information and cybersecurity issues to all the entities, dealing in critical information infrastructure particularly. Indian Prime Minister Mr. Narender Modi also has shown his
concern in the about the digital war where the attackers remains unidentified, so the cyber awareness can be the best way to fight with the cyber menace.

One of the major reasons for swift escape of cyber criminals is that the crime investigating agencies, prosecution and Judicial officers are not well versed with information technology and laws governing IT. In most of the cases of cyber crimes affected people have no clue whether they have any remedies available against such acts. That is the reasons that most of such incidents go unreported. Thus, there is a need to bring awareness in this regard among the people. Then only such law can show its real force. But usually people are hesitant to report such offences. Even those who are aware of the criminalization of such acts are unwilling to file complaint because they do not believe that such crimes could be effectively redressed by the law enforcement agencies. True statistics related to the incidents of cyber crimes will only be known once the hesitation of the common people to report such crimes would be removed.

Delhi Police rightly realized the seriousness of the situation and have made the training in computer is compulsory for head constables and sub-inspectors. Two specialized training centres have been set up in Police Training College in Jharoda Kalan. Delhi Police has decided to give special training to a selected group of officers for the purpose to train them in computer and internet related crime.

7.2.17 Networking of Investigators

Every set of persons involved in investigating or combating cyber crimes, in various states of a countries or even in other countries across the world must worked in a networked environment if the nature of case demands. Technical experts from various countries can share their knowledge and help solving
complex cyber crimes. Investigation techniques in those countries that have been facing such cyber threats since long are naturally more developed. Thus India can afford to base their cyber laws and investigation techniques on laws and techniques adopted by the said countries. Also it would be much better if some sort of standard reporting format and investigation protocol is adopted in the countries frequently facing such cyber threats.

Police or other investigating agencies in various countries may collectively form a website wherein they may contact their counterparts in other countries which have faced success in similar situations in the process of handling cyber crimes. They may rightly suggest to each other, the do’s and don’ts while dealing with particular type of cyber crime. Also there is possible situation when effect of cyber crimes would be in multiple countries at the same time and in such investigators would need to collect evidence available in various jurisdictions.

**7.2.18 Need for Modernization of Existing Laws and Enactment of New Laws**

There is a need for modernizing the penal laws of countries which predate the advent of computers. On the one hand, the existing laws have to be changed to cope up with computer-related frauds such as hacking, data theft, software theft, etc. and on the other hand, new legislation is also necessary to ensure data protection and privacy\(^\text{14}\).

7.2.19 Cooperation with the Hi-Tech industry

Involvement of high-tech industry is essential for successfully controlling the cyber crimes. Experts from IT Industries can provide valuable support to Police and other investigation agencies in this regard. IT Companies can assist and contribute towards combating cyber crimes in various ways. It would be great help if they start reporting the cyber attacks or attempts to commit cyber crimes against them. Private IT Industry may also sponsor training of police in hi-tech crimes or hold training workshops for sharing the knowledge of experts they have. They may also share their equipment and develop software for detection of such crimes or collection of intangible evidence. Students from renowned IT colleges must be inspired to join cyber crime investigation task forces.

There are many companies which have their own dedicated ‘information security units’ to protect their data and detect intrusions etc.. Presumably, they have set-up such units only because they faced a large number of attacks. Still, hardly any of such companies report such attacks. They probably think is wiser not to report as that may affect their public image and stock values etc.. Due to non-documentation of such incidents modus operandi of such criminals remains hidden. Government may itself frame some sort of rules and regulation which in turn may make it mandatory for the private industries to exchange the technical information. Thus, clearly there is a need of regular co-operation between government investigators and private industries. It will in turn help to document the valuable statistics about the cyber-attacks and also in protecting critical infrastructures of the country.
7.2.20 Special Courts, Judges and Prosecutors etc.

Special courts should be set up for the trial of cyber crimes and its presiding judges should be properly and technically trained to evaluate evidence technologically.

With the advent of technology in everyone field lawyers and judges are also resorting to laptops and Compact Disks instead of heavy books. But still they may not be well versed with the basics of computer forensics as traditional curriculum of law does not include such technical education. Thus present times demand a change in legal education in this regard. Technical training in computers,

i. internet and basics of computer forensics must be taught to law students to have a hold over the subject of cyber crimes.

ii. At present number of specialized courses in cyber laws available in various institutions.

iii. Specialized lawyers and judges trained via such courses could only handle such crimes effectively.

Beside judges and lawyers there is also need of special training for probation or parole officers in cyber crimes. If they are not aware of such technicalities they would never come to know that whether the person released is attempting those crimes again or not.

Finally, it may be concluded that in the present computer age of 21st century, internet has influenced every facet of human life and no one can even think of life without the use of computers. Therefore, in the present scenario, it is highly desirable that the computer technology should be preserved for the
progress and prosperity of the society rather than being allowed to be misused by the terrorists and criminal conduits for perpetration of terrorist’s activities or crimes. At present, there are number of websites in the cyberspace that provide powerful tools for communicating, storing and processing information. The web service providers should therefore, exercise due diligence and caution while pasting information in their web page. The ease with which the data and information flows through the internet across the world may sometime be exploited by the criminals for the commission of crimes, which may be a serious cause of concern for the law enforcement agencies at the national as well as the international level.

7.3 Conclusion of Hypothesis

In the light of analysis done the three hypotheses find a strong support i.e., the law and policy on cyber terrorism has not been robust enough to:

a) Protect the critical infrastructure of the country.

b) Respond effectively to the menace of cyber terrorism.

c) Build confidence in cyberspace.