A. GENERAL

Commenting on the Information Technology revolution which has transformed the world into a global community, Waler B Wriston observed, “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 advancement of technology has brought about radical changes in the modern society. But human experience has shown that every technological change brings with it some unforeseen problems, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities. In fact, technology-generated crimes not only affect individuals or a nation, but have a widespread ramification throughout the world. Internet is one such gray area, which has given rise to the menace of cybercrimes. The computer based global communication system has crossed the territorial borders, thus creating a distinct field for online criminal activity warranting global attention.

Cybercrimes have emanated from development of computer network. Internet in the present millennium has become all pervasive and omnipresent. It has also brought with it new problems hitherto unknown to humanity. Internet in a sense is analogous to the ‘high seas’ which no one owns yet people of all the nationalities use it. The term ‘cybercrime’ encompasses within it a variety of criminal activities taking place in the cyberspace through the media of global communication and information via internet. It is an inevitable evil having its origin in the growing dependence of mankind on computers in modern life, the reason being that the computers despite being high technology devices are extremely vulnerable. Thus, whenever any crime or criminal activity takes place with the use of computer, it constitutes a cybercrime. It is for this reason that ‘cybercrime’ has been defined as ‘an unlawful act wherein the computer is either a tool or a target or both’.\(^2\)

Thus, cybercrimes are such harmful activities in the cyberspace which may cause damage to a person, property or even the state or society as a whole. Being radically different from the conventional crimes, the law enforcement agencies find it difficult to tackle

\(^1\) Walter B. Wriston, The Twilight of Sovereignty – How the Information Technology Revolution is Transforming Our World, (2003), p. 31

\(^2\) Ibid.
cybercrimes with the existing infrastructural mechanism because of lack of adequate knowledge about the computer operating systems. This is the main reason why this relatively new variety of crime is posing a challenge to the legal regime.

The menace of cyber criminality is not confined to one or two countries but the whole world is facing this gigantic problem as a ‘technological scorn’. India is no exception to this computer generated menace. However, as a measure to prevent and control internet crimes, the Parliament enacted the Information Technology Act, 2000 which came into force on October 17, 2000. The Act categorically defines offences relating to cyberspace such as tempering with computer source document, hacking with computer system, breach of confidentiality and privacy etc. It is not that prior to this legislation there was no law to deal with these offences. The Indian Penal Code, 1860 already contained provisions to prevent and control cybercrimes but they were not found to be sufficient enough to tackle all varieties of cyberspace crimes. The obvious reason being that no one knew about computer or internet\(^3\) at the time when the Indian Penal Code was enacted.

It hardly needs to be stated that Science and Technology has extended its tentacles cutting across the national frontiers whereas the law is still struggling to define and redefine the boundaries for the control of cybercrimes. Following a similar course, the cyber law particularly, the Information Technology Act, is engaged in prevention and control of cybercrimes within the country’s territorial jurisdiction overlooking the fact that cyber criminality is a global phenomenon which has no territorial limits.

B. **CONCLUSION**

Cybercrime being global in character, generally affects the person far away from the place of offence, may it be in the same country or some other country. It, therefore, requires policing at international level as also the active cooperation of the international community. The European Convention on Cybercrime\(^4\) was indeed a praiseworthy attempt as it laid down guidelines to be followed by the member states in combating cybercrime. The Convention suggested measures to be initiated by the states for restructuring their cyber laws to meet the new challenges. The Convention not only dealt with the changes and improvements in the substantive part of the criminal law but also referred to the procedural aspect which must be

---

3 The Computer Technology has mainly developed and expanded throughout the world only during the last quarter of 20\(^{th}\) Century.

4 Effective from June, 2001
taken into consideration while restructuring the existing law to meet the current needs of the developing technology. It has been generally accepted that procedural aspect of the criminal law is the main hurdle in tackling the problem of cybercrime effectively but at the same time, substantive part of the cybercrime also needs to be redefined to fight against ongoing cyber criminality. Out of a variety of cybercrimes, the European Convention has chosen ten specific cybercrimes and urged the member states to include them in their information technology laws and provide a concrete mechanism to fight against them. But it is rather unfortunate that many cybercrimes of a particular country are not treated as crime under the criminal law of other countries, which really pose a problem when cross-country cybercrimes are involved. The solution to this problem lies in enacting a global cyber law uniformly applicable to all the countries of the world. The crux of the matter is that universally accepted standard cybercrime preventive laws should not vary from place to place.

A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to frame laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law poses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detection and punishment. All the nations should therefore, realize the need and urgency for generating awareness about the dangerous nature of cyber crimes which are perpetuating illegal online activities in cyber space. Cyber criminality is perhaps the deadliest epidemic spread over the world in the new millennium which has to be curbed by adopting a global preventive strategy.

An overall global view of the cyber law indicates that many countries do have their national legislation for combating cyber criminality, but they radically differ from each other as a result of which, a particular cyberspace activity which is considered as a criminal offence in one country may not be necessarily so in another country. This variation in law provides loopholes for the cyber offenders to escape punishment. Therefore, there is dire need for international cybercrime legislation which could be uniformly acceptable by all the countries to tackle the problem of cybercrime. Not only that, there should also be an international policing agency for countering cyber offences. The solution to the problem therefore, lies in

---

5 The European Convention on Cyber Crimes; Section 1, Chapter II contains Articles 2 to 13 defining ten cyber crimes under five separate titles.
the concerted and united efforts of nations around the world and their mutual cooperation in fighting against cyber criminality.\(^6\)

Broadly speaking, the law enforcement agencies all over the world are confronted with four major problems while dealing with cybercrimes in a network environment. The detection and prosecution of cyber criminals online is hindered by the challenges, which may be technical, legal, operational and jurisdictional.

As regards technical challenges, cybercrimes such as hacking of a website, stealing data stored in computers, espionage, exchange of pornographic material, blackmailing etc. involve detection of source of communication which is a complicated task. Therefore, the cyber criminals find it easy to impersonate on the internet and hide their identity.

The legal challenge emerges from the fact that cyber criminality is no longer confined to the developed countries alone but it has assumed global dimensions in recent decades. The conventional legal techniques of investigation of cybercrimes are inadequate particularly, in case of cross-country crimes. The problem becomes more complex because of lack of any universally accepted definition of cybercrime. Therefore, a cybercrime in a country may not necessarily be a crime in another country. There are hardly 20 countries in the world which have enacted comprehensive cyber laws. In the absence of an adequate cybercrime laws, the cyber criminals carry on their illegal activities undeterred. Therefore, effective handling of cybercrimes 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 cybercrime, thereby resulting in his acquittal by the court. The traditional modes of procuring evidence are unsuited in case of cybercrime 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.\(^7\)

In the context of electronic evidence, it is significant to note that despite the fact that digital signatures have facilitated e-commerce by reducing paper-work and ensuring quick transactions, it has not been widely accepted in India because of the technicalities involved in

---


\(^7\) Id. at p. 11.
it and therefore, people in general still believe that paper-based documents are more dependable and trustworthy than the paperless electronic records. The reason being that former are tangible and serve as best piece of evidence before a law court. However, 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.

The jurisdictional challenge impeding the efficient handling of cybercrime investigation result out of widespread inter-connectivity of the computer networks and the supporting infrastructure such as telecommunication information dissemination on the website etc. In fact, jurisdiction is a broad concept which refers to whether a court has power to adjudicate, i.e., whether it has personal jurisdiction to try the case and territorial jurisdiction over the location or place where the crime is committed or the parties concerned reside. 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.

C. SUGGESTIONS

In view of the expanding dimensions of computer-related crimes, there is need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. Even a short delay in investigation may allow cyber criminals enough time to delete or erase the important data to evade detection, which may cause huge loss to the internet user or the victim. That apart, the peculiar nature of cybercrimes is such that the offender and the victims do not come face to face, which facilitates the criminals to carry on their criminal activities with sufficient sophistication without the fear of being apprehended or prosecuted. It is for this reason that a multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of cybercrime cases. A common cybercrime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality.

The process of crime prevention essentially requires cooperation and active support of citizens, institutions, industries and the government alike. Therefore, a sound strategy for prevention of cybercrimes necessitates mobilization of community participation in combating this menace. This calls for participative role of all those who perceive that the growing incidence of cybercrime is a potential danger to the society as a whole. It also calls for self
protection initiatives by the people who are vulnerable to cybercrimes. They must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers incurred by them. Obviously, media has an important role to play in warning people against the possible dangers and evil effects of cybercrimes on victims and also the nation and the safety measures which are necessary to combat this high-tech criminality.\(^8\)

Regulatory control through effective laws is yet another measure of cybercrime prevention. It is possible to exercise control over these crimes by effective implementation of laws by enforcement agencies. The legal preventive measures may help in reducing the incidence of cybercrimes provided they get community’s active support in exposing the criminals.

Some other suggestions to prevent and reduce the incidence of cybercrimes at the domestic level are as follows:

---

1. **Net Security be Tightened Up**

Computer technology has proved to be a boom to the commercial world. Perhaps, it is the area which has been most benefitted by the advent of computers. Most of the commercial, industrial and business transactions are carried on through internet services at the national as well as the international level. The increasing use of computers in the field of trade and commerce has at the same time opened new vistas for the perpetration of cybercrimes by the offenders for their personal monetary gain. With the liberalization and globalization of economy, the business houses now believe that there is a huge and profitable market for commercially exploiting the networks. With the increased dependence on computer in commercial field, most of the money transactions are being carried out with the help of computer network making it possible for the cyber criminals to illegally intercept and commit financial frauds. It is, therefore, necessary that an adequate security mechanism be developed for safeguarding e-commerce and e-banking against possible online frauds, forgeries, or misappropriation of money etc.  

First of its kind, recently the US along with the cooperation of other nations has drafted the International Cyber Security Scheme. According to this 30-page scheme if a nation’s security is threatened by cyber attacks then it is lawful for that nation to use its defence forces against the aggressor. It is alleged that in response to America’s declaration that any cyber attack on US will be treated as a war against US, China had hacked e-mail accounts of Senior Government Officials and Army Commanders of US. Internet search engine Google has accepted that such hacking was done from Zizan City of China by using techniques of phishing and virus attacks. Though China had denied such allegations and has said that it is strictly against cyber crimes and is ready to help the world community in investigating cyber crimes.  

As regards the legality of financial transactions on the internet, the Securities Exchange Board of India (SEBI) vide its notification dated January 25, 2000, has provided that trading of securities on internet will be valid in India but there is no provision to this effect in the Information Technology Act, 2000 which provides legal validity and prevent security frauds and stock manipulations over the internet. A specific provision for protection

---

11 “China Ka America Par Cyber Hamla”, *Dainik Bhaskar*, June 3, 2011, p. 16
of confidentiality in the net-trading, therefore, needs to be incorporated in the Information Technology Act, 2000.

2. **Use of Encryption Technology**

   It should be mandatory for all government, semi-government and non-government commercial organizations which have resorted to massive computerization for the transmission of information and commercial transactions, to appoint well trained Information Security Officers who should be responsible for overall protection of computer resources and they should also be made accountable for any lapse in computer security.

   The use of encryption technology may also help to protect data and communications from unlawful and unauthorized access, disclosure or alteration. It also helps to prevent crime by protecting valuable secret information over inter-connected computer and networks. The law enforcement agencies should therefore, develop and support the use of strong and recoverable encryption services for protecting personal and business data from being misused or stolen by miscreants.

   Similar to encryption, there is one more technique known as ‘steganography’, which 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.12

   Firewall device is yet another tool which may be extensively used to provide an alert against attempted intrusions in database. It is a software program which monitors data flowing between one computer to another on the network. Firewall device can be used to control the amount of data flowing over one’s computer network.

3. **Intrusion Management**

   A new preventive strategy called as the ‘intrusion management’ may be used for testing, detection and investigation of cybercrime. It is a process which primarily aims at preventing intrusions in the computer system thus providing effective e-security control mechanism. The computer users and e-commerce organizations should ensure that functional areas of vulnerability of the computer system are kept properly controlled so that, as for as data is concerned, following is absolutely safeguarded-

   (i). Identification and authenticity,

(ii). Access,  
(iii). Accountability,  
(iv). Accuracy, and  
(v). Reliability  

It has been observed that most cybercrime investigations end up with the conclusion that victim’s computer system has been damaged due to cybercrime attack but the source of attack could not be traced or located. Therefore, one of the most important aspects of intrusion management is to plug the security loopholes so as to render the computer system absolutely safe and secured.

The protective measures contemplated under the intrusion management system include protection against viruses by adopting anti-virus strategies, use of firewalls, authentication and encryption technology.

4. **False E-mail Identity Registration be Treated as an Offence**

Cyber criminals often furnish fictitious information while registering themselves for an e-mail address with a website because the e-mail service providers refuse to provide two ID’s to the same person. This false and misleading information on the internet helps the criminal to suppress his real identity and mislead the investigating authorities in reaching the real culprit.\(^{13}\) There being no provision in the Information Technology Act, 2000 to prevent registration of a person for an e-mail address with a website by providing false information, a person can establish false e-mail identity with a fictitious IP address and misuse the same for the perpetration of a cybercrime. This lacuna in the Act has been taken care of by inserting a new Section 66A in the principal Act by the I.T. (Amendment) Act, 2008 which provides that any false e-mail identity registration with a website will be an offence punishable up to 2 years of imprisonment. It is certainly a step forward towards the prevention and control of cybercrimes.

\(^{13}\) Suresh T. Vishwanathan, “The Criminal Aspect in Cyber Law”, *The Indian Cyber Laws*, 2001, p. 81
5. **Self-regulation by Computer and Net Users**

Self-regulation may be suggested as one of the practicable solution to reduce the incidence of cybercrime. 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.

6. **Liberalization of Law Relating to Search and Seizure**

Government’s regulatory mechanism to control widespread cyber criminality needs to be further intensified. Most importantly, the existing legal regimes should enable the law enforcement agencies to accomplish their tasks fearlessly without any external pressure. The law enforcement agencies should be empowered to seek such details from the Service Providers as may be necessary for the investigation of internet crime without, however, violating any of the fundamental or privacy rights of the parties. The law relating to search, seizure and arrest as applicable to cyber-offences needs to be liberalized so as to enable the police or the investigating agencies to apprehend the cyber offenders and initiate criminal proceedings against them.\(^\text{14}\)

The telecommunication department should also review its policy towards ISPs and impose selective restrictions on them while extending internet services by classifying them on the basis of age, profession or standing as Internet Service Providers.

7. **Use of Voice-recognizer, Filter Software and Caller-ID for Protection against Unauthorized Access**

Technology indeed is itself a powerful tool which has generated cybercrime. Therefore, as a first step to prevent its misuse, the places where computer is popularly used as a means for carrying out routine life activities, should be equipped with some safety and security devices to protect against unauthorized usage of computer systems. For example, the modern voice recognition system which relies on voice pattern for activation may effectively

be used. So also, anomaly detection software, which identifies unusual pattern of computer use, helps the users or organizations to respond and frustrate the attacker. Similarly, filter software have afforded protection against known threats. The use of Caller-ID technology in the telecommunication as a protective measure may also help in eliminating e-mail crimes.

8. Development of Cyber Forensics and Biometric Techniques

In order to provide substantial technical assistance to the investigating agency in identification, location, preservation and extraction of digital information from a computer system so as to produce it in the form of evidence of cybercrime before the court of law, the cyber forensic techniques need to be developed. The cyber forensic techniques consist of three components, namely, computer forensics, cyber forensics and software forensics. Obviously, the three are inter-related to constitute a compact cybercrime detection mechanism.

i. **Computer forensics** deal with collection of evidence from computer media seized at the scene of crime by extracting hidden or deleted information from the computer disk.

ii. **Cyber forensics**, also called as ‘network forensics’, relate to digital evidence that is distributed across the large computer network. The main object of the cyber forensics is to discover the evidence and access the intent and identity of the cyber criminal as also to determine the impact of crime on the victims.

iii. **Software forensics** mainly deals with author of the malicious code and provides substantial clues to identify the perpetrator of cybercrime.

The use of computer forensics as a technique of analyzing the legal evidence would certainly facilitate cybercrime investigation and help in reaching the criminal and establishing his guilt on the basis of evidence procured and produced against him before the court.15

The use of biometric techniques can also be of great help in identifying the real perpetrator of cybercrime. 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 cybercrime, though it needs to be corroborated by other material evidence.

---

9. **Need to Establish a Computer Crime Research & Development Centre**

Perhaps the most effective method of preventing cybercrime is to create awareness among the computer users about the possible dangers emanating from misuse of information technology for criminal activities. It is all the more necessary because every user of network is a potential victim and his ignorance about the information security and safeguards, multiplies the chances of his vulnerability to cybercrime. Therefore, generating awareness among the owners and users of computers through proper education may substantially help in reducing the threats as well as the damages caused by these crimes. Generally, the internet users remain unaware of the fact that while they are online, they may fall a victim to cybercrime or may themselves unknowingly involve in an activity which constitutes an offence though they did not intend to commit it. This is truer particularly, in case of adolescents who, for the sake of entertainment or fun, switch over to pornographic websites and sometimes themselves become a victim of such crime. This possibility can be eliminated by apprising the internet users about the dangers and consequences of the unlawful acts which they may inadvertently or ignorantly commit on the net.  

There is dire need to set up a National Computer Crime Resource Centre with members from different segments of society such as law enforcement personnel, forensic and legal experts, computer experts, members from Central Bureau of Investigation (CBI) and the Reserve Bank of India (RBI), which should collect, collate and disseminate all data relating to computer crimes among the users. The Centre should also lay down a model standard procedure to ensure safe computing.

10. **Need for a Universal Legal Regulatory Mechanism**

Law and criminal justice delivery system have not kept pace with the technological advancements made around the world during the preceding years, which has provided ample scope for the abuse of internet. The conventional old laws pertaining to protection of property are no longer valid for protecting the unauthorized manipulation of information through computer networks. Therefore, there is need for restructuring of the substantive as well as the procedural law relating to computer generated crimes so that offenders may be brought to justice. At present, the definition of cybercrime varies from country to country depending on the incidence of such crimes and the State’s sensitivity to them. In the absence of any

---

universally accepted definition of cybercrime, investigation of cross-border crime cases is carried on according to the procedural law of the place where the cybercrime is committed.

The problem arising due to divergence of laws and procedure of different nations may be eliminated to a considerable extent if at least major cybercrimes are uniformly recognized and incorporated by all the countries in their penal laws. This would ensure uniformity as regards identification of various actions as cybercrime. Since these crimes have wide ranging ramifications, the penalties imposable on cyber offenders should be stringent and even exemplary so that they may desist from indulging in cyberspace criminality.

The question of a nation’s jurisdiction in case of a cybercrime committed outside the country but having disastrous effect on that country itself, still remains unresolved as there is no general consciousness of different nations on this vital issue. The jurisdictional uncertainty regarding crimes committed in cyberspace has made committing of such crime easier but punishing the perpetrator thereof more difficult. Therefore, the need of the hour is drafting of a uniform global cyber law with the cooperation of all the countries of the world.17

Jurisdictional uncertainty as regards the investigation and trial of cybercrime is perhaps the most ticklish problem which the law enforcement agencies all over the world are facing. Cyber criminals may cause irreparable damage to victims from a distant place without the risk of being spotted out or identified. This enables them to commit crimes beyond national borders without being physically present at the scene of crime. The cross-country jurisdictional nature of internet and lack of adequate international cooperation to address the problem of cross-border cyber criminality enables criminals to escape arrest and prosecution. Therefore, in order to meet the jurisdictional challenges involved in cybercrimes, it has been suggested that an International Criminal Tribunal18 with global jurisdiction be set up with power to investigate, try and punish cybercrime criminals.

11. **Global Code of Digital Law for Resolving IPR Related Disputes**

It has been generally accepted that intellectual property is going to be the real estate of the Third Millennium.19 The information technology revolution during the closing years of 20th century has opened scope for new variety of disputes in IPR regime, both at national and international level. The resolution of these disputes needs a Global Code of Digital Law to be developed which should have universal acceptance all over the world. This is all the more

---

17 “Net Police and Cyber Lawyer will Soon be Here”, *The Tribune*, December 11, 2008, p. 2
18 As suggested by G-8 countries in the Paris Convention on Cyber Crimes held in France in May, 2000
necessary in view of the expanding dimensions of IPR transactions having multi-national ramifications.

12. **Need for Universalization of Cyber Law**

   It has been generally observed that the perpetrators of cybercrime usually exploit the weaknesses inherent in the computer which is being used or attacked. Therefore, some special security measures may be adopted to prevent unauthorized use of the computer systems. It is often alleged that the domestic laws controlling computer security are mostly directed to safeguard national safety, security and integrity rather than providing adequate protection to computer users, whether they are individuals or corporate entities. Therefore, the criminal laws of various countries including cyber law should be universalized so as to extend adequate protection to citizens, institutions, organizations, government and non-government agencies and society as a whole against the menace of cybercrime.²⁰

13. **Interpol and Emergency Response Computer Security Team**

   At present, the International Police Organization called ‘INTERPOL’ is functioning at the global level to facilitate police co-operation from different countries and provide essential tools and services for effective detection and investigation of cross-country cybercrimes, but its efficiency is hampered due to the lack of desired co-operation from the affected countries. INTERPOL has a network linking of nearly 200 countries with the Interpol General Secretariat and it is actively engaged in crusade against cross-country cyber criminality. Through this network, the countries use e-mails to send information about cybercrime and criminals to the General Secretariat which incorporates it in the international database and then makes that data available to every country or those countries which are owners of such authorized information.

   Besides being a member of INTERPOL, many countries have established their own Forum of Incident Response & Computer Security Teams (FIRCST) to tackle cybercrime within their territorial boundaries. ²¹ The US Forum has achieved commendable success in exercising effective control over cybercrimes within its territorial limits. However, there is

---
²¹ 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.
need for establishment of such a forum at the international level\textsuperscript{22} to share the exchange of information relating to cybercrimes and criminals and initiate preventive strategies to combat this menace.

14. \textbf{Combating the Menace of Cyber Terrorism}

Perhaps, the greatest threat posed by computer system and internet is that of cyber terrorism. It has changed the traditional concept of terrorism as the development of information technology has enabled terrorists to acquire more sophisticated and destructive technology and weapons to attack their targets.\textsuperscript{23} The damage caused by the cyber terrorists is so catastrophic and irreparable that it completely shatters the national security and adversely affects the nation’s economy. Presently, cyber terrorism has assumed international dimensions therefore, there is need to tackle this problem by developing e-security technology and adopting stringent penal policy both at the national as well as international level. It may be suggested that India should make use of SAARC forum to evolve consensus among the member countries about the need for concerted efforts to curb cyber criminality particularly cyber terrorism through regional co-operation. Efforts should also be made to acquire advance cyber technology from the developed countries adopting a mutual Code of Cyber Legislation.

15. \textbf{Special Cyber Crime Investigation Cell for Hi-tech Crimes}

In keeping with the demand of time, the setting up of a Cybercrime Investigation Cell under the Central Bureau of Investigation (CBI) was notified in September, 1999 which actually started functioning with effect from March 31, 2000. The Cell is headed by a Superintendent of Police and has jurisdiction all over India. It has the power to investigate the offences specified in Chapter XI of the Information Technology Act, 2000 and is also empowered to probe into other hi-tech crimes. There are presently 6 cybercrime investigation cells functioning in India with headquarters at Delhi, Mumbai, Chennai, Bangalore, Hyderabad and Kolkata.

Similar to the establishment of Special Cyber Crime Investigation Cell of CBI, there has been a growing demand for setting up Cyber Crime Police Stations by the State Governments. Taking initiative in this direction, the State of Karnataka was the first to set up

\begin{itemize}
  \item Proceedings of the Asian Pacific Law Enforcement Conference against Transnational Organized Crime, Tokyo (Japan), 2001
  \item Terrorist attack on U.S. World Trade Center (WTC) on September 11, 2001; Indian Parliament on December 13, 2001; Taj and Oberoi Hotel, Mumbai on November 26, 2008 etc. are the glaring examples of blatant misuse of computer technology for heinous cyber crimes.
\end{itemize}
the country’s first Cyber Crime Police Station on August 30, 2001, which has jurisdiction all over the State. Subsequently, Cyber Police Cells were also set up in the metropolitan cities for handling cybercrimes. These cells are manned by specially qualified and trained police officials assisted by computer experts as and when required for the investigation of cybercrimes. But most States have no special police cyber cells and the cybercrimes are being handled by the general police. It is therefore, suggested that it should be mandatory for each State to set up at least one Special Cyber Crime Police Station well equipped with electronic technology and computer trained staff where complaints relating to cybercrime could be lodged online so that hi-tech cybercrimes could be investigated efficiently and expeditiously. The police official working in these special cells should be empowered to conduct search of publicly accessible data or data in private systems, computer equipments, disk etc. with the prior permission by the concerned magistrate.

16. E-Judiciary and Video-conferencing for Speedy Justice

In order to evolve right standards and practices in the emerging area of cyberspace crime adjudication, the three phased e-judiciary framework as proposed under the National Policy on Information and Communication Technology (NICT) must be completed within the prescribed time limit so as to ensure speedy disposal of cybercrime 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 cybercrime cases. It would reduce workload of the courts and ensure speedy disposal of cases as also eliminate problems associated with paper-based records such as their collection, maintenance, retention etc. it is much easier to retain and retrieve electronic record.

The courts in India, have already adopted the system of video-conferencing for recording evidence of witnesses or under trial prisoners etc. at the district level, which has reduced the security risk of the prisoners escaping during transportation and has helped in saving the valuable time of the courts. Further expansion of the video-conferencing in subordinate courts needs to be accelerated.

24 Bangalore to have country’s first Cyber Crime Police station, Indian Express, August 31, 2001, p. 4; For details see www.indianexpress.com
It hardly needs to be stressed that computerization can help in enhancing the productivity of the judicial work. It can create accessible database to help judges, lawyers and litigants etc. as also facilitate case-management by the courts.

17. **Need for Cyber Crime Reporter or Cyber Law Journal**

So far computer crime statistics are concerned; they do not reflect the true picture of incidence of cybercrimes. The reason being that the operational speed and capacity of computer software makes it very difficult to detect cybercrime. That apart, many victims of computer crime desist from reporting the crime because they apprehend unnecessary harassment and waste of time, energy and money in litigation which may drag on for years. The trading community and businessmen are particularly reluctant to report having fallen a victim to cybercrime due to the fear of adverse publicity, like loss of goodwill, embarrassment or harmful repercussions.

The lack of necessary technological expertise to deal with cybercrime on the part of law enforcement agencies is also a contributing factor for non-reporting of cybercrime cases by the victims. The intangible nature of cybercrime and anonymity of the perpetrator of the crime further complicates the issue of cybercrime reporting. It may be concluded that reporting of cybercrime cases is, by and large, scanty and whatever cases are reported, they are mostly either dropped for want of sufficient evidence or withdrawn or compromised by the parties before they are finally disposed of by the court. However, in view of the consistently rising graph of the incidence of cybercrimes and more and more cases coming before the courts for adjudication, it would be worthwhile to start publication of a ‘Cyber Crime Reporter’ or ‘Cyber Law Journal’ for the benefit of the members of the Bar, Bench, Police and enforcement agencies and all others who are concerned with the detection, investigation and prosecution of cybercrime and criminals.

18. **Information Technology (Amendment) Act, 2008 – A Step in the Right Direction**

With the march of time and advance of technology, the problem of cybercrime is touching alarming dimensions and therefore, calls for concerted action to evolve a universal regulatory mechanism for the prevention and control of these crimes. In the Indian setting, there is need to inculcate information consciousness among the Indian citizens. Though the Information Technology Act, 2000 as amended in 2008, has reasonably succeeded in

---

providing relief to computer owners/users by extending the reach of law to almost all the online criminal activities and increasing awareness among the people, but it is not a foolproof law as yet since it was primarily enacted for the promotion of e-commerce to meet the needs of globalization and liberalization of economy. The Act still suffers from certain lacunae as it does not provide adequate security against web-transactions nor does it contain adequate provisions to prevent securities fraud, stock confidentiality in the internet trading although the Securities Exchange Board of India (SEBI) has notified that trading of securities on internet is legally recognized and valid.27

19. **Digital Time Stamping System (DTS)**

The Information Technology Act, 2000 allows transactions signed electronically to be recognized and made enforceable by law but there is no mechanism or device to know as to when and exactly at what time the particular electronic document was prepared and signed electronically. The non-availability of any reliable evidence to establish the exact date and time when the disputed electronic document was made and signed leaves enough margin for uncertainty resulting in weakening of the prosecution case in such cybercrimes. This problem can be overcome by introducing an electronic device called as ‘Digital Time Stamping System’ (DTS) in electronic transactions. It consists of an apparatus called as ‘Tamperproof Box’ in which a highly secured time-stamping server is used to create Digital Time Stamps (DTS). The system has been successfully working in the United States for the last so many years.28

20. **Extradition Treaty: Need of the Hour**

The Indian information technology law recognizes the extra-territorial jurisdiction of cyber law but it cannot be effectively implemented in cases where the culprit happens to be in a country with which India has no extradition treaty. This problem may be resolved by making a suitable amendment in the law that cyber criminals from non-extradition countries can be brought to India for trial and prosecution in accordance with the established principles of international law.

21. **Establishment of Special Cyber Courts to try Cyber Crimes**

---


28 Bhadra Singh and Sumit Mishra Pandey, “Despite IT Act, Cyber Criminals have the Net in their Web”, *The Times of India*, January 30, 2001, p. 8
In the backdrop of increasing number of cyber crimes and lack of expertise to deal with them, it is suggested that special cyber courts with efficiently trained Judicial Officers, prosecution and police personnel should be set up to settle cases of cyber crimes expeditiously. The regular courts feel handicapped to decide cyber crimes because of lack of IT expertise.29

22. **Diffusion of Internet Technology in India**

Today, almost all types of works, more or less, depends upon the computer but the population at large particularly in rural areas do not understand even the basics of computer, what to talk about cyber crimes. Therefore, in order to bridge India’s widening digital divide, the Government should focus on increasing physical access to computers connected to the internet. In a recent policy initiative, the Government has promised to put in place in rural India a hundred thousand Common Service Centres (CSCs) – broadband enabled computer kiosks that will offer a range of Government-to-citizen and business-to-customer services, besides providing sheer access to the internet.30

23. **Technical Means for Blocking of Errant Websites**

The Centre should put in place an advance screening system at bandwidth landing stations to block websites and blogs that are perceived as threats to national security. The technology should be capable of blocking websites at a sub domain level, thus saving ISPs from a sweeping shutdown. The Government should realize that the most effective way to keep out such sites is through URL-based blocking solutions installed at international gateways. After the system is in place, the Department of Telecom (DoT) can direct ILD players who own the landing stations to block a particular URL at the sub domain level.

This will come as a major relief for ISPs in the country, who were responsible for blocking specific web pages till now. The issue of blocking individual websites had come into prominence following the Mumbai blasts in July 2006, when DoT had directed ISPs to ban 18 blogs and websites. However, an ISP did not possess the technologies needed to execute the directive, the service providers implemented the ban at the domain level. This

---

29 “Call for Special Courts to Try Cyber Crimes”, *The Hindu*, August 30, 2006, p. 5
30 “India is Online But Most Indians are Not”, *The Hindu*, September 25, 2006, p. 4
resulted in public outcry and international criticism as users were unable to access hundreds of thousands of websites and blogs.  

24. **Planting of Baits in Cyberspace for Worms and Viruses**

With the cyber crime on rise the Government should work on new strategies like planting of baits in cyberspace for worms and viruses. Aimed at tightening cyber security, a proposal to this effect is being considered by the Department of IT (DIT) which has signed MoUs with McAfee and Microsoft. The technology to develop such baits will attract unusual internet traffic patterns. The trapped pattern will then be analysed so that warnings can be issued before any damage is done.

The scientists of Wake Forest University of North Carolina, USA in collaboration with the Pacific North West National Laboratory (PNNL) are conducting an experiment to prepare an army of digital ants which can detect and attack internet viruses. Such a technique will strengthen the cyber security as it can predict the virus attacks in advance.

25. **Regulation of Social Networking Sites**

Though social networking sites like Orkut, Facebook, Twitter etc. has benefited the masses and brought friends together but they have also destroyed the life of so many users who were trapped by the wrong people with fake identities. From creating fake profiles of girls to getting involved in murders, the misuse of social networking sites has been on the rise in recent years. The murder of Adnan Patrawala, the 16 year old son of a Mumbai based businessman, by friends he had made on the orkut website has once again raised questions about the safety of users of such websites which have been in news for all the wrong reasons in the past also. It is the need of hour that some regulations are made to keep a check on such sites.

26. **Decentralization of the National Informatics Centre**

India is on fast track to computerization. The Government networks are managed by the National Informatics Centre (NIC) and are often hosted on its servers, which makes this

---

32.“Government to lay traps for Cyber Worms and Viruses”, *The Economic Times*, March 12, 2007, p. 5
premier agency a prime target. Decentralizing such system is just one of the many steps that need to be taken to ensure better cyber security for Government networks.  

27. **Appointments under the IT Act, 2000: Fair, Transparent and Speedy**

Justice Rajesh Tandon, head of the Cyber Regulations Appellate Tribunal (CRAT) is dissatisfied with the ‘unreasonable’ provision relating to the retiring age of the Tribunal’s Presiding Officer and the procedural delay in appointments. Under the IT Act, the presiding officer of a tribunal is required to be either a Judge of a High Court or is/has been a member of the Indian Legal Services and holds/has held a Grade I post in that service for at least 3 years. The term of a presiding officer has been limited to 5 years from his joining the post or till he attains the age of 65 years, whichever is earlier as per sec. 51 of the IT Act. However, a High Court Judge retires at 62 years and hence he is left with only 3 years term to serve the office. A presiding officer will naturally need time to get adjusted to the new arena of cyber laws. By the time he gets accustomed to the functioning of the tribunal, his tenure is almost over.  

28. **Need for Increased Awareness among Victims of Cyber Crimes**

The prospective victims mainly women and children should be cautious and should not reveal their phone number or address to unknown persons while chatting on the net. According to a study conducted on internet users, particularly teenagers and their parents, it was found that some parents were unaware that their children were exposed to unpleasant exchange of information through the internet. Therefore parents should keep a vigil at what their children are watching on the internet.  

Recently, the Global Intelligence Lab of the E-security Company Simetech has revealed that the cyber mafia has now started to use Hindi language on internet for phishing, virus and Trojan attack. Since the large fraction of population of Hindi speaking nations like India, Nepal, Bhutan, Bangladesh and Pakistan do not understand English easily, therefore, the cyber criminals employ Hindi in order to gather financial and personal details of these nationals by giving them fake lucrative offers.
29. **Need for Imparting Training to Officials to investigate Cyber Crimes**

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. Showing concern over incompetency of officers in investigating cyber crimes and the need for IT training to officials, recently Justice Alok Singh of Punjab and Haryana High Court, Chandigarh has asked the Director General of Police (Punjab) as to how many officers of Punjab Police are competent to investigate computer crimes. According to Section 78 of IT Act, 2000 no officer below the rank of DSP can investigate cyber offences. In the present case it was alleged that Mr. Satinderjit, who was an employee of Dhiman Group of Industries, has misused the secret password of the company to commit cyber fraud and he has applied for anticipatory bail before the HC. The investigation of this case was handed over to DSP Rajinder Singh who accepted before the HC that he has no knowledge of computer and IT and he even does not know how to operate a computer.\(^{40}\)

30. **Need for connecting Cyber Cafes with Police Control Rooms**

Uptil now the cyber cafes were required to maintain a register in which record of all the users of cafe was to be mentioned but the cafe operators were not performing this duty sincerely. Therefore, in order to prevent the commission of cyber crimes in cyber cafes it is suggested that the cyber cafes should be connected with the police control rooms so a constant vigil can be kept on the ongoing activities in cafes. First of its kind, recently in Oct. 2010 a plan was prepared by which the Police Control Room of Cyber City Gurgaon will be connected to all the cyber cafes of the city.\(^{41}\)

31. **Periodical reviewing of licenses of Internet Service Providers (ISPs)**

An ISP is required to take licence from the Department of Telecom (DoT) but various illegal ISPs are also operating in India without licence. Therefore, the licenses of ISPs should be reviewed periodically and strict action should be taken against the ISPs functioning without licenses. Recently the Intelligence Agencies in Shimla (H.P.) have initiated an inquiry into illegal ISPs functioning at McLeodganj and found that one such ISP named as ‘Tennor Network’ is illegal and is providing the facility of wireless internet connectivity to Tibetans residing in the area.\(^{42}\)

\(^{40}\)“Computer Se Anjaan Kareenge IT Case Ki Jaanch”, *Dainik Bhaskar*, February 11, 2011, p. 11

\(^{41}\)“Cyber Cafe Ka Record Foren Police Ke Pas”, *Navbharat Times*, October 18, 2010, p. 18

\(^{42}\)“Illegal ISPs under Scanner”, *The Tribune*, June 30, 2010, p. 10
32. **Need for development of Anti-hijacking Software**

Showing concern on the recent hijacking of official websites of CBI and Central Aviation Ministry in 2011, Mr. V.K. Saraswat, the Chief Scientific Advisor to the Defence Ministry has said that in the present scenario internet crimes are the greatest challenge to our national security and he warns the nation to be alert in this regard. According to him, nowadays all human activities have become based on Information and Communication Technology (ICT) through the use of computers, mobile phones etc. and in this backdrop its security concern have become more important. He further said that India needs to adopt such techniques which can assure the security of theses delicate systems. Moreover, in order to prevent cyber attacks from foreign countries he emphasized on the need to develop anti-hijacking software in India.\(^{43}\)

33. **Encouragement of Cyber Crime Victims to Lodge Complaints**

In most cases of cyber crime, the victims hesitate to lodge a case. Cyber crime expert Pawan Duggal says that out of every 500 incidents, only 50 get reported, out of these one gets registered. Therefore, the victims of cyber crimes should be encouraged to come forward to lodge complaints against violators of cyber law. Recently, in a first of its kind initiative in the country, Delhi Police has launched a 24x7 helpline for cyber crime victims from January 2008.\(^{44}\)

**Table: Cyber Crime involving e-banking, Data theft, Time theft, Hacking, Data conversion in Delhi**

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of cases</th>
<th>No. of victims</th>
<th>Amount involved</th>
<th>Arrest</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>12</td>
<td>22</td>
<td>50 lakhs</td>
<td>12</td>
</tr>
<tr>
<td>2006</td>
<td>17</td>
<td>32</td>
<td>90 lakhs</td>
<td>17</td>
</tr>
<tr>
<td>2007</td>
<td>25</td>
<td>28</td>
<td>1 crore</td>
<td>24</td>
</tr>
<tr>
<td>2008</td>
<td>78</td>
<td>59</td>
<td>2.5 crore</td>
<td>37</td>
</tr>
<tr>
<td>2009</td>
<td>254</td>
<td>176</td>
<td>3.2 crore</td>
<td>46</td>
</tr>
<tr>
<td>2010</td>
<td>1080</td>
<td>784</td>
<td>7 crore</td>
<td>79</td>
</tr>
</tbody>
</table>

34. **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

---

\(^{43}\) “Cyber World Se Hai Sabse Jyada Khatra”, *Dainik Bhaskar*, February 12, 2011, p. 15

\(^{44}\) “24x7 Police Helpline to Tackle Cyber Crime”, *Times of India*, December 30, 2010, p. 2
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.45

35. **Implementation of the Recommendations of Malimath Committee on Reforms in the Criminal Justice System**

The genuine efforts should be made to implement the recommendations of the Malimath Committee on reforms in criminal justice system which also gave following suggestions relevant in the context of investigation of computer crimes:

i. **Investigation**

The committee recommended that there should be specialized cyber crime squad in every State Crime Branch.46

ii. **Intelligence Network**

It further recommended that concrete steps ought to be taken to institutionalize criminal intelligence system and the main task of such body would be to collect, collate and disseminate information about major criminal gangs operating in the country involved in cyber crimes and other organized crimes. It would have a computerized data base, accessible to all State Police Forces and Central Agencies.47

iii. **Training of Officials**

The committee heavily recommended that facilities should be developed for imparting training in modern disciplines such as Forensic Accounting and Information Technology for cyber crime.48

36. **Computer and Cyber Crimes: Education and Awareness**

The subject of basic cyber laws should be made compulsory at the school, college and university level so as to increase awareness among the masses.

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

---

47 *Id* at p. 117
48 Supra note 46, at p. 102
being allowed to be misused by the criminal conduits for perpetration of 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.