Cyber Crime and Cyber Terrorism in India

Sarita Singh

Abstract: ***From cars to kitchen appliances, computers and the Internet continue to pervade human life in everything. With the discovery of machines, the Internet has amplified human enslavement. Although we have achieved many benefits in terms of effectiveness and management, many detrimental consequences and drawbacks have also been brought to the forefront. Cyberspace may now be used by individuals or organizations to serve foreign governments, or to terrorize a nation's people. By hooking a person "Cracking" on a government or military-maintained website, the crime of "cracks" will accelerate into terrorism. Cyber-terrorism could be a hospital hack. As a retaliatory act, dose. Informatics is a double-edged sword that can be used both for negative and positive work. Therefore, the fate of many businesses depends on the benevolent or vice intentions of the individual working with and through the technology, as the case may be. A malevolent intention communicated in the form of hacking, data theft, virus attack, etc., for example, can only bring negative effects. However, these methods can also be used to search for the authenticity, protection and security of one's technical device, which has been mainly relied on and effective to provide a specific organization with security. The whole thing seems to be intolerable, for example, the train ticketing system, if we currently think of society without the machine. Airline Ticketing and Traffic Control as well. Bill for electricity. The Telephone Bill Office functions etc. Without the machine, it seems to be intolerable. The most important means of communication, information, trade and entertainment has become computers with the aid of the Internet today. The internet is like life being expanded and carrying on in the real world in another medium that cuts space, time, nationality, citizenship, across borders, Competence, gender, sexual orientation, and age. Likewise, each coin has two sides, the internet with all the advantages of obscurity, transparency, and convenience has become an ideal place for criminals involved in making the net for illicit lucrative purposes, either monetary or otherwise.***

Keywords: The Information Technology IT Act, 2000, Joint Academic Network, JANET, National Science Foundation Network, NSENET

1. Introduction

In our daily lives, the threat of cyber terrorism has created a huge challenge. The insufficiency of the state system to resolve the problem has been proven by terror attacks in major metropolises, cities and tourist resorts around the world.

Many primary protection schemes are being introduced by countries to cope with the challenges. Most of the attempts, however, are designed as a common technique that could be effective in traditional terror attacks.

However, the insufficiency of the state system to resolve the problem has been checked by restrictions when it comes to a terror attack of an exceptional type. Many key counter measures for addressing the challenges are accomplished by the states. Most of the attempts, however, are designed as a common technique that could be effective in traditional terror attacks. There are limits, however, when it comes to a conventional-type terror attack.

The Information Technology (IT) Act, 2000 has exposed the consumer to a vast information bank of data on anything and everything. It still has more aspects of terrorism, however. The latest stories tell us that the terrorist is now being furnished to use the cyber space to carry out terrorist attacks. It is difficult to ignore the possibility of such attacks in the near future. Cyber space-related terrorism is commonly referred to as 'cyber terrorism.'

India has engraved a niche in IT for itself in the last couple of years. By replacing the manual method, most of India's banking industry, post offices, other offices, and financial institutions have implemented IT. In these IT agencies, cyber terrorist attacks are often carried out, i.e. hacking, fraud e-mails, ATM hacking, mobile phones, satellite phone hacking, etc. i.e. hacking, fraud e-mails, ATM hacking, cell phones, satellite phone hacking, etc. The paper envisages and understands the essence and efficacy of cyber-attacks and makes an attempt to research and evaluate India's attempts to resolve the problem and illustrate what else could be done

Definition of cyber terrorism and cyber crime

Cybercrime is a crime linked to information technology and computer technology. The system may have been used in a crime, or it may be an object. Cyber-crimes can influence the national security and economic situation of a country.

Hacking, copyright infringement, child pornography, and child grooming are all forms of crime. In this aspect, individuals can be affected by disclosure in open place of their confidential issues such as ATM Pin, bank information, etc.

When any terrorist groups write about women's protection, cross-border crimes, fiscal robbery, etc., a nation would be targeted.

In terrorist acts, cyber terrorism is the action of internet terrorism. Which implies the deliberate use of computers, networks and the public internet to cause disruption and damage to a person for their own purposes. These terrorists may have a political or ideological motive, which can then be seen as a form of terrorism. There are militant groups such as Al-Qaida, ISIS, Mujahidin, etc. In order to connect with their members, these organizations use the Internet.

2. Conceptual Analysis of Cyber Crime

Computers are currently becoming an integral part of the rapidly growing population in India as well as around the world. Computers are used in many areas, such as banking, manufacturing, health care, defense, insurance, scientific analysis, strategic decision making, law enforcement, etc.

For example, if we think about the current society without the machine, it seems to be an impossible railway ticketing system. Ticketing for airlines and traffic control. Electricity charge, office working for the telephone bill, etc.

Without a machine, it all appears to be an impossible thing. Computers today have become the most important medium for communication, information, commerce and entertainment with the aid of the Internet. In the real world, the internet has become like life that is being enlarged and carried on by another platform that cuts between the borders of space, time, nationality, citizenship, authority, sex, sexual orientation, and age. Likewise, each and every coin has two sides, the internet has all the advantages of anonymity, a liability, and convenience has become an ideal place for pensions involved in making the net for illicit gains, either monetary or otherwise.

The Internet has just turned the world into the Global Village of Knowledge. History is also a witness to much of the evidence that the destructive application of all technical inventions is as much as the positive one. IT is no longer different, with the majority of decent people using IT to find better ways that will improve the quality of human life.

History and development of Internet

The Internet has turned the world into a Global Village for Knowledge. The Internet has made this planet a virtual global marketplace without sleep. The Internet is a part of the global computer network. Internet and online networks, also referred to as "new media" services, as they provide some production-oriented content such as music, audio, video, graphics, text and games in certain ways close to conventional media.

The internet's origins can be traced back to the 1950s. The first satellite, Sputnik I, was launched by the Soviet Union in 1957, leading US President Dwight Eisenhower to create the ARPA agency for the arms race. Thus, through the use of ARPANET, funded by the US military, which was set up in 1969, the evolution of the internet may be said to have been developed. The very first point of contact between research centers at Los Angles University of California and the Stanford Research Institute.

ARPANET was a joint venture between the Massachusetts Institute of Technology and the Advance Research Project Administration of the American Department of Defense as a source of contact in the event of wars between remote computer resources. The contact ties to the military, defense contractors and the university laboratories involved in defense-related research were cramped. The developments took place in the early 1970s, such as the likelihood of electronic mail increased. Other networking equivalent to the ARPANET started during the time, such as the Joint Academic Network of the United Kingdom (JANET) and as the National Science Foundation Network of the United States. (NSENET).

In the year 1990, the US authorities have released ARPANET and have transferred it to the National Science Foundation (NSFNET).

The US authorities released ARPANET in the year 1990 and moved it to the National Science Foundation (NSFNET).

In the year 1993, he was the person who created the Time Bemers-Lec,

The World Wide Web (www) at the European Particle Physics Laboratory (CERN).
The first commercial browser known as Netscape was released in 1994, with the aid of the previous year's launch of its own Internet Explorer by Microsoft. So, there are browsers that make access to the internet from personal computers possible. A number of commercial Internet Service Providers (ISPs) have entered the market since the mid-1990s and provided a number of Internet connections via traditional telephone lines.

The Federal Networking Council (NFNC) has consistently adopted a resolution describing the word 'Internet' on the date 24 October 1955. This concept was created in conjunction with members of the Internet and the community of Intellectual Property Rights.

The term internet is characterized as a global information system that is logically connected by some globally specific Internet Protocol (IP)-based address space or its various extensions that can support communications using protocols such as the transmission control protocol/internet protocol (TCP/IP) suit or its subsequent extensions, or the other IP-compatible protocol.

Evolution Nature and scope of Cyber Crime

In this age, cybercrime is the harmless broad-range that threatens our world. Like a multi-headed hydra, it raised its head. Cybercrime can involve criminal acts that are usual in nature, such as theft, fraudulent forgery, defamation and mischief, where one is cutting other and newer forms of crimes are apparent or suddenly rising. The above machine also provides a variety of new-age crimes such as hacking, cyber stalking, web defacement, web jading, etc. In 1820, the first cybercrime was registered. The loom was designed by Joseph-Marie Jacquai'd, a textile not produced in France. The device made it possible to reproduce a series of steps in the interlacing of special fabrics. This resulted in a distress in Jacquard's jobs that threatened their normal employment and livelihoods. The acts of disruption were committed to freeing Jacquard from further use of the new technology. So, this is the first cybercrime that has been noted.

3. Cyber Criminality Categories

There are various cybercrime groups that are as follows:

3.1 Data Crime

a) Data Interception

In order to collect information, an attacker observes a data stream to or from a target. This attack may be tackled in order to gather information to help a later attack, or the ultimate aim of the attack might be the data collected. Sniffing network traffic also involves this attack, but it can involve detecting other forms of data brooks, such as radio.

The attacker is passive in most varieties of this attack and merely follows normal contact, however the attacker attempts to recruit the formation of a data brook in certain variants or affect the existence of the communicated data. Furthermore, The attacker is not the intended receiver of the data stream in all variants of this attack and distinguishes this attack from other data collection methods. The attacker detects explicit data channels (e.g. network traffic) and understands the information, unlike some other data infiltration attacks. This differs from attacks that gather more contextual information not freely shared through a data source, such as contact frequency.

b) Data Modification

Communication privacy is important to safeguard information that cannot be modified or accessed in transportation. Dispersed environments carry with them the risk that by messing with information as it travels between sites, a mischievous third party may commit a computer crime. In a data manipulation attack, before retransmitting it, an unauthorized party on the network interrupts data in transportation and changes parts of that data.

c) Data Theft

The time used to determine when information is illegally copied or taken from a corporation or another individual. This information is also operator information, such as passwords, social security numbers, and information about credit cards, other private information, or other sensitive corporate information. Because this information is unlawfully taken, it is possible that he or she will be punished to the fullest extent of the law when the person who took this information is arrested.

3.2 Network Crime

a) Network Interferences

Network Interfering with a computer network's operation by accessing, distributing, harming, removing, failing, modifying, or overpowering network data.

b) Network Sabotage

Sabotage Network' or incompetent administrators are attempting to do the jobs of the people who are normally responsible for the network. It could be just the overhead, or a combination of things. But if Verizon uses the kids' aid, delaying the line of first responders, then they might use network issues as an excuse to get the federal government to intervene with the public safety interest. Of course, if these people are returned to work by the federal government military, what is the point of unions and strikes anyway'

3.3 Access Crime

a) Unauthorized Access "The machine biscuit underground is an insider's point of view. An Unauthorized Access 'looks at the characters behind the computer screens and tries to distinguish the outlaw hacker's media ads from the reality.

b) Virus Dissemination

Examples of malicious software that ruins the victim's device are deceptive software that attributes itself to other programs such as viruses, worms, Trojan horse, Time Bomb, Logic Bomb, Rabbit and Bacterium.

3.4 Related Crimes

a) Aiding and Abetting Cyber Crimes

For most assisting and assisting charges against a person, there are three components. The first is that the crime was committed by another person. Second, the person who was charged had knowledge of the crime or the intent of the principals. Third, the person supplied the principal with some sort of assistance. Usually, an addition in legal terms is characterized as an individual who assists in the commission of a crime committed by someone or others.

b) Content-Related Crimes: Unwanted lucrative communications, cyber fraud and cyber risks are included in content-related offenses for cyber-sex. The overall cost to victims of these attacks is in the millions of dollars each year, which is critical for turning the condition of immature or underdeveloped countries into industrialized countries.

Classification of **Cybercrime**

Mostly speaking, the cybercrimes refer to all actions done with criminal intention in cyber space. Which is divided into three categories:

1) Cyber Crime against person;
2) Cyber Crime against property (against business and Non business organization);
3) Cyber Crime against Government.

1) Cyber Crime against Person

The first classification of cybercrimes perpetrated against people, including many such as child pornography transmission, sexual abuse against someone using a computer, such as e-mail and cyber stalking. Stalking can be considered to be any unwelcome communication between two individuals who directly or indirectly communicate a threat or put the victim in fear. One of the most relevant cybercrimes is today recognized by human trafficking, uploading and dissemination of absence content like pornography, indecent exposure and child pornography institutions. "The potential harm to humanity from such a crime can hardly be overestimated." Similarly, cyber harassment is a different cybercrime that can and does occur in cyber space or in cyberspace. The internet is a wonderful place to work, play and not less than a mirror of the real world, which means that it also contains electronic representations of real-life problems,

2) Cyber Crime against property

The second type of cybercrime is that against property of all sorts. Hacking is an unauthorized use of computer and network resources and breaking any breaks into another computer system often on a network or deliberately violates computer protection, Vims is a programmed computer that can duplicate itself and cause data contamination to be lost, copy-right protects creative or artistic works. Patent is a collection of exclusive rights given by a state to an author or to his assignment for a specified period of time in return for the disclosure of an invention. You can only copy or patented work with a violation of the copyright owner's permission. Violation. Cyber-squatting is registering, trading in or using a domain name with the intention of bad faith to benefit from the goodwill of a trademark belonging to someone else, etc. Among the most serious cybercrimes known to date are hacking and cracking. Knowing that someone has cracked into your operating networks without your knowledge and consensus has messed with priceless sensitive information and information is an awful feeling. The truth, coupled with this, is that no computer device in the world is evidence of hacking. So, it is unanimously accepted that it is possible to hack any and every scheme in the world.

Cyber Crime against Government

It would be possible to describe cyber terrorism as premeditated. Politically attacking the information system, computer systems, and data to refuse service or obtain information in order to damage the target's political, social or physical infrastructure, resulting in public violence. During 1998, LTTE Liberation Tigers of Tamil Elam attacked a large number of the computer system of the Sri Lankan Embassy around the world by releasing 800 e-mails to each embassy, usually with the messages over a two-week span, we are internet black tigers and we are using this to disrupt your communications: this is the first documented terrorist attack on the computer system of a country.

Cybercrime and Indian Position

The first cyber-crime occurred in the year 1820. But only in the recent past did India gain traction. The Indian Parliament thus gave effect to a resolution of the United Nations General Assembly on the adoption of a Model Law on Electronic Commerce. The passage of the Information Technology Act 2000 was significant. The Act aims to control and legalize e-commerce and to take cognizance of crimes coming from there. The IT Act covenants with the following cybercrimes together with others:

Tampering with computer source documents

An individual who knows or intends to conceal, rescind (demolish or reduce), alter (change features) or cause another person to hide, rescind, and change any computer source code that is used for a computer, computer program, computer system, or computer network is punishable if the computer source code is needed to be preserved or maintained by law. For e.g, beating the C.D.ROM where the source code files are stored, converting the C file to a CPP file, or deleting a file's read-only attributes.

Hacking

The unauthorized access to a computer system and networks is commonly considered to be hacking. The word "hacker" initially defines any amateur computer programmer who has found ways to run software more resourcefully. Hackers typically "hack" on a problem before they find a solution and keep trying to operate in new and more efficient ways with their equipment. A Code Thief, Cracker, or a Cyber Punk may be a hacker.Whoever intends to cause or recognize that it is likely to cause unjust loss or harm to the public or any person abolishes or erases or modifies any information in a computer resource or decreases its value or usefulness or damages it by means of hacking is said to commit.***VinodKaushik and Ors.*** **Vs** ***Madhvika Joshi and Ors.***[1]The key concern in this situation is if accessing the email account of a husband and father-in-law without their permission amounts to 'unauthorized access'. It was a case where the first respondent had accessed her husband and father in law's email account in order to collect evidence in a Dowry abuse case. The Adjudicating Officer held that it is a violation of section 43 of the Information Technology Act 2000 to access an e-mail account without authorization. The claimant was not given any money because the respondent had only provided the details collected to the police department and the court.

However, the Adjudicating Officer ordered the first respondent to pay a fine of Rs.100, as it was held to be in violation of the IT Act 2000, Section 66-C (identity theft and deceptive use of any other person's password). It should be noted that, in the event of a breach of privacy by accessing e-mail accounts without the consent of the recipient, there can be no defense of bonafide intent. It will still be construed as 'unauthorized entry'.

It will still be construed as 'unauthorized entry'. It is also interesting to note that the adjudicating officer relied on the reasoning that only the Court and the police were aware of the details collected by the 'unauthorized access, so the respondent is not liable to pay the claimant any compensation.

Publishing of information, which is obscene in electronic form

Any person who publishes, transmits or causes to be published in electronic form, any material that is lascivious, or if its effect is such that it threatens to harm and corrupt persons who are likely to read, see or hear the matter contained or incorporated in it, shall be liable to punishment. Publishing (generally making known or releasing copies for sale to the public) or distributing (transferring or acting as a conduit for) or causing (the effect of publishing) pornographic content in electronic form are essential components of such an offense.

Child Pornography

It is a part of cyber pornography, but it is a vital offense that is often known as a cybercrime by individuals. The Internet is highly used by its users around the world to access and sexually assault children. A domiciliary product in India is very easily flattered by the Internet. The explosion made the children a potential cyber-crime suspect. If more families have access to the Internet, more of the children use the Internet, and so are the chances of falling prey to Pedophiles' violence. In order to lure children and even contact them in different chat rooms, the pedophiles use their fake identity to support them and obtain personal information from the innocent prey. They also began to target kids through their e-mail addresses. In order to assess sexual harassment or to use them as a sexual object, these pedophiles slog children to the net.

Breach of confidentiality and privacy

Any person who, without the consent of the person concerned, obtains access to any electronic record, book,

[1] *VinodKaushik and Ors.* v. *Madhvika Joshi and Ors Air 2015*

register, correspondence, information, document or other material or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable for punishment under the Information Technology Act. **Nirav Navin Bhai Shah and Ors Vs State of Gujarat and Another.**[2]The appellants were accused of having hacked into the complainant's computer system and pilfered substantial data. The key question was whether criminal charges could be quashed on the basis that an amicable settlement had been reached by the parties. The Court ruled that the Court would quash criminal charges to that effect if the 'whole' dispute had been amicably resolved. In this case, along with other offences under the Indian Penal Code 1860, the appellants were convicted under sections 66 and 72 of the Information Technology Act 2000. The defendant argued before the Court that, because the issue is civil in nature, the criminal procedure should be quashed. The Court dismissed the claim, arguing that the crime cannot be treated as a civil conflict since the offences are offenses against society under sections 66 and 72 of the Information Technology Act 2000 and cannot be condoned. The Gujarat High Court ruled that privacy and hacking breaches are offences against society and cannot be condoned or viewed as a civil conflict. However, if the parties agree to a settlement of the 'whole' conflict, in the interest of justice, the Court can approve such a settlement.

Cyber Crime against Government

(Cyber Terrorism)

There are various languages, religions, cultures and geographic regions, but the birth process is the same. A man sees the sunshine in the said identical phase regardless of caste and religion in the entire world. A developed mechanism regulates the birth and death of a man. There can be no difference in the S3 method between politics, culture, linguistic religion and geographical areas. The birth right of every human being is the right to life, the right to liberty, the right to speech, free air and water pollution, small shelter over the head, a piece of cloth and bare minimum food to save life.

These rights are the fundamental rights of a civilized human being without whatever language he speaks or wherever he lives, without which no one can survive a decent life, but because of the structure itself creating a gap between the classes and the people, those rights are again and again affected today.

The innocent poor people do not get their proper share of what they are entitled to and for this reason some segments of people are unhappy with the system and resort to taking the law into their own hands to accomplish their goals by violence that is an expression of frustration or indignation, and this phenomenon is not to be labeled as terrorism. In order to achieve specific objective or desired objectives through force, terrorism can be described as a method of violence-murder, abduction, bombing, hijacking of aircraft, and taking air hostages.

Terrorism defined by Federal Bureau of Investigation " Unlawful use of force or violence against individuals or property in order to threaten or induce a government or a civilian population, or any component thereof, to achieve political and social goals. As individual terrorism, group terrorism, state terrorism, revolutionary terrorism, international terrorism and the last one developed through technological growth, i.e. cyber terrorism

Forms of Cyber Terrorism

Cyber terrorism is a very severe problem which involves a wide variety of attacks. Cybercrime is a crime that attacks devices. Cybercrime may include theft of intellectual property, patent defilement, trade secrets, or copyright laws. Cybercrime, however, also involves attacks on machines in order to purposely disrupt processing, which can include spying to produce unsanctioned copies of sensitive data. Botnets, Estonia, 2007, Malicious Code Hosted on Websites, Cyber Espionage etc., may be some of the main cybercrime methods.

It is necessary to note here that other forms may be included under the heading of Cyber Crime and are also important instruments for terrorist activity at the same time. One by one, these illegal acts are addressed as follows:

Attacks via Internet

(i) Unauthorized access & Hacking: Unauthorized access can be described as any kind of access without either the rightful owner or the individual who is allowed to access a device, computer system or computer network being approved by anyone. Hacking is any act committed to breaching a device or network. To attack the target computer, hackers inscribe or use acceptable computer programs. They own the ability to kill, and they get the kick out of destruction like that. Some of the person hacks for own fiscal gains, such as theft of credit card numbers, transfer of money to their own account from different bank accounts, followed by withdrawal of money. By hacking the web server of someone or taking control of the web site of some other person called web hijacking.

(ii) Trojan Attack:

The software is called Trojans, which behaves like something valuable but does stuff that are quietly hindering. The Trojan horse is a common name. Trojans come in two parts, a pail for the client and a section for the server. The attacker will then use the client to connect to the server and start using the Trojan while the victim (mistakenly) is running the server on his computer. The TCP/IP' 'protocol is the normal form of protocol used for communication, but the UDP protocol is often used by some Trojan functions.

(iii) Virus and Worm attack:

The virus is a program that has the potential to contaminate other programs and render copies of itself and the banquet into other programs. Worms are named programs that spread like viruses but feast from machine to machine. The "Michael Jackson e-mail virus-Remembering Michael Jackson" is the most recent of these attacks. Once the computer is contaminated, the worm will spread to other internet users automatically.

[2] *Navin Bhai Shah and Ors. v. State of Gujarat and Another Air 2006*

E-mail & IRC related crimes

(i) Email spoofing:
Email spoofing refers to emails that appear to have come from a source when they have actually been sent from another source.

(ii) Email Spamming:
Email spamming, similar to a chain letter, refers to the sending of emails to thousands of people.

(iii) Sending malicious codes through email-
This is the offense when e-mails are used to send any viruses, trojans, etc. as an attachment via emails or by sending some sort of website connection that downloads different malicious code when visiting.

(iv) Email bombing:
E-mail bombing is characterized by abusers who deliver an identical email to one specific address repeatedly.

Attack on Infrastructure These are all managed, regulated and facilitated by sophisticated computers, networks and software by our banks and financial institutions, or transportation systems such as air, sea, rail and highways, telecommunications, electrical power grids, oil and natural gas supply lines. Characteristically, in these networks, control centers and main nodes are far more vulnerable to cyber than physical assaults, giving many cyber terrorists significant opportunities. In addition to infrastructure or business, there may be several potential sanctions for a cyber-terrorism act, including a separation of costs into direct as well as indirect effects.

Attacks on Human Life:

Examples: -In the case of an air traffic system that is strictly high-tech and is designed to classify aircraft flight paths, the flight courses shall be calculated for all aircraft to be followed in the air. Aircraft pilots will need to search the course as well as the other aircraft around using the on-board locator systems that are not linked to external networks, so the cyber terrorist can target it. The act of cyber-terrorism against a highly automated factory or plant production of any kind of food goods, machinery, cars, etc. will be another example.

Rajagopalvs. State of Tamil Nadu.[3]Violation of both civil and criminal penalties under the respective rules. Modem effort and exploration have exposed him to mental pain and suffering by assaults on his privacy, far greater than mere physical injury could inflict. The right to privacy is protected under Article 21 of the Constitution of India and forms part of the right to life and personal liberty. The traditional notion of the right to privacy has taken on new dimensions with the advent of information technology, which needs a distinct legal viewpoint.

4. Conclusion and Suggestions

4.1 Conclusion

Changes are inevitable and it is not possible to escape the dilemmas presented by advances in technology. As per current society, the fact is that criminals have modified their crime tactics and have just begun to rely on technological innovation, and now society, civil, and law enforcement agencies, private businesses, as well as organizations, will need to adapt their mechanism to combat it in order to cope with these types of crimes.

In addition, such experts not only need to be competent, but also need to be equipped with necessary technological hardware and software to combat cyber criminals effectively. Therefore, in many parts of the country, the requisite facilities need to be recognized so that crimes can be monitored in the virtual world.

The alternative factor to be stressed is that the culture of continuous cyber education and learning needs to be educated among law enforcement officials as well as law enforcement authorities, since the field of information technology is now very complex as expertise has become redundant in a very short period of time.

Finally, the prelude to the Information Technology Act 2000 provides that the Act was passed in order to provide legal appreciation for transactions carried out through the exchange of electronic data and other means of e-commerce, and the Act has also made several amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1872. While the purpose of the Act is not to resolve unlawful crime, certain wrongdoings and punishments to overcome such omissions are well established in this act.

It can be indirect from this that the legislation cannot continue to be stagnant, it must be altered with the advancing times.

Since with the rise in the number of computer device and internet users worldwide day by day. With the aid of the internet, which is the intermediary for enormous facts and a large communications base around the world, it is becoming easier to access any information quickly in very few seconds. People need to take clear protective steps when using the internet, which will help to challenge the major threat of cybercrime.

Countries around the world are facing these challenges and are doing their best to avoid this problem. However, this issue cannot be successful without the assistance of the general public and the judiciary. In addition to general public sentiment, the legislature does not support a rule for the country at large. Therefore, it is first important to receive public support not only at the national level but also at the international level. People around the world are not opposed to the interpretation of legislation prohibiting the use of malware, but they are also mindful of their own legitimate rights.

[3] *Rajagopal vs. State of Tamil Nadu Air 1994*

Thus, on a priority basis, the legislation to be enacted by the legislature ought to take care of the public interest. This can only be done if legislation embraces the necessary technologies, which could only take care of the threat created by computers by sending malware. Therefore, before a law is enacted that explicitly deals with cyber terrorism, we should not feel shy and unwilling to use the existing provisions. To sum up, because the achievements in the field of communications and information technology lie in the contemporary world, it is highly imperative to check the appearance and rising danger of cybercrime.

4.2 Suggestions

1) In the enforcement of cyber law, the judiciary can only play a critical role if it is equipped with high technology. To be recognized as e-justice, it must follow new mechanisms of justice administration. Electronic justice will have speedy trials without unnecessary delay in order to prosecute cyber criminals. Delay in trial may result in loss of evidence as, compared to other records, electronic records are not of a permanent nature. It is proposed to enact the Electronic Code of Criminal Procedure for e-courts for expeditious trial by the Indian Parliament. The Law Commission of India has stressed the need for more cyber laws to be enacted and for electronic courts to be created to deal with cybercrimes.
2) It is proposed that the scope of current legislation can be expanded to include a range of cyber operations, but it is not appropriate to overlook the compliance element. Prevention is better than cure, so proactive steps to secure electronic data are more fruitful than enactment, and this mission can be better accomplished by high-tech professionals. Law is an important tool for controlling human actions, but scientists and technical people should play a better role here in high-tech. It is noted that adolescents commit cybercrimes and often play hacking games to take on daring tasks.They are unaware of the results of their actions. They are also unaware of the cyber law's deterrence provisions. In school education, cyber ethics should also be included in the course curriculum. Hacking-minded children's programs can be used for constructive purposes.
3) Some training and infrastructure development in this field should also be supported by our judiciary.
4) Investigative agencies must be allowed to deface extremist websites and networks in order to stop and monitor net warfare.
5) There is a need to establish laws to deter and monitor cyber terrorism where terrorists use mobile and wireless devices. Specific legislation was required to establish the responsibility, liability and transparency of internet service providers: e.g., they must be prevented from using their customers' user numbers.
6) Through investigating suspected wireless, mobile phones, and service providers such as 'history' in computers, cyber terrorism can be monitored via Change administrator's password from the default password. If the wireless network does not have a defaulting password, create one and use it to defend the network.
7) Switch off the network, disable file sharing on machines, etc. during extended periods of non-use.
8) Check your online account regularly to make sure that all the transactions listed are accurate. Using a number of passwords, not the same for your whole account.
9) Never respond to text messages from someone you don't know and carefully open an email attachment.
10) Never let your mobile phone be used by someone you don't know and stop sharing your cell phone number online.

References

[1] https://www.meity.gov.in/content/cyber-laws
[2] https://www.ikigailaw.com/cyber-security-framework-under-the-it-act-in-india/#acceptLicense
[3] Text book the art of invisbility by kevinmitnick release date 4 Feb 2017
[4] https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf