CYBER CRIMES THREAT TO NATIONAL AND INTERNATIONAL SECURITY: AN ANALYTICAL STUDY

[1]KAMSHAD MOHSIN, [2]PROF. (DR.) KB ASTHANA
[1]Research Scholar (Law)
Kamshadmohsin@gmail.com
[2]Prof. of Law and Dean, Maharishi Law School
kbasthana001@gmail.com

Abstract
Despite the fact that most individuals would claim to understand what terrorism is, there is startling lack of a universally accepted definition. The use of violence or the threat of violence is the sole overarching thread among the literally hundreds of definitions currently in use. Only "Political" and "fear, terror emphasised" are the other components that are included in more than 50% of definitions. As a result, some governments view some terrorist organisations as having the right to fight. This hinders international collaboration. The motivation behind terrorism is different from those of other crimes; it is carried out with a specific goal and strategic objective in mind.

Keywords: Cyber Crimes, National, International, Threat

INTRODUCTION

We must think about who the terrorists are. There are countless organizations of various sizes and capabilities that, in some cases, qualify as terrorist organizations. There are four standard reasons for terrorism. First, there are terrorists who only support one cause and are willing to use violence to spread that message in the hopes that their particular grievance will be resolved. The two most common of these topics are animal rights and anti-choice in terms of abortion. Researchers who study vivisection or family planning professionals have been the targets of ongoing campaigns and murders in protest of these issues.

MISUSE OF INTERNET BY EXTREMIST

These logical terrorists require a platform to spread their message and "justify" their actions in order to carry out their campaigns for a political or social end goal. Terrorism depends on propaganda. Before the Internet, it was fairly difficult to reach a broad audience using this. Print and television media would carry reports on terrorists, but they would be subject to editorial control and occasionally to legal restrictions. Only a small number of people who were interested in the terrorists' cause would read books, journals, and pamphlets.

The terrorist group can easily and unrestrictively spread its message by simply including the appropriate keywords or links on what appears to be a mainstream website. As they control the information, they may use it to publicly broadcast the main grievances that drive terrorists and support them with 'evidence' that the organisation has created and altered. These websites use multimedia to draw attention and give visitors a sense of legitimacy while giving them the appearance of being official.

These websites use multimedia to draw attention and give visitors a sense of legitimacy while giving them the appearance of being official. They also have the advantage that their information operations are not constrained by truth or traditions, allowing them to modify propaganda to make it seem credible without any true foundation. There were about 4500 websites that supported terrorism by May 2005, according to the US State Department's list of terrorist organisations, and there were over 5500 by 2007. The German Bund Deutscher Juristen serves as an illustration of how readily disinformation may be spread via websites.

The chairman of the German Lawyers' Association, Dr. Claus Grötz, was featured in an artic le on this website, and it quoted him as saying that testimony obtained through minor torture might be admissible in German courts. The public demanded his resignation, and it became major news. Before the'story' went viral, the site had only been up for two days, and neither the Association nor Dr. Grötz actually existed. Despite the fact that this is not a terrorist case, it illustrates the potential weaknesses that a terrorist organisation could have. The report wasn't verified and

presented to the German people as legitimate by the mainstream media, which was considered lazy journalism.

To have this about a State's action relating to a terrorist situation could be used by the terrorist organization to gain public sympathy and international condemnation of the victim state.

The groomer will pass the potential recruit onto a recruiter who, at that stage will, for the first time, make indications that they are from a terrorist organization. From this point the skill set of the potential recruit will be examined and their commitment finally checked before they are in a position to ever actually meet or know the identity of anyone they have been engaged with.

According to U.S. National Infra-structure Protection centre, Cyber terrorism defines as-
A criminal act perpetrated by the use of computer and telecommunication capabilities, resulting in violence, destruction and disruption of service to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government population to conform to a particular political, social or ideological agenda.[1]

In order to coerce or intimidate a government or its people in order to further a political, social, or ideological objective, unlawful attacks or threats of attacks against computers, networks, and the information stored therein are referred to as cyberterrorism. Either assaulting the key infrastructure online or abusing the internet are methods of cyber terrorism.[2]

CYBER CRIMES AGAINST PERSONS:

There are certain offences which affect the personality of individuals can be defined as:

- Harassment via E-Mails: • Email-based harassment: This sort of harassment is fairly widespread and involves sending letters with attachments of files and folders. Because more people are using social media sites like Facebook, Twitter, etc., harassment is becoming more widespread.

- **Cyber-Stalking:** It implies using computer technology, such as the internet, e-mail, phones, text messages, webcam, websites, or films, to express or imply a physical threat that incites terror.

- **Dissemination of Obscene Material:** It involves hosting websites that carry these illegal materials, as well as indecent exposure and pornography (essentially child pornography). The adolescent's mind could be harmed by these offensive topics, which have a tendency to deprave or corrupt it.

- **Defamation:** • Impersonating someone with the purpose to diminish their dignity is done by hacking into their email account and sending offensive emails to other people's accounts.

- **Hacking:** It denotes taking control of a computer system without authorization and entirely erasing all data and computer programmes in the process. Hackers frequently target mobile and telecom networks.

- **Cracking:** It is one of the most serious cybercrimes known to date. It's a terrifying feeling to realise that someone has broken into your computer systems without your knowledge or authorization and messed with sensitive secret data and information.
- **E-Mail Spoofing:** A spoofed e-mail is one that falsely represents its origin. It demonstrates that its origin is distinct from where it truly originates.

- **SMS Spoofing:** Spoofing is the blocking of unwanted unwelcome messages via spam. In this case, an offender steals another's identity in the form of a mobile phone number and sends SMS via the internet, and the receiver receives the SMS from the victim's mobile phone number. Cybercrime against any individual is quite severe.

[1] *Wilson Clay: Computer attack and Cyber Terrorism (2003).*
[2] *Sastry P.K: Computer Science and Computer Forensis (2001).*

- **Plastic Money:** It refers to fraudulent debit and credit cards,that are used by thieves to steal money from victims' bank accounts. In this category of cybercrimes, there is always unauthorised usage of ATM cards.

- **Cheating & Fraud:** • It indicates that the individual stealing passwords and data storage has committed the cybercrime with a guilty mind, which results in fraud and cheating.

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

For instance in the case if supervisory control and data acquisition system (SCADA)[3] which is connected to the internet and run in commonly understood operating systems using well known standard communications protocol include railroads track switches, draw bridges, sewage treatment and water purification plants, traffic signals in busy cities, the electrical distribution grid, subway control systems and other critical systems that can easily cause massive injuries and loss of life if exploited maliciously.
For eg. Cyber terrorism attacks in these systems in Romania where a cyber terrorist illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. This is possible because in many cases, access to these systems is not controlled as tightly as expected given in their potential impact on life and safety.

ROLE OF CYBER SPACE IN PROPAGANDA

Senior Al Qaueda leader Ayman-al-zawahiri wrote “we are in a battle and more than half of this battle is taking place in the battlefield of the media” and internet plays a very important role in propagating the acts of terrorism.
Terrorist organizations exploit the internet medium to raise awareness for their cause, to spread propaganda and to inspire potential across the globe. Websites operated by the terrorist groups can contain graphic images of supposed successful terrorist attack, lists and biographies of celebrated martyrs and forum for discussing ideology and methodology.

As an example:
i) According to reports, the Quetta Shura Taliban runs a number of dedicated websites, one of which features an Arabic-language online magazine and daily electronic press releases on other Arabic-language jihadist forums.

ii) Websites may also contain detailed instructions on how to construct and deploy weapons, including cyberweapons.

iii) The website of HAMAS, for example, shared more than 20 really beneficial design elements, such as search engines, mission statements, a what's new part, and a frequently asked questions page.

ROLE OF CYBER SPACE IN FUN-RAISING

To enable fund raising various techniques and methods are adopted by terrorist group and one of the easiest way of raising fund is the through phishing, through online credit card fraud. Further, terrorists and extremists in the Middle East and South Asia are increasingly collaborating with cyber criminals for the international movement of money and for the smuggling of arms and illegal grogs.

CYBER SPACE AS MEANS OF COMMUNICATION

The primary advantage of the Internet offers to all including terrorist group centers around its used as a medium for communication, networking and publishing. And such communication is executed by the means if chat rooms, email, even hidden messages found in websites. Such means offers for

[3] *Supervisory control and data acquisition system (SCADA) related to the nation’s critical infrastructure and are the industrial controls systems that are managed by computer system)*

relatively sure and rapid communication between terrorist operatives. Furthermore, beyond the normal use if email and chat room communication, terrorist take advantage of commercial encryption software to enhance their security, uses steganography, the use of secret messages, hidden in apparently harmless information, that is then posted online

All of this suggests that the internet can serve as a primary means for strategic communication also DOD has defined strategic communication as focused United States government efforts to understand and engage key audience to create, strengthen or preserve conditions favorable and engage key audiences to create, strengthen or preserve conditions favorable for the advancement of the United States government interest, policies and objectives through the use if coordinated programs, plans, themes, messages and products synchronized with the actions of all instruments of national power. The use of such as facebook and twitter as a means of strategic communications and public diplomacy.

These tools can not only spread propaganda but can also host embedded malicious software in links and applications that can corrupt an unsuspecting user's electronic device. Based on these security concerns, several services and offices within DOD had banned certain social networking sites from access on unclassified networks.

PLANNING AND COORDINATION

Terrorist have been known to use the internet as a major took to plan and organize attacks for instance, through using public email addresses and chat rooms to provide instructions, orders and plans for communication operations.

TO SPREAD PUBLICITY IN FOLLOWING WAYS

1. Internet can be used to wage 'psychological warfare' for instance through the dissemination of horrific images and threats aimed to spread fear such as the release of execution videos in which Islamic fundamentalist groups behead kidnapped western victims.
2. Internet can be used to garner support: terrorists spread publicity which attempts to emphasize issues of victimization and injustice and arouse the emotions of supporters and potential supporters.

Thus these six differences categories, sometimes overlapping, also include Data mining[4] Networking, Recruitment and Mobilization, instructions and Online manuals (Training) Planning and Coordination, fund-raising and attacking other terrorists. Such use if Internet is described as Instrumental use if Internet)

The Question can be raised as to why the internet is being such an attractive medium for terrorists?

1. The technological difficulty associated with tracking and tracing cyber communications which is based on Internet Protocol (IP).
2. Another layer of difficulty in tracking and tracing cybercrimes is caused by disparities in the various legal systems around the world.
3. Inadequate and inconstant legal frameworks governing cybercrimes and government access to information.
4. Jurisdictional issues such as the necessity of letters oratory, dual criminality requirements, extradition restrictions, conflicts of laws and inadequate procedural laws.
5. Lack of sufficient technical experience of law enforcement prosecutors and judges regarding investigative assistance and the search and seizure of electronic evidence and
6. Inadequate mechanisms and procedures for international cooperation.
7. Easy access and way to propagate through numerous televised broadcasts, published memoirs, giving interviews, giving instruction on as to how to post videos, defeat and ehance security, conduct anonymous browsing, crack server vulnerabilities and use third party hosts to disseminate information and posting speeches on the Internet (Al-Zarqawi posted beheading of the U.S contractors and took credit for suicide bombings on behalf of Al-Queda. He showed his face in an internet video and accused the President Bush of lying to Americans about military successes in Iraq. His posting and media campaign, conducted largely over the internet, helped attract Al Queda followers to Iraq and establish the irony that tge U.S invasion is Iraq, not Saddam Husssein, had enabled Al Queda to use Iraq as a breeding ground for terrorist activities. Setmariam called on

[4] *in the data mining the internet is a vast source of information on the topics and is utilized by terrorists ti gather any information that may be relevant to their causes or to future operations- such as the satellite images, maps and blueprints of future targets. Information from http://www.unicri.it).*

internet for the use of weapons of mass destruction against the United States. Dirty Bombing for dirty nations.).

The threat of misuse if this technology is growing with each day and with every development in technology and this is possible because of:

1. Globalization if the Internet user that makes governmental efforts to control Internet attacks much more challenging than ever before.
2. Many hackers oriented sites resulting in democratization of the tools to be used for disruption and destruction.
3. Terrorist organizations have broken away from their place causing further complications to our technologically vulnerable societies.

These new political realities, coupled with easily accessible cyber weapons, have enhanced the threat and capabilities of terrorist group to the degree in which they could forever alter our planets existence as already stated that information technology is double edge sword, which can be used for destructive as well as constructive work. Thus, it is upon the intention of the user, vise or benign that the fate of many ventures depends.

For instance, where IT has been used for the benefit if the society,

1. The creator of the "Sasser worm" has been hired as a "security software programmer" by a German firm, so that he can make firewalls, which will stop suspected files from entering computer systems. Thus, these methods may also be used for checking the authenticity, safety and security of one's technology device, which has been primarily relied upon and trusted for providing the security to a particular organization.
2. Another commonly offered scenario involves the air traffic system. The world's air traffic control system is highly computerized. The terrorist either obtains control of the system of alters the system in such a fashion that airplanes are flown into each other, resulting in mass death.

Ross Anderson[5] has also suggested research into how to port techniques and experience from the world of electric warfare (EW)[6] analysis, which is a tool of the signal intelligence (SIGINT) community. Traffic analysis is looking at the number of messages by source and destination. This can give very valuable information not just about imminent attack but also about unit movements[7].

However, sometimes terrorists have targeted critical infrastructure to cause disruption only. At other times terrorists have target critical infrastructures, including critical information infrastructures to maximize disruption in addition to generating fear through deliberate attacks on human life (as occurred with the world trade center attacks). Worldwide there have been numerous cases of conventional methods used to attack critical information and other infrastructure.

There are many instances of where internet is being used leading to catastrophic results such as:

1) During the 1990s some of the operations planned and conducted by the provisional Irish republican Army were assessed to have the primary goal of causing damage and disruption to critical infrastructures while minimizing harm to people.
2) The October 1992 week end bombing of the square mile financial district of London and the planned bombing of six substation of the London power grid 1997.
3) In Romania, cyber terrorist illegally gained access to the computers controlling the life support system at an Atlantic research station thereby endangering life 58 scientist.
4) In October 2007, the website of Ukrainian President VikatorYushchenko was attacked by the hackers.

Likewise there are innumerable examples of attack of terrorism using internet as the means, thereby causing huge loss to human in terms of life and money both. Cyber attacks are not only a national concern but is a worldwide problem for which all the major nations of the world are coming together in order to find out a solution and to combat the problem of terrorism including cyber terrorism.

[5] *Ross Anderson is a researcher, writer and industry consultant in security engineering at the University of Cambridge computer laboratory, where he is engaged in the Security Group.*

[6] *Electronic warfare is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection and electronic warfare support.*

[7] *Paper presented by M.W David, K. Sakurai combating cyber terrorism: countering cyber terrorist advantages of surprise and anonymity", cubic corporation, Kyushu University.*

CYBER SECURITY IN INDIA

The purpose of cyber security is not to stop data from moving "down" a hierarchy, but rather to stop it from moving "across" departments. Relevant applications include everything from national intelligence to healthcare. There are various techniques for implementing access controls and information flow controls in a multilateral security architecture (the intelligence community uses compartmentation for this). the BMA model, created by the British Medical Association to define the information flows permitted by medical ethics, and the Chinese Wall model, which describes the processes employed to prevent conflicts of interest in professional practises and the BMA model, which was created by the British Medical Association to represent the information flows that are allowed under ethical standards in medicine. However, these models are not the final answer to the issues we are currently facing; rather, they are meant to create a security framework that can be used by both individuals and governments to prevent the misuse of ICT.

The ICT and e-governance foundation is secured by a cyber security system. Although not sufficient to address the issues presented by the internet, India has established cyber security provisions that go some way towards attempting to curb the annoyance brought about by improper use of the internet by making physical laws effective in the virtual realm. Cybersecurity is defined in India under Section 2(1)(n)(nb)[8] as the process of preventing unauthorised access to, use of, disclosure of, interruption of, alteration of, and destruction of information, equipment, devices, computers, computer resources, and communication devices.[9]

Immune: To create havoc in the country these are lucrative targets to paralyze the economic and financial institutions and the damage that can be done with the use of internet and technology can be catastrophic, irreversible and beyond imagination[10].
In recent year's cyber Attacks have taken a toll, some targeted attack and other are opportunistic attacks[11].

Targeted attacks, which are pre-planned, primarily aim to bring down government infrastructure. Opportunistic (Directed) attacks, which can be planned or unplanned, target private sectors, while random attacks target internet users, or citizens. All three types of attacks are carried out either to incite terror or to produce disastrous outcomes. However, despite this attack, India continues to lag behind other countries in the fight against crimes conducted via the internet, computers, computer systems, and computer networks. The following issues and problems are mostly to blame for this-

a) Lack awareness and the culture if cyver security at individual as well as institutional level.
b) Lack of trained and qualified manpower to implement the counter measures.
c) Too many information and security organization which have become weak due to 'turf wars' or financial compulsions.
d) A weak Information and technology Act which has become redundant due to non-exploitation and age old cyber laws.
e) No email accounts policy especially for the defence forces, Police and the agency personnel.
f) Cyber attacks have come not only from terrorist but also from neighboring countries inimical to our National interests.
g) In India there is no emergency response team for phishers and they don't respond as fast as an Amercian or European bank would[12].

Even though India faces significant difficulties in combating cyberattacks, some initiatives have been taken by India. Madhabi Puri Buch explains that we have taken an initiative that includes introducing true factors verification on the websites. This means that in addition to the user ID and

[8] *Inserted vide Information technology Amendment Act 2008.*
[9] *Information and technology Amendment Act 2008.*
[10] *Cyber security in India's counter Terrorism strategy, available at: www.ids.nic.in*
[11] *B J Srinath "Cyber security : threat and concerns, Indian computer Emergency response team (CERT-In), Ministry if communications and Information technology Government of India, Source: Data breach Investigation report, 2014. Available at: www.cpri.in/security2015/TI_Lecture_1_ Securing_Indian_cyber.*
[12] *Cyber Law cases available at: http://www.cyberlawsindia.net data assessed on 15th May, 2023.*

password, the customer now has a challenge mechanism, where we ask them things only they know and only if the answer is correct, do we allow him to do a transaction. Phishing plays a significant role in raising the funds for terrorists.

Further to promote, it is vital to look into the technical tools that organisations use to assist terrorist actions, such as looking at ICT infrastructure, in order to manage and combat the act of using the internet to promote terrorism. This include looking into things like electronic propaganda, social networking technologies, and anti-forensics techniques. Improved intelligence gathering tools against terrorists are needed, as are appropriate legislation, proper procedures for terrorist capture, prosecution, and punishment, and increased security at locations where terrorists have been able to cause significant damage, most notably airports.

Additionally, with the aid of IPv6, which has a larger header space and a 128-bit IP address, some actions can be made to identify and trace the cyber communication. This enables unique IP addresses to be provided to all users. In fact, IPv6 adoption will enable many quadrillion distinct IP addresses, which is sufficient to give addresses to all computers, RFID tags, sensors, unmanned aerial vehicles, and other networks-communicating devices. Additionally, IPv6 requires either authentication, encryption, or both for every packet, preventing spoofing and enhancing tracking and tracing.

Another technique of tracking cyber communication is the concept of security and cyber forensics. However the two concepts are not only interrelated but also indispensably required for the success of each other.

THE INFORMATION AND TECHNOLOGY ACT, 2000

As amended by the Information technology Amendment Act 2008 which came into force on 27-102009 provides legal framework to address the issues connected with hacking and security breaches of information technology infrastructure. Section 70 of the Act provides to declare any computer resource which directly or indirectly affects the facility of critical Information Infrastructure, to be a protected system. Section 70 (a) provides for establishment of National Nodal Agency in respect of critical information Infrastructure protection. Section 70B has empowered Indian Computer Emergency response Team (CERT-In) to serve as national nodal agency in the area of cyber Security[13].

LOGICAL SECURITY

It is a cyber-security battlefield where digital information is being exchanged or stored and security measures are performed by a non-human device in the digital world. This Logical Security is carried out by:

a) Encryption
b) Network security
c) System security
d) Application security
e) Security monitoring/auditing

NATIONAL INFORMATION CENTRE (NIC)

A premier organization providing network backbone and e-governance support to the Central Government, Union Territories, Districts and other Government bodies. It provides wide range of information and communication technology services including nationwide communication network fir decentralized planning improvement in government services and wider transparency and local government.

Provides services to Ministries/Departments that is continuously strengthening the security if the network operated by them and its services by enforcing security policies, conducting regular security audits and deploying various technologies at different level of the network to defend against the newer techniques being adopted by the hackers from time to time.

[13] *Crisis management Plan for cyber attacks, Ministry if communication and information technology, available at : http://pib.nic.in*

ANOTHER STEPS THAT CAN BE TAKEN TO ENABLE CYBER SECURITY IS PROVIDING TRAINING TO THE CYBER TROOPS

Training the Cyber Troops is also important to insure cyber security. Such training can be provided in three ways by:

1. Proactive securing of target includes the deployment of a system with the applications of security checklists in order to bring the systems and network components to a securely configured level. There are passive security measures deployed to monitor the system as well as provide sufficient auditing data to identifying that happened.
2. Immediate reaction on an attack and security of the target in analogous to security drills on a military case. Here, an alert is issued to team members who have to gain control over the system and remove all the attackers from the system (It is done in cooperation with offensive warfare teams). After alert is issued there needs to be an escalation procedure executed which informs global Security Control center (GSC2) of an ongoing attack.
3. Security forensics after attack and securing of targets infrastructure to prevent more attacks that takes place in systems which are already hacked. Its main objective is to analyze system state and logs and reconstruct the actions that attackers did. This can help to secure the system as well as give some information to offensive warfare teams how to perform similar attacks. It objective is to detect what has been changed in the system to prevent further damages or fraud.

FURTHER, IN 2014 A NOTIFICATION WAS ISSUED LAYING DOWN GUIDELINES FOR STEPS TO BE TAKEN BY CYBER CAFES TO ENSURE CYBER SECURITY[14].

1. That all cyber café will be registered with the agency called as registration agency as notified by the Appropriate Government in this regard including:

a) Name of the establishment;
b) Address with contact details including email address;
c) Whether individual or partnership or sole proprietorship or society or company;
d) Date of incorporation;
e) Name of owner/partner/proprietor/director;
f) Whether registration or not (if yes, copy of registration with Registrar of firms or registrar of companies or societies);
g) Type of service to be provided from cyber café.

2. That the cyber café shall not allow any user to use its computer resource without the identity of the user being established with documents such as:

a) Identity card issued by any school or college; or
b) Photo credit card or debit card issued by a Bank or Post Office; or
c) Permanent Account Number (Pan) card issued by Income tax Authority; or
d) Voter Identity Card; or
e) Passport; or
f) Photo identity issued by the employer or any government agency;
g) Driving License issued by the appropriate Government; or
h) Unique Identification Authority of India (UIDAI)

3. The Cyber café should keep a record of the user identification document by storing a photocopy or a scanned copy of the document fully authenticated by the user and authorised representative of the cyber café. Such record must be kept in a secure location for at least one year.

4. That the cyber café may photograph the user using a web camera installed on one of the cyber café's computers in order to establish the user's identification. Such web camera photos, officially authenticated by the user and an authorised representative of the cyber cafe, must be included in the log register, which may be kept in physical or electronic form.
5. A minor who does not have a photo identity card must be accompanied by an adult who has any of the documents that serve as identification.
6. That the cyber café shall record and retain the required information for each user and accompanying person, if any, in the log register for a minimum of one year, and that the cyber café may maintain an online version of the log register. The online log register version must be authenticated using digital or electronic means. Address, gender, contact number, kind and detail

[14] *Notification no G.S.R. 315(E), New Delhi, the 11th April, 2014, available at: http://www.mit.gov.in/sites/upload_files/dit/files/GSR_10511(1).pdf*

of identification document, date, computer terminal identification, log in time, and log out time must all be recorded in this register.

7. If the cyber café has legitimate doubts or suspicions about any user, they must immediately notify the appropriate authorities.

8. That the cyber café shall prepare a monthly report of the log register showing date wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of the next month.

9. That the owner of the cybercade keep backups of the following log records for each access or login by any user to its computer resource for at least one year. This contains the history of websites viewed via computer resources at the cyber café, as well as logs from the proxy server installed at the cyber café.

10. Management of physical layout and computer resource:

a. Partitions of cubicles built or installed if any, inside the cyber café shall not exceed four and half feet in height from the floor level.

b. The screen of all computers installed other than in partition or cubicles shall face outward i.e. they shall face the common open space of the cyber café.

c. Any cyber café having cubicles or partition shall not allow minors to use any computer resource in cubicles or partitions except when they are accompanied by their guardians or parents.

d. All time clocks if the computer systems and severs installed in the cyber café shall be synchronized with the Indian Standard time.

e. All the computers in the cyber café may be equipped with commercially available safety or filtering software so as to avoid as as possible, access to the websites relating to pornography including child pornography or obscene information.

f. Cyber café shall display a board, clearly visible to the users, prohibiting those viewing pornographic sites as well as copying or downloading information which is prohibited under the law.

g. Cyber café shall take sufficient precautions to ensure that their computer resources are not utilized for any illegal activity.

h. Cyber café shall incorporate reasonable preventive measures to disallow the user from tampering with the computer system settings.

i. Cyber cafe shall also maintain a record of its staff for period of one year.

j. Cyber café shall maintain the user identity information and the log register in a secure manner.

k. Cyber cade shall mot misuse or alter the information in the log register.

These guidelines are one of the effective steps that are being taken by Indian Government to combat misuse of Internet by the terrorist. Also, follow the above mentioned guidelines will to some extend help in ensuring cyber security and protection of communication and information infrastructure. It can prove as an effective tool in the hands of government to check the activities if terrorist groups and to have catch hold wrongdoer.

CONSTITUTION OF INDIA

The Indian constitution, like all other constitutions around the world, is organic and living in character, capable of moulding itself according to the time and needs of the society. It is because of this transformation in society that effective law in a country is required to deal with the problems that are taking on new shapes and positions in a society. Terrorism on the internet is the worst type of crime perpetrated in the cyber world, with a significant impact on the physical world. It is necessary to broaden the scope of physical rules so that it includes the act that requires urgent attention. Hence, the protection of various articles are extended to safeguard the rights of an individual in cases if misuse if internet.

Besides these provision there have been other initiatives taken in India to ensure cyber Security.

NATIONAL INFORMATION SECURITY ASSURANCE PROGRAMME

The National Information Security Assurance Programme (NISAP) is an initiative launched by the Government of India to enhance information security and protect critical national assets from cyber threats. It is a comprehensive program aimed at establishing a robust security infrastructure across government organizations and promoting a secure digital ecosystem for the country.

The primary objective of NISAP is to strengthen the security posture of government entities and ensure the confidentiality, integrity, and availability of information and information systems. The

program focuses on creating a proactive and risk-based approach to information security management, taking into account emerging cyber threats and technological advancements.

In conclusion, the National Information Security Assurance Programme (NISAP) of the Government of India is a comprehensive initiative that aims to strengthen information security across government entities. By establishing robust security measures, promoting capacity building, fostering collaboration, and ensuring compliance, NISAP plays a vital role in protecting critical national assets from cyber threats and building a secure digital ecosystem for the country.

Cryptography, Privacy and National Security Concerns- Users now have a new platform on which to voice their opinions and grievances thanks to the internet. The freedom to talk and communicate must be permitted with the least amount of State intervention, or in other words, without State intrusion, as a necessary corollary. The contentious subject of the right to privacy is instantly brought up by this. It might be seen as a logical extension of the right to free speech and expression. At the same time, it is well known that constraints must be placed on liberty in order for each member of society to be best protected. People can communicate using methods that a third party cannot comprehend unless they have been specifically given permission to do so by the communicators themselves thanks to the practise of encryption and the study of cryptography. Therefore, it would appear that this practise is a lawful application of the right to freedom of expression as well as the right to an uninhibited private dialogue.[15]

BREACH OF CONFIDENTIALITY AND PRIVACY UNDER THE INFORMATION AND TECHNOLOGY ACT 2000

If a person has secured access to any electronic record, book register correspondence, information, documentor othermaterial without the consent of the person concerned and discloses the same to any other person then he shall be punishable with imprisonmentupto two years, or with fine which may extend to one lakh rupees, or with both.[16]

the celebrated case of *P.U.C.L.* v. *U.O.I,*[17] Where the issue of telephone tapping of several wellknown personalities connected with the field of politics was examined, the Hon'ble supreme court, speaking through Hon'ble justice Kuldip Singh held that:

"Telephone tapping was definitely a move against privacy and therefore, ought not to be permitted except in the gravest of grave circumstances such as public emergency."

The Indian Telegraph Act's section 5[2] clause, which is analogous to section 69 of the Information Technology Act of 2000, was challenged in this case. The Indian Telegraph Act's Section 5(2) had its constitutional validity upheld by the Court, but it also stated that the right to privacy could not and should not be violated unless a public emergency had occurred or the public's safety was in danger.

Along the decades, the concerns surrounding privacy rights have also generated considerable debate in the United States of America. The US government has exhibited the necessary care to protect national security while keeping the question of the right to privacy under close scrutiny. The Federal Bureau of Investigation in the United States has proposed installing monitoring software with every ISP so that everyone may watch and observe all of the suspects' emails and online browsing history. They have set up diagnostic tools like Carnivore, which has been utilised effectively a number of times and has shown cases when adults attempted to have sex with kids online. It has also used the carnivore to capture bomb-makers.

CONCLUSION

Negative thoughts are responsible for the digital divide and brain drain. The development of technology has brought hackers and terrorists together. Being a hacker and being a cyberterrorist

[15] Supra Note 47, p. 40

[16] According to section 72 of the above mentioned Act.

[17] [1997 (1)SCC318].

are tightly related, and the day will soon come when terrorists themselves will be skilled hackers, changing the face of terrorism forever. As in the Bruce Willis film "Live Free or Die Hard," in which hackers bring down the communications network, transportation network, and power grid in that order. This is why a common vision is required to ensure cyber security and prevent cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy while governments are trying to counter and catch those using traditional means.

Thus to ensure cyber security and avoid misuse of internet in terrorist activities, nationally and internationally many steps can be taken. In India, at individual as well as at governmental level some of the steps that can be taken can be summarized as below:

1. Implementing strong access control systems to ensure that only authorized individuals can access cyber systems. For which CERT-In should engage academic institutions and follow an aggressive strategy.
2. Using strong encryption to ensure confidentiality and integrity of information stored, processed, and transmitted on and through cyberspace.
3. Closely monitoring all cyber activity by using log files and log analyzers.
4. Implementing effective detection systems to recognize cyber-attacks quickly. Like "Check the Web" initiative adopted by European Union.
5. Appointing active cyber-security leadership, giving training to officials in the field of cyber-security, to implement a real-time national defense strategy, Joint efforts by all Government agencies including defence forces to attract qualified skills personnel for implementation of counter measures. Similar to Cyber Intelligence (CYBERINT)[18] Analysis Center (CAC) established by China.
6. Developing filters, like one created by china "The Great Firewall of China", to remove terrorism-related content from the web or to deny access to terrorist websites through ISP filtering systems. Like ISPs in the United Kingdom already cooperate with law enforcement to shut down sites with illegal content, including sites containing child pornography.

Further, efforts must be made to educate the general public about the dangers of cyber terrorism, and these efforts must be made not only at the international and national levels but also at the level of the individual. This is necessary because the cyber world is a place where activities can be carried out with ease and without concern for punishment or detection. In today's information and technology age, everyone on the internet faces the risk of being utilised inappropriately, not just high profile websites.

Therefore, every internet user should exercise caution and vigilance when using the internet, and they should take precautions like frequently changing their passwords and avoiding opening emails from strangers. Another action that can be performed is to include a significant portion of our population in the effort to address issues with cyberspace security and endure in the race to save ourselves. However, there are steps one may take to reduce the likelihood of harmful incursions and their potential for damage. Unfortunately, there is no 100% guarantee that even with the best protection some negative things won't happen.

[18] *The creation of a Cyber Intelligence (CYBERINT) Analysis Center to develop and evaluate methods to improve the ability to detect, identify and deter Cyberterrorist attack. It also proposes ways to implement responsible, accountable and identifiable use of the Internet, and deny anonymity to the attackers.*