CHAPTER V

CYBER CRIME AGAINST
GOVERNMENT
CHAPTER V

CYBER CRIME AGAINST GOVERNMENT
(CYBER TERRORISM)

Language, religion, culture and geographical areas are different but the process of birth is same. A man sees the sunlight irrespective of caste and creed in the entire world in the said identical process. Birth and death of a man is controlled by an evolved process. The politics, culture, language religion and geographical areas cannot create any variation in the system.

Right to life, right to liberty, right to expression, pollution free air and water, small shelter over the head, a piece of cloth and bare minimum food to save the life are the birth right of every human being. Whatever language he speaks or wherever he stays, these rights are the basic rights of a civilized human being without which nobody can survive a decent life, but due to creation of difference by the system itself between the classes and the masses those rights are nowadays affected often times and again.

The innocent poor people are not getting their due share to what they are entitled and for this reason some section of people are annoyed with the system and resort to take the law in their own hands to achieve their goals by
way of violence which is an expression of anger or resentment, and this phenomenon is not to be branded as terrorism.¹

Terrorism can be defined as a system of violence- murder, kidnapping, bombing, hijacking of aircraft and taking air hostages to achieve particular purpose or desired goals by force.

**Terrorism defined by Federal Bureau of Investigation**

"The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political and social objectives".

**USC Title 22, Ch. 38, Sec. 2656 (f) d²**

Terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The United States has employed this definition of terrorism for statistical and analytical purposes since 1983. U.S. Department of State, 2002, Patterns of Global Terrorism, 2003.

Various forms of terrorism are as: individual terrorism, group terrorism, state terrorism, revolutionary terrorism, international terrorism and last one which is established by technological development i.e. cyber terrorism.


5.0 Conceptual Framework

The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism".

Cyber-terrorism is starkly different from common Internet crimes like identity theft and money fraud in that it can involve use of technology to divert or destroy systems and infrastructure, cause injury or death and undermine economies and institutions. To accomplish their goals, cyber-terrorists target the computer systems that control air traffic, electric power grids, telecommunications networks, military command systems and financial transactions.

The world was shocked by the despicable attacks and loss of innocent life on Sept 11, 2001, carried out by 19 airplane hijackers on a suicide mission. But that tragedy, horrific as it was, could be dwarfed by just one or two skilled Internet users who don't even set foot in their target country. It is frightening to imagine the human and economic toll if the computer systems

---

which control air traffic, nuclear power plants or major dams were brought down or thrown into confusion by cyber-terrorists.  

In 1997 Barry Collin who is said to have coined the term cyber terrorism as “the intentional abuse of digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action”.  

The FBI defined Cyber Terrorism, “the premeditated, politically motivated attack against information, computer system, computer programs and data which results in violence against non combatant targets by sub national groups or clandestine agents”.  

Security expert Dorothy Denning defines cyber terrorism as “... politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage.  

The Federal Emergency Management Agency (FEMA)
Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

**The U.S. National Infrastructure Protection Center:**

A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda.

The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism. The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace" is such that new methods and technologies are invented regularly; hence it is not advisable to put the

---

9 The expression “includes,” means that an inclusive, and not exhaustive, option is given by the legislature to meet the future challenges. If the expression “means” is used, then it signifies that the subject matter is exhaustive in nature.

10 The concept of cyber space signifies that the act or omission occurred due to the use of information technology (internet), which generally is intangible in nature, but may have adverse tangible consequences.
definition in a straightjacket formula or pigeon hole. In fact, the first effort of
the Courts should be to interpret the definition as liberally as possible so that
the menace of cyber terrorism can be tackled stringently and with a punitive
hand. The law dealing with cyber terrorism is, however, not adequate to meet
the precarious intentions of these cyber terrorists and requires a rejuvenation
in the light and context of the latest developments all over the world. The
laws of India have to take care of the problems originating at the international
level because the Internet, through which these terrorist activities are carried
out, recognises no boundaries. Thus, a cyber terrorist can collapse the
economic structure of a country from a place with which India may not have
any reciprocal arrangements, including an "extradition treaty". Cyber
terrorism emerges as a lethal pathogen in a shrinking world whereby we are
all surrounded by an unknown enemy. The fanciful notion of cyber terrorism
is looming larger than ever. It is said, "..The modern thief can steal more with
a computer than with a gun. Tomorrow's terrorist may be able to do more
damage with a keyboard than with a bomb".11 The only safeguard in such a
situation is to use the latest technology to counter these problems. Thus, a
good combination of the latest security technology and a law dealing with
cyber terrorism is the need of the hour.

5.1 Forms of Cyber Terrorism

Cyber terrorism as mentioned is a very serious issue and it covers a wide range of attacks. Here, the kind indulgence is asked toward the definition of Cyber Crime. "Cyber Crime" is crime that is enabled by, or that targets computers. Cyber Crime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws. However, cyber crime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data.\(^{12}\)

Some of the major tools of cyber crime may be: Botnets, Estonia, 2007, Malicious Code Hosted on Websites, Cyber Espionage etc. It is pertinent to mark here that there are other forms which could be covered under the heading of Cyber Crime & simultaneously are also the important tools for terrorist activities. Discussing these criminal activities one by one are as:

5.1.1 Attacks via Internet

(i) Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any

---

kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another person’s website called as web hijacking.

(ii) Trojan Attack:

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan Horse is popular. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP\textsuperscript{13} protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

(iii) Virus and Worm attack:

\textsuperscript{13} Transmission Control Protocol/ Internet Protocol.
A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms. The latest in these attacks is “Michael Jackson e-mail virus-Remembering Michael Jackson”. Once it infects the computer it automatically spread the worm into other internet users.

5.1.2 E-mail & IRC related crimes

(i) Email spoofing:

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

(ii) Email Spamming:

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

(iii) Sending malicious codes through email:

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

(iv) Email bombing:

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address. It includes:

(v) Sending threatening emails
(vi) Defamatory emails

(vii) Email frauds

(viii) IRC (Internet relay chat) related

5.1.3 Attack on Infrastructure

Our banks and financial institutions; air, sea, rail and highway transportation systems; telecommunications; electric power grids; oil and natural gas supply lines—all are operated, controlled and facilitated by advanced computers, networks and software. Typically, the control centers and major nodes in these systems are more vulnerable to cyber than physical attack, presenting considerable opportunity for cyber terrorists. There, could be possible consequences of a cyber-terrorism act against an infrastructure or business, with a division of costs into direct and indirect implications:

(i) Direct Cost Implications by cyber terrorism:

- Loss of sales during the disruption

- Staff time, network delays, intermittent access for business users

- Increased insurance costs due to litigation

- Loss of intellectual property - research, pricing, etc.

- Costs of forensics for recovery and litigation

- Loss of critical communications in time of emergency

(ii) Indirect Cost Implications by cyber terrorism:

- Loss of confidence and credibility in our financial systems
- Tarnished relationships and public image globally

- Strained business partner relationships - domestic and internationally

- Loss of future customer revenues for an individual or group of companies

- Loss of trust in the government and computer industry.

(iii) Attacks on Human Life:

Examples:

- In case of an air traffic system that is mainly computerized and is set to establish the flight routes for the airplanes, calculating the flight courses for all the planes in the air to follow. Also, plane pilots have to check the course as well as the other planes being around using the onboard radar systems that are not connected to external networks, therefore it can be attacked by the cyber-terrorist.

- A different example would be the act of cyber-terrorism against a highly-automated factory or plant production of any kind of product: food, equipment, vehicles etc. In case this organisation is highly reliant on the technological control, including a human control only in the end of production, not on the checkpoint stages, then any malfunction would be extremely hard to point out, fix and as a result to spot out a cyber-crime being committed.
5.2 Privacy violation

The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate.\textsuperscript{14} The right to privacy as an independent and distinctive concept originated in the field of Tort law. In recent times, however, this right has acquired a constitutional status in \textit{Rajagopal v. State of Tamil Nadu},\textsuperscript{15} the violation of which attracts both civil as well as criminal consequences under the respective laws. Modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. With the advent of information technology the traditional concept of right to privacy has taken new dimensions, which require a different legal outlook. To meet this challenge recourse of Information Technology Act, 2000 can be taken. The various provisions of the Act protect the online privacy rights of the net users. These rights are available against private individuals as well as against cyber terrorists. Section 1 (2) read with Section 75 of the Act provides for an extra-territorial application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of

\textsuperscript{14} Merriam-Webster Online Dictionary, definition of “privacy” available at http://www.merriam-webster.com/dictionary/privacy; (Visited on June 22, 2010).

\textsuperscript{15} AIR (1994) 6 SCC 632.
computer, computer system or computer network located in India, he would be liable under the provisions of the Act. This makes it clear that the long arm jurisdiction is equally available against a cyber terrorist, whose act has resulted in the damage of the property, whether tangible or intangible.

**Secret information appropriation and data theft:**

The information technology can be misused for appropriating the valuable Government secrets and data of private individuals and the Government and its agencies. A computer network owned by the Government may contain valuable information concerning defence and other top secrets, which the Government will not wish to share otherwise. The same can be targeted by the terrorists to facilitate their activities, including destruction of property. It must be noted that the definition of property is not restricted to moveable or immovable alone. In *R.K. Dalmia v. Delhi Administration*\(^\text{16}\) the Supreme Court held that the word "property" is used in the I.P.C in a much wider sense than the expression "movable property". There is no good reason to restrict the meaning of the word "property" to moveable property only, when it is used without any qualification. Whether the offence defined in a particular section of I.P.C can be committed in respect of any particular kind of property, will depend not on the interpretation of the word "property" but on the fact whether that particular kind of property can be subject to the acts covered by that section.

\(^{16}\) AIR 1962 SC 1821.
5.3 Demolition of e-governance base

The aim of e-governance is to make hassle free interaction of the citizens with the government offices and to share information in a free and transparent manner. It further makes the right to information a meaningful reality. In *P.U.C.L. v. U.O.I.*\(^{17}\) the Supreme Court specified the grounds on which the government can withhold information relating to various matters, including trade secrets. The Supreme Court observed: “Every right- legal or moral- carries with it a corresponding objection. It is subjected to several exemptions/ exceptions indicated in broad terms”.

In a nutshell the Cyber terrorists use various tools and methods to unleash their terrorism. Some of the major tools are as follows:

1. Hacking
2. Cryptography
3. Trojan Attacks
4. Computer worms
5. Computer viruses
6. Denial of service attacks
7. E-mail related crimes

**Motives behind any Attacks are:**

1. Putting the public or any section of the public in fear; or

\(^{17}\) AIR 2004 SC 1442.
2. Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or
3. Coercing or overawing the government established by law; or
4. Endangering the sovereignty and integrity of the nation.\textsuperscript{18}

5.4 International Effort in Combating Cyber Terrorism

International cooperation in order to confront with cyber terrorism has different form of relationship among government and law enforcement agencies. The cooperative efforts are divided into three types: international and global efforts, multilateral and multinational effort and regional effort.

A. Efforts from International and Global Organization:

(i) United Nation

United Nation is the lead organization which involves in the coordination and cooperation relating to the problem of international terrorism.\textsuperscript{19} In their resolutions, they require the member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats. These resolutions have the same motive to improve the cyber security awareness at

\textsuperscript{18} \url{http://www.mondaq.com/article.asp?articleid=28603} (Visited on January 13, 2010).

\textsuperscript{19} Nazura Abdul Manap and Pardis Moslemzadeh Tehrani; Cyber Terrorism: Issues in Its Interpretation and Enforcement. Available at \url{http://www.ijiee.org/papers/126-I149.pdf}; (Visited on June 8, 2012).
both the international and the national levels. However, following the tragedy of 11 September the Security Council resolution 1373 moves forward to fight against terrorism. The aim of this resolution is to counter terrorism effort. This resolution provides an internationally recognized definition of terror for the first time which seems to provide an inclusive ban on all forms of violence that internationally targeted civilian, regardless of the motive, as well as calls on countries to prosecute terrorists.

(ii) Interpol

The basement of Interpol is to prevent and combat international crime even where diplomatic relations do not exist between particular countries and it works on the gaps between the legal framework and criminal phenomena. Interpol has created an anti-terrorism section in September 2002 in the wake of alarming of international terrorist attack which is called Fusion Task Force (FTF). The primary objectives are to: identify active terrorist groups and their membership, solicit, collect and share information and intelligence, provide analytical support, enhance the capacity of member countries to address the threats of terrorism and organized crime. Interpol has identified public safety and terrorism as a priority crime area, and countries can benefit from

---


Fusion task force, http://www.interpol.int/Public/FusionTaskForce/default.asp; (Visited on May 12, 2010).
Interpol’s unique position in the international law enforcement community in the fight against terrorism.

**B. Efforts from Multilateral and Multinational Organization:**

(i) **The Commonwealth Nations**

Commonwealth nation’s main task is to harmonize their laws of its member states. It creates the Model Law on Computer and Computer Related Crime and had a great impact on the domestic legislation. It expands criminal liability including reckless liability for the offences of interfering with data, interfering with computer systems, and using illegal devices. Also, it covers the problem of dual criminality by condemning the act which has done by offender out side his territorial nationality, if he does an offence under a law of the country where the offence was committed. Another task of the commonwealth is to consider the legal mutual legal assistant between commonwealth member and also between commonwealth member and non commonwealth. The commonwealth law minister proposes to member state to take the convention on cybercrime as a basis for mutual legal assistance between Commonwealth member states and Non-commonwealth States.\(^{22}\)

(ii) **The Group of G 8**

The group G8 is an informal forum and so it lacks an administrative structure compare with international organization. The group of G8 was

originally formed in 1975 with six members and it was known as the G6. Canada then joined in 1975 and Russia became a formal member in 1998. The leaders from the United States, United Kingdom, France, Germany, Japan, Canada, Italy, and Russia have been meeting annually since 1975 to discuss issues of importance, including crime and terrorism, and the information highway.\(^23\)

(iii) **Organization for Economic Cooperation and Development (OECD)**

The OECD is a unique forum where the governments of 30 countries work together to address the economic, social and environmental challenges of globalization. The OECD has been working for many years on a range of policy issues associated with the information society. These include infrastructure and services, consumer protection, privacy and security, through to broader issues surrounding ICT and economic growth.\(^24\) The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to establish a heightened priority for security planning and management and to promote a culture of security among all participants as a means of protecting information systems and networks.\(^25\) The aim of this guideline is to develop a global culture of security through advice on policies and measures to address

\(^23\) What is the G8, http://www.g7.utoronto.ca/ (Visited on May 10, 2010).

\(^24\) http://www.intgovforum.org/brief.htm (Visited on June 2, 2010).

\(^25\) Ibid.
internal and external threats such as cyber-terrorism, computer viruses or hacking in a globally interconnected society, while preserving important societal values such as privacy and individual freedom.

C. Efforts from Regional Organization:

(i) European Union

After the terrorist attack at Madrid, the European Union and its members promise to do everything in their power to combat all forms of terrorism. Therefore, the European union approves the decision of European Parliament to declare 11th March as European day commemorating the victim of terrorism.26 By December 2004, European union calls on member states to ratify the convention on the mutual assistance in criminal matters, its protocol and the three protocols to Europol convention. Also, their framework implement in other aspects such as, traffic data by service provider, cross-border pursuit, exchange of information on conviction for terrorist offences and etc. The council adopted necessary measures for council regulation to identify new and applicable function for the Schengen information system (SIS).27

(ii) Council of Europe

The main task of council of Europe since 1949 has been to maintain human rights, the rule of law and pluralist democracy, and is determined to

27 Id at p. 7.
combat terrorism which combats with these values. Following the unparalleled
terrorist attacks in the United States, its efforts were stepped up in 2001. It tried to
fight against cyber terrorism by strengthening legal action against terrorism,
safeguarding fundamental values, and addressing the causes of terrorism.28

The Council of Europe set its focus area on cyber terrorism and the subject of
CODEXTER (the Committee of Expert against Terrorism) is about cyber terrorism. It has been surveying the situation in member states to evaluate whether existing international instrument are sufficient to respond cyber threat or not.29 The CODEXTER has concluded at the end of these meeting that the use of Internet for terrorist purposes includes several elements:

(i) attacks via the Internet that cause damage not only to essential electronic communication systems and IT infrastructure, but also to other infrastructures, systems, and legal interests, including human life

(ii) dissemination of illegal content, including threatening terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for

---

and financing of terrorism; training for terrorism; recruiting for terrorism; as well as

(iii) other logistical uses of IT systems by terrorists, such as internal communication, information acquisition and target analysis.\(^{30}\)

(iii) Convention on Cybercrime

The Convention put into effect in July 2004, which is the first and only international treaty to deal with breaches of law over the Internet or other information networks. This convention has not only been ratified by all European Union member states, but also it does not specifically address cyber terrorism. The Convention requires participating countries to update and synchronize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other unlawful cyber activities.\(^{31}\) Indirectly, it can be applicable for cyber terrorism as well. Although the convention on cyber crime does not define the term cyber crime and cyber terrorism specifically, Article 2 to 6 mention various forms of criminal activities that are prohibited which may include cyber terrorism activities.


(iv) **Council of Europe: Convention on the Prevention of Terrorism**

The Council of Europe has adopted the Convention on the prevention of terrorism to increase the effectiveness of existing international texts on the fight against terrorism. The aim of the convention is to strengthen member states’ efforts to prevent terrorism and sets out two ways to achieve this objective: first, establish a certain acts of criminal offences, and second, it reinforces the cooperation on prevention both internally (national prevention policies), and internationally (modification of existing extradition and mutual assistance arrangements and additional means). In other words, the Convention contains a provision on the protection and compensation of victims of terrorism.

(v) **Asia Pacific Economic Cooperation (APEC)**

APEC is a regional forum which was established in 1989 for facilitating economic growth and its goal is to strengthening the Asia- pacific community. APEC has 21 members and it has not obliged their members and decisions made within (APEC) are reached by consensus. After September terrorist attack on United States, APEC issued a statement on counter- terrorism and condemns these attacks and efforts to collaborate to fight against terrorism.

(vi) **North Atlantic Treaty Organization (NATO)**

NATO was founded in 1949 on the basic principle of collective defense. The parties are following the basic principle of the Charter of the United Nations.
This cooperation and commitment to security continues among the members nations today. However, the Internet, cyber space and cyber crimes were not in existence at the time that NATO was established.

Nevertheless, NATO has changed their political and technical requirement and improved their capabilities in the area of cyber defense. NATO has also to address new challenges posed by terrorists and the threats to computer information systems (CIS).32

(vii) **International Multilateral Partnership against Cyber Terrorism (IMPACT)**

The International Multilateral Partnership Against Cyber Threats (IMPACT), backed by the United Nations (UN) International Telecommunication Union (ITU) and International Criminal Police Organization (Interpol), which is known as the world’s first comprehensive global public-private partnership between governments, industry leaders and cyber security experts to enhance the global community’s capacity to prevent, defend and respond to cyber threats. It has launched its global headquarters in Cyberjaya of Malaysia on 20th March 2009. It will act as a centralized anti-cyber-terrorism intelligence centre which allows its 191 member countries to be alerted on cyber-terrorism threats such as attacks against the global financial system, power grids, nuclear plants, air traffic control systems and others.

IMPACT seeks to bridge the gap that exists between domestic and international spheres in countering cyber threats. It promotes greater cooperation in combating cyber threats. Impact is supported by International Telecommunication Union and it functions as an operational home for International Telecommunication Union.

5.5 Laws in Various Countries on Cyber Terrorism

5.5.1 Singapore

New laws allowing Singapore to launch pre-emptive strikes against computer hackers, have raised fears that Internet controls are being tightened and privacy is compromised in the name of fighting terrorism. The city-state's parliament has approved tough new legislation aimed at stopping "cyber terrorism," referring to computer crimes that endanger national security, foreign relations, banking and essential public services. Security agencies can now patrol the Internet and swoop down on hackers suspected of plotting to use computer keyboards as weapons of mass disruption. Violators of the Computer Misuse Act such as website hackers can be jailed up to three years or fined up to S$10,000 ($5,800).

5.5.2 Malaysia

Malaysia is to establish an international centre to fight cyber-terrorism, providing an emergency response to high-tech attacks on economies and trading systems around the globe, reports said. Prime Minister Abdullah
Ahmad Badawi, during a visit to the United States said, that the facility, sited at the high-tech hub of Cyberjaya outside Kuala Lumpur, would be funded and supported by governments and the private sector. The New Straits Times said the centre would be modelled on the Centre for Disease Control in Atlanta, which helps to handle outbreaks of disease around the world.

Abdullah who announced the initiative at the close of the World Congress on Information Technology in Austin, Texas said the threat of cyber-terrorism was too serious for governments to ignore.

The Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism. They are helping all the member countries and training their personnel. The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 members and non-member countries including Japan, the USA, and Canada. This treaty has already enforced after its ratification by Lithuania on 21st March 2004.

The Association of South East Asia Nations (ASEAN) has set plans for sharing information on computer security.

5.5.3 The United Kingdom

The United Kingdom adopted Terrorism Act, 2000, which gives the definition of terrorism and also gives various provisions for Cyber terrorism.
5.5.4 Pakistan

Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life," according to the ordinance, which was published by the state-run APP news agency. The Prevention of Electronic Crimes law will be applicable to anyone who commits a crime detrimental to national security through the use of a computer or any other electronic device, the government said in the ordinance. It listed several definitions of a "terrorist act" including stealing or copying, or attempting to steal or copy, classified information necessary to manufacture any form of chemical, biological or nuclear weapon.

5.5.5 India

Earlier the term “cyber terrorism” was absent from the terminology of the Indian law, Section 69 of the Information Technology Act was a lone strong legislative measure to counter the use of encryption by terrorists. This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource. But after the 26/11 attack on Mumbai the Government of India took strong steps to strengthen the cyber security, including prohibition of terrorist activities through cyber space by way of amending the existing Indian information Technology Act, 2000. The provision that was specifically
inserted in this legislature for this purpose was section 66F which defines and describes cyber terrorism. Section 66F mentions that,\textsuperscript{33}

(1) Whoever,

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database,

\textsuperscript{33} Information Technology Act 2000 (Bare Act), Universal Law Publishing Co. Pvt. Ltd.(2011), p-36.
with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life’.

(a) Constitution of India

Any person who fails to assist the Government agency in decrypting the information sought to be intercepted is liable for imprisonment up to 7 years. Article 300A of Constitution of India states that all persons have a right to hold and enjoy their properties. In a specific case of Bhavnagar University v. Palitana Sugar Mills Pvt. Ltd. Supreme Court applied the constitutional clause with the interpretation that anyone can enjoy his or her property rights in any manner preferred. This also includes property rights to information stored on computers or in any electronic format.

34 AIR 2003 SC 511.
Articles 301 to 305 refer to the right for free trade. As long as an individual carries out a business in accordance with law, it cannot be interfered. Besides, free trade and any commercial activities cannot be visualized without technological rights, which mean that any distortion of those is illegal. In India these provisions have been effectively used to protect individual property rights against the actions of cyber-criminals.

(b) Penal Code

A big deal of protection is also provided by Indian Penal Code. Section 22 of it gives a definition of a "movable property" stating that it also includes all corporal properties. It means that any information stored on a computer can be conveniently regarded as a movable property as it can definitely be moved from one place to another and is not attached.\(^{35}\)

Section 29A of the Code with Section 2(1) (t) of the Information Technology Act provides that "electronic record means data, record, or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche".\(^{36}\)

5.6 Cyber-terrorism and Human Rights

Universal Declaration of Human Rights in its Preamble talks about a "freedom from fear and want". Freedom from fear is mostly a term of psychological nature, however, it is being used very widely nowadays

\(^{35}\) Misra, S.N.; Indian Penal Code; Central Law Publications; ed-13; p-88.
\(^{36}\) Id. p-94.
especially in cases of terrorism. Article 3 of the Declaration sets the right to “security of person”. As we know, term “person” also includes an environment (s)he exists in, different from the term “individual” which under one of the concepts imagines it as something abstract, apart from any other surrounding conditions. So protecting a personal security would also mean protecting his (her) social, economical and other connections, “threads” established with the environment. As long as in modern reality these are sometimes predominantly based on technology, computers or internet, cyber-terrorism protection also deals with “security of person”. Here I would also add Article 5 with its protection against “degrading treatment”. Personal harm is also a part of degradation and treating a person in a current way is something that may be provided by cyber-criminal act as it was proven above.

One important provision that I would like to pay special attention to is Article 12 of the Declaration. It states: “No one shall be subjected to arbitrary interference with his privacy, nor to attacks upon his honour or reputation”. “Privacy” is defined as “the quality or state of being apart from company or observation” which in combination with another definition of “freedom from unauthorized intrusion” given by the same source, also includes the privacy of computer-stored data and a right to enjoy its private state of non-interference without personal will of the possessor.

Article 17 sets a right to property and a restriction to deprive anyone from possessed property. Property is defined as “anything that is owned by a
person or entity”, including two types of it: “real property” and “personal property”. Personal property or “personality” includes “movable assets which are not real property, money, or investments.”

Article 19, however, plays a different role in this topic and is mostly associated with internet use by terrorists in general.

5.7 Cyber terrorism and Modern Terrorist

Cyber terrorism is an attractive option for modern terrorists, who value its anonymity, potential to inflict massive damage, psychological impact, and media appeal. This enables them to carry out acts of terrorism from their own tent, cave, bunker, or palace. Other considerations are as under:

(a) Low cost.

(b) Large variety of targets.

(c) Low risk to terrorists.

(d) Greater media coverage.

Cyber terrorism is an attractive option for modern terrorists for several reasons.

---


39 Ibid.
First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.

Second, cyber terrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

Third, the variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that
critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyber terrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

- Fourth, cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyber terrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.

- Fifth, as the I LOVE YOU virus showed, cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

Over a period of time, the level of sophistication required to hack into an information system has decreased. At the same time, the quality, quantity, and availability of hacking tools has increased. Cyber warrior tools are often readily available for downloading from the Internet. A comparatively low technology adversary with minimal funding, training, manning, and defence
infrastructure can resort to cyber terrorism at short notice from anywhere in the world. This creates a very dangerous target-rich and low-risk combination.

Some incidents of cyber terrorism:

The following are notable incidents of cyber terrorism:^40

- In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

- During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

- Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with

rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals. Electro hippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999.

One of the worst incidents of cyber terrorists at work was when crackers in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. More recently, in May 2007 Estonia was subjected to a mass cyber-attack by hackers inside the Russian Federation which some evidence suggests was coordinated by the Russian government, though Russian officials deny any knowledge of this. This attack was apparently in response to the removal of a Russian World War II war memorial from downtown Estonia.41

5.8 Technological Protection from Cyber Terrorism

Information Technology is the lifeline of most organizations today, and as such a disrupted information system can cause your company to lose market share and eventually bring it to its knees. 94% of companies without a tested crisis plan go out of business after a severe loss of service for two weeks or more. We are so bound as a global community that a disaster in a

---

single major city results in significant ripple effects around the world.\textsuperscript{42} Cyber terrorism, whether direct or indirect, is an issue all businesses should anticipate and arrange for backup plans. Depending on the size of the company, backups of the backup plan may need to be considered. Politically charged events frequently unleash a nest of virus', worms and Trojan horses on the Internet, and with increasing intensity. In one day, the current Nimda virus generated one hundred times the traffic that the code red virus took three days to do.

A group setup by the federal government to counter Cyber terrorism released a report stating that "A personal computer and a simple telephone connection to an Internet service provider anywhere in the world are enough to cause a great deal of harm. The right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend."

To protect your business in the event of a disaster you need to identify the mission critical information streams that need to be protected. This may include both print material and computer hardware and software.

\textsuperscript{42} http://technoworldinc.com/viruses/how_to_fight_cyberterrorism-135432.0.html;wap2=; (Visited on March 13, 2008).
(i) **Backup your Data**

Minimizing the loss of valuable documents or data can be accomplished quite easily by performing regularly scheduled backups. It is absolutely essential that OFF-SITE copies of backups be kept. This will assure quick recovery from disasters.

Backups may be done using a variety of medias, such as, floppy disks, zip disks, re-writeable cd's, and removable hard drives. The type of media you use will depend on the quantity of data being stored. Larger companies may also consider installing "mirror" servers, which allow the same real time information being kept in different locations. Consideration should also be given to outsourcing applications to ASPs (Application Service Providers) which have mirrored data centers. Any paper documents which are considered critical should also be backed up with the help of a scanner and stored off-site. Myriads of paper documents were strewn all over New York following the world trade centre (WTC) disaster. Many of the organizations and companies affected have no idea of what they have lost or even how to recover missing files. Some of which have irreplaceable information and signatures.

(ii) **Anti-Virus Software**

A good anti-virus software is essential in your counter terrorism arsenal. It will offer continuous protection and automatically scans all file inputs, outputs, downloads, program executions, and other system-related activities.
to help prevent virus penetration. If a virus is discovered, you will have the option to clean or delete the infected file.

(iii) Fire Walls / Detection Networks

Firewalls screen all communications to a system, including e-mail messages, which may carry logic bombs. The term "firewall" is a relatively generic term for methods of filtering access to a network. They may come in the form of a computer, router or other communications device, or in the form of a network configuration.

The services and access that are permitted to each user are defined by firewalls. One method is to screen user requests to check if they come from a previously defined domain or Internet Protocol (IP) address. Another method is to prohibit Telnet access into the system. Here are a few key things to remember in order to protect yourself from Cyber terrorism:

i. All accounts should have passwords and the passwords should be unusual, difficult to guess, and alphanumeric where possible.

ii. Change the network configuration when defects become known.

iii. Check with vendors for upgrades and patches. iv. Audit systems and check logs to help in detecting and tracing an intruder.

iv If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.
5.9 Legal Protection from Cyber Terrorism

If the three sovereign organs43 of the Constitution work collectively and in harmony with each other, the menace of cyber terrorism can be effectively curbed, if not completely eliminated. Further, a vigilant citizenry can supplement the commitment of elimination of cyber terrorism.

5.9.1 Legislative commitment

The legislature can provide its assistance to the benign objective of elimination of cyber terrorism by enacting appropriate statutes dealing with cyber terrorism. It must be noted that to give effect to the provisions of Information Technology Act, 2000 appropriate amendments have been made in the I.P.C, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. A new section dealing with cyber terrorism has been added in the Information Technology Act, 2000 by way of its amendment Act 2008. The repealment of POTA and its likely replacement with a new ordinance is an opportunity for the legislature to make the terrorist law effective to deal with cyber terrorism.

5.9.2 Executives concern

The Central Government and the State Governments can play their role effectively by making various rules and regulations dealing with cyber terrorism and its facets from time to time. The Central Government can, by

43 These are the “Legislature”, “Executives” and “Judiciary”.

203
notification in the Official Gazette and in the Electronic Gazette, makes rules to carry out the provisions of the Information Technology Act.\textsuperscript{44} Similarly, the State Government can, by notification in Official Gazette, makes rules to carry out the provisions of the Act.\textsuperscript{45} In exercise of the powers conferred by section 90 of the Information Technology Act, 2000 (Central Act 21 of 2000), the Government of Karnataka has made the Information Technology (Karnataka) Rules 2004.\textsuperscript{46} The Rules define "Cyber Cafe" as premises where the Cyber Cafe Owner/Network Service Provider provides the computer services including Internet access to the public.\textsuperscript{47} Rule 3 (1) provides that the owner of the Cyber Cafe shall take sufficient precautions so that computers and computer systems in the Cyber Cafe are not used for any illegal or criminal activity. Rule 3 (2) mandates that the Cyber Cafe Owner/Network Service Provider shall not allow any User to use his Computer, Computer System and/or Computer Network without the identity of the User being established before him before use. The Rule provides that the intending User may establish his Identity by producing any Photo Identity Card issued by any School or College or a Photo Credit Card of any Bank or Passport or Voters Identity Card or PAN Number Card issued by Income-Tax authorities or Photo Identity Card issued by the Employer or Driving License to the

\footnotesize{\textsuperscript{44} Section 87 of IT Act 2000. \\
\textsuperscript{45} Section 90 of IT Act 2000. \\
\textsuperscript{46} No: ITD 07 PRM 2004, Dated: 05.08.2004. \\
\textsuperscript{47} Rule 2(C) of the IT Act (Guidelines for cyber café Rule) 2011, p-196.}
satisfaction of Cyber Cafe Owner. Rule 4(1) provides that after the identity of the User is established, the owner of the Cyber Cafe or the manager or the attendant or on his behalf any authorized person managing the Cyber Cafe shall obtain and maintain the following information in the Log Register for each user: (i) Name of the User, (ii) Age and Sex of the User, (iii) Present residential address of the User, (iv) Log in time, and (v) Log out time. Rule 4 (2) provides that if a User cannot produce any Photo Identity Card to establish his identity to the satisfaction of the Cyber Cafe Owner/Network Service Provider, he may be photographed by the Cyber Cafe Owner/Network Service Provider after obtaining his consent using a 'Web Camera' hooked onto one of the computers or computer systems in the Cyber Cafe and the User shall be explained that his photograph will be taken and stored in the hard disk of the computer, for verification by Law enforcement authorities, whenever required. This is in addition to the entries made in the log register. The Rule further provides that in case the User does not agree for storing his photograph he shall not be allowed to use any computer, computer system and/or computer network or access to the Internet in the Cyber Cafe. Rule 4(3) provides that all time clocks in Cyber Cafes must be regularly checked and synchronized with Indian Standard Time (IST). Rule 4(4) provides that maintaining proper account of the User as explained shall be the responsibility of the Cyber Cafe Owner/Network Service provider. Rule 5(5) provides that the Log Register and the Photograph of the User shall be
maintained by the Cyber Cafe Owner/Network Service Provider for a minimum period of ONE YEAR and the same shall be provided to Law enforcement agencies as and when required. Rule 4(6) provides that the Cyber Police authorities may on complaint inspect Cyber Cafes at all reasonable time to ensure compliance of these rules. If any Cyber Cafe Owner/Network Service Provider fails to maintain Log Register and records he shall be liable for penalties as provided in the Act or any other Law, for the time being in force. These provisions are sufficient to take care of illegal use of cyber cafe for terrorist activities.

Further, the government can also block web sites propagating cyber terrorism. It must be noted that the Indian Computer Emergency Response Team (CERT-In) has been designated as the single authority for issuing of instructions in the context of blocking of web sites.\textsuperscript{48} CERT-In has to instruct the Department of Telecommunications to block the web sites after verifying the authenticity of the complaint and satisfying that action of blocking of website is absolutely essential. There is no explicit provision in the IT Act, 2000 for blocking of websites. In fact, blocking is considered to be censorship; hence it can be challenged if it restricts the freedom of speech and expression. But websites promoting hate, contempt, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism, pornography and violent sex can reasonably be blocked since all such
websites cannot claim the Fundamental Right of free speech and expression. The blocking of such website may be equated to "balanced flow of information" and not censorship. If the blocking of a website is arbitrary, unreasonable and unfair and is based on extraneous and irrelevant materials and reasons, then it would be vulnerable to the attack of unconstitutionality, being in violation of Articles 14, 19 and 21 of the Constitution of India.49

5.9.3 Judicial response

The judiciary can play its role by adopting a stringent approach towards the menace of cyber terrorism. It must, however, first tackle the jurisdiction problem because before invoking its judicial powers the courts are required to satisfy themselves that they possess the requisite jurisdiction to deal with the situation. Since the Internet "is a cooperative venture not owned by a single entity or government, there are no centralized rules or laws governing its use. The absence of geographical boundaries may give rise to a situation where the act legal in one country where it is done, may violate the laws of another country. This process further made complicated due to the absence of a uniform and harmonised law governing the jurisdictional aspects of disputes arising by the use of Internet. It must be noted that, generally, the scholars point towards the following "theories" under which a country may claim prescriptive jurisdiction:

(a) a country may claim jurisdiction based on "objective territoriality" when an activity takes place within the country,

(b) a "subjective territoriality" may attach when an activity takes place outside a nation's borders but the "primary effect" of the action is within the nation's borders,

(c) a country may assert jurisdiction based on the nationality of either the actor or the victim,

(d) in exceptional circumstances, providing the right to protect the nation's sovereignty when faced with threats recognised as particularly serious in the international community.

In addition to establishing a connecting nexus, traditional international doctrine also calls for a "reasonable" connection between the offender and the forum. Depending on the factual context, courts look to such factors, as whether the activity of individual has a "substantial and foreseeable effect" on the territory, whether a "genuine link" exists between the actor and the forum, the character of the activity and the importance of the regulation giving rise to the controversy, the extent to which exceptions are harmed by the regulation, and the importance of the regulation in the international community. The traditional jurisdictional paradigms may provide a framework to guide
analysis for cases arising in cyberspace.\textsuperscript{50} It must be noted that by virtue of section 1(2) read with section 75 of the Information Technology Act, 2000 the courts in India have "long arm jurisdiction" to deal with cyber terrorism.

5.9.4 Vigilant citizenry

The menace of cyber terrorism is not the sole responsibility of State and its instrumentalities. The citizens as well as the netizens\textsuperscript{51} are equally under a solemn obligation to fight against the cyber terrorism. In fact, they are the most important and effective cyber terrorism eradication and elimination mechanism. The only requirement is to encourage them to come forward for the support of fighting against cyber terrorism. The government can give suitable incentives to them in the form of monetary awards. It must, however, be noted that their anonymity and security must be ensured before seeking their help. The courts are also empowered to maintain their anonymity if they provide any information and evidence to fight against cyber terrorism.


\textsuperscript{51} The term citizenry is used in this chapter to cover people working in the real space and the expression netizen covers those operating in the cyber space.